障害再発事例へのD-CASE適用評価
T証券取引所

2013年10月11日

独立行政法人
科学技術振興機構
Japan Science and Technology Agency

1. 障害の概要

- T証券取引所での2012年2月、8月の2度にわたり発生したシステム障害の概要について示す

1. 株式売買システムの障害（平成24年2月2日）

（1）障害内容と経緯

- 午前1時27分
  - ◆ 情報配信ゲートウェイサーバーでハード障害が発生し、監視端末上に異常メッセージが表示された
  - ◆ 保守ベンダーが調査を行い、当日の売買業務への影響はないと判断（結果的に誤認）
  - ◆ 午前2時44分、上記、異常メッセージへの対応を完了
- 午前7時38分
  - ◆ 株式売買システムの一部銘柄で相場情報が配信できない事象が発生。その後、同日午前1時27分に発生したハード障害を契機とした予備系への切替え処理が正常に完了していないことが原因であると判明
- 午前9時00分
  - ◆ 当取引所の241銘柄及びS証券取引所の全74銘柄の売買を停止
  - ◆ 午前10時33分、システム障害の復旧作業を完了
  - ◆ 午前10時56分、売買再開に向け、売買業務及び相場報道業務に問題ないことを最終確認
- 午後0時30分
  - ◆ 取引を開始（後場）

1. 障害の概要

（2）株式売買システムの障害発生に関する再発防止措置等を金融庁に報告 （平成24年2月16日）

報告書では、障害の原因、当取引所の対応状況、責任の所在、処分、再発防止措置についてとりまとめ、報告されている

➢ 障害の原因

◆ サーバーを三重化することによって高い信頼性（注）を確保すること、障害診断ツールを整備して確実に障害を検知する仕組みを構築すること等、システム稼働前後の取組みから、システムの信頼性を過信していたため、業務影響が出る可能性があるにも関わらず、当取引所職員が主体的にシステムの状態を確認せず、問題なしと判断したことにありました。

◆ 本来であれば、本システムの稼働状況を、常時、監視及び確認できる体制を敷くべきでありましたが、深夜・早朝時間帯の十分な監視体制が整備できておりませんでした。また、業務に影響を与える可能性がある障害が発生した場合には、経営陣まで報告すべきでありましたが、業務に影響があると確定した場合に経営陣まで報告するルールとなっていたため、障害発生時の報告体制に不備がありました。

（注）99.999%以上の可用性の確保（5年間で10分程度の停止時間）を目標
（出典：ET2011講演資料より（「T証売買システム(arrowhead)のディペンダビリティ実現のための方式および機能」））

1. 障害の概要

（2）株式売買システムの障害発生に関する再発防止措置等を金融庁に報告 （平成24年2月16日）（つづき）

➢ 再発防止措置

1) 株式売買システムの障害発生に関する再発防止措置等

（注）青字の部分は、D-Case適用時の考慮ポイントを示す

◆ 障害対応の体制面での改善及び強化

» 障害時においては、業務影響があると確定した場合に、経営陣まで報告を行うルールとなっていましたが、業務影響の可能性がある場合には、経営陣まで報告を行うルール及び体制を確立します。また、開発を所管するIT開発部においては、障害対応時に直接状況を確認するよう体制を強化します。一方、運用を所管するITサービス部においては、深夜・早朝時間帯に、運用ベンダーに加え、当取引所職員もコンピューターセンターに常駐するよう体制を強化します。

◆ 確認手順及び確認項目の明確化

» 発生事象ごとの具体的な対応内容、確認手順及び対応の完了基準の明確化、障害対応アクションリストの再整備、深夜・早朝時間帯における障害連絡及び報告ルールの明確化など、計6つの対策を実施します。

◆ 速やかな復旧に向けた取組み

» 障害発生時の体制を強化するため、当取引所の早朝出社体制を強化します。また、保守ベンダーと協力し、ハード障害からのリカバリー手順を再整備のうえ、操作訓練を実施します。訓練は以降も継続実施します。

◆ 自動切替え発生時の動作確認

» 自動切替えを伴うハード障害が発生した場合には、設計どおりの動作となっているか毎回確認することとし、当該確認手順を整備します。

2) 本システムにおける切替え試験の実施

◆ 擬似障害再現による切替え機能及び対応フローの確認

◆ 全サーバーの切替え機能の確認

3) 再発防止策の他システムへの展開

2. デリバティブ売買システムの障害（平成24年8月7日）

（1）障害内容と経緯

- 午前9時18分
  - ◆ デリバティブ売買システムのネットワーク機器である業務L3スイッチの本番系（1号機）においてハードウェア障害が発生
  - ◆ 直ちに障害対策本部を立ち上げ、障害の特定・復旧に向けた対応に着手
- 午前9時22分
  - ◆ 全派生商品の取引を停止
  - ◆ 午前10時20分、システムの復旧作業を完了
- 午前10時40分
  - ◆ 注文受付再開
- 午前10時55分
  - ◆ 取引を再開

1. 障害の概要

(2)障害原因と対策

- 本番系(1号機)のハード障害に伴い、待機系(2号機)自体は本番系へ状態変更する自動切替処理を正常に動作させたが、本来の製品仕様と異なり、1号機では、内部の部分的なハード障害を1号機自身が正しく検知できなかったことから、1号機も本番系の状態のままとなっており、1号機、2号機の両方が、本番系の状態となった
- その結果、これらスイッチに接続されている装置から見て、1号機、2号機のどちらに電文を送信すべきなのか特定することが不可能となり、通信ができなくなった
- 本不具合に係る製品内蔵プログラムの改修版のシステムへの取込みは、テスト環境での十分な検証を経た後、9月中に行う。(なお、同様の事態が発生した場合にも、速やかに切替処理の実行が可能となるよう対策を既に講じている)

1. 障害の概要

（3）金融庁より業務改善命令を受けるとともに、再発防止策を発表（平成24年8月24日）

➢ 業務改善命令の内容

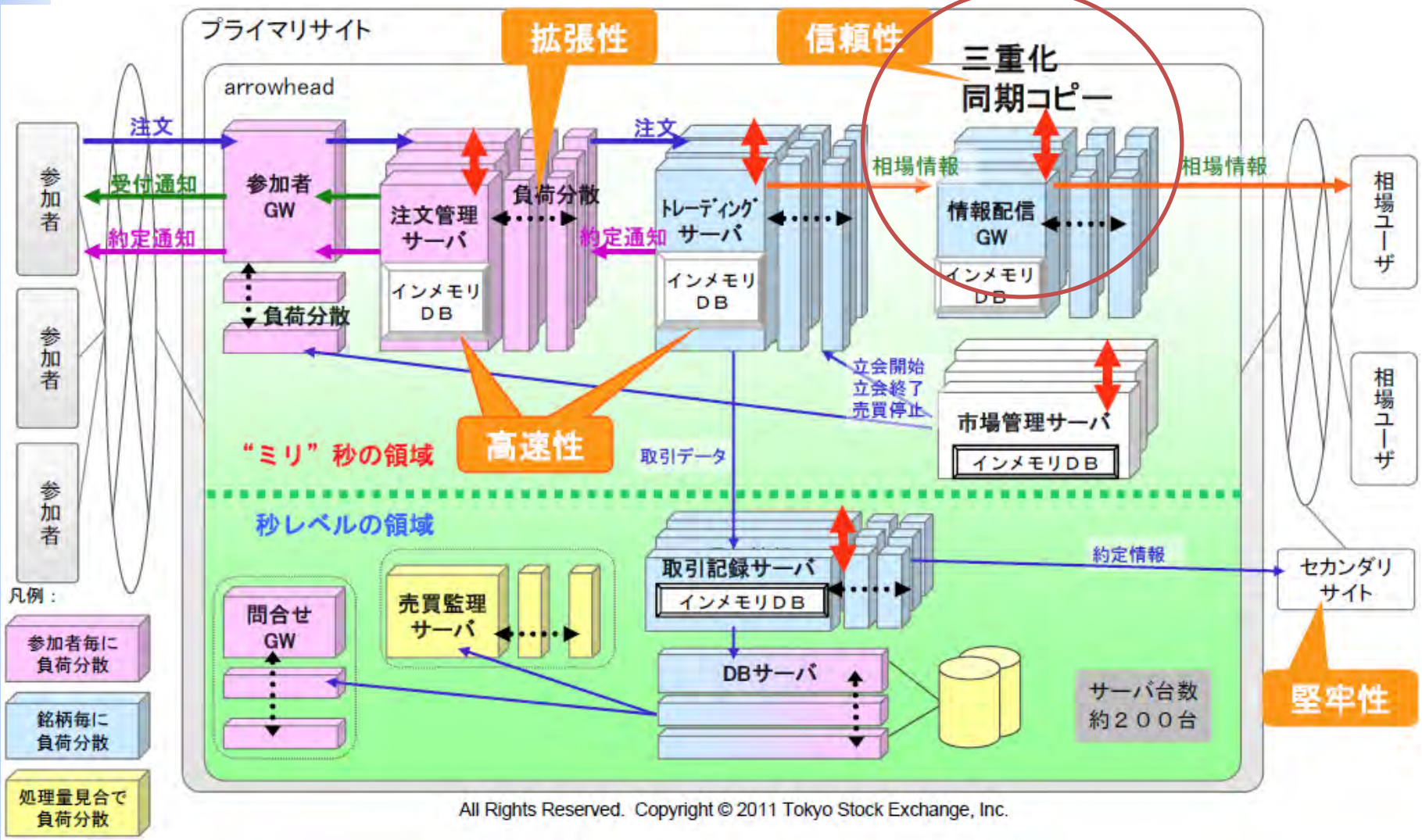
- ◆ （1）T証が策定・報告した各種対応策について、その実効性を確保するため、社外の専門家による検証を受けること。
- ◆ （2）社外の専門家による検証を経た対応策を迅速かつ確実に実施すること。
- ◆ 上記（1）及び（2）について、定期的にその状況を報告すること。

➢ 再発防止策の概要

- ◆ 未然防止の観点での施策（業務継続の観点から万一の場合を想定）
  - » デリバティブ市場、現物市場及びToSTNeT市場の注文等のデータの流れをもとに、システム障害時に取引停止につながる可能性の観点から全サーバ及びネットワーク機器の洗出し、切替えの仕組みや設計値の妥当性等を確認する（業務継続の視点）
  - » 万が一、切替えが正常に機能しない場合の対策等について確認を行い、当該総点検を踏まえた改善施策の検討・対応の実施計画を策定する（万一を想定）
  - » 市販品の選定基準を策定する。
- ◆ 障害発生時の業務影響を極小化するための施策
  - » 障害発生時の初動体制の整備や障害テスト等を通じた担当者の教育及び訓練を行う。
  - » システム障害が発生した場合でも、復旧作業を更に短縮し業務影響を極小化するため、障害発生時に対外影響のある、デリバティブ売買システム、株式売買システム、ToSTNeTシステム（現物立会外取引システム）、相場報道システム、指数統計算出エンジン、清算システム及びTDnet（適時開示情報伝達システム）の7システムを対象に障害時運用プロセスの再点検を実施する。

1. 障害の概要 （参考：株式売買システムの概要）

●1回目（2月2日）に障害が発生した情報配信ゲートウェイシステム（三重化による高信頼化）
（なお、2回目のシステム障害は、本システム図には含まない）



All Rights Reserved. Copyright © 2011 Tokyo Stock Exchange, Inc.

出典：ET2011講演資料より（「T証売買システム(arrowhead)のディペンダビリティ実現のための方式および機能」）

2. 障害の分析

- 2度のシステム障害とも、サーバ、ルータの違いはあるものの、冗長構成での予備系への切り替え時の障害に起因するものであった。両障害とも、障害時の対応に課題があったと考えられる。

（1）冗長構成でのハードウェアの信頼性への過信（1回目の反省点）

- 障害遭遇を回避できるとの認識を前提とした考え方になっていた
- 人間系の役割を明確にしない（必要性を考慮しない）対応となっていた
- そのため、
  - 取引所主体でシステム状態を確認する運用がなされていなかった
  - 深夜・早朝時間帯の十分な監視体制が整備できていなかった
  - 経営陣への障害発生時の報告体制に不備があった

（2）サービスへの影響視点での対策の不備（2回目の反省点）

- システムの障害回避を中心に据えており、サービスへの影響回避の視点が欠けていた
- そのため、切替失敗時の復旧対応が迅速に行われなかった

3. 障害の原因に対応するD-CASE適用のポイント

＜適用にあたっての基本的な考え方＞

- ハードウェア冗長構成での予備系切り替え時の障害においても継続的なサービスが実現できるようなケースを明確化する

原因	D-Case適用ポイント
1. 冗長構成でのハードウェアの信頼性への過信（1回目の障害時） ● 障害遭遇を回避できるとの認識を前提とした考え方になっていた ● 人間系の役割を明確にしない（必要性を考慮しない）対応となっていた ● そのため、 - 取引所主体でシステム状態を確認する運用がなされていなかった - 深夜・早朝時間帯の十分な監視体制が整備できていなかった - 経営陣への障害発生時の報告体制に不備があった 2. 冗長構成時での予備系への切替が行われない場合の対策の不備 ● 1回目の障害対策では、システムの障害回避を中心に据えており、サービスへの影響回避の視点が欠けていた ● そのため、切替失敗時の復旧対応が迅速に行われなかった	1. 体制も含めた運用面の強化として、障害対応時の体制や運用の確認手順と確認項目、復旧手順等を明確化する（1回目の障害後の対応策） ● 訓練の実施 ● 自動切り替え発生時の確認手順、など 2. 業務継続（未然防止策）や障害発生時の業務影響最小化の観点から運用を整備する（2回目の障害後の対応策） ● 影響を最小化する障害時運用プロセスの整備 ● 製品選定基準の整備

4. D-Case適用時の有効性
①初回（2012年2月2日）の障害発生前の高可用性運用のD-Caseで記述

再発防止策の記載内容から、障害前の運用内容を抽出してD-Case形式で記述したもの

Goal: G_1
情報配信ゲートウェイサーバは高可用性である

Context: C_1-1
我が国の証券市場の中心を担う重要なシステムであることから、障害に対するシステムの信頼性を最高度に高める仕組み、施策を講じる

Strategy: S_1
ハードウェアが障害となっても、余裕をもってシステムを動作可能とする。障害後の処置状況は確認する

Goal: G_2
ハードウェアは3重化し、障害ハードウェアは自動診断し、システムが自動で正常ハードウェアに切替える。

Context: C_2
99.999%以上の可用性の確保を目標

Goal: G_4
ハードウェアは3重化する

Goal: G_5
システムは障害診断ツールで障害を監視する

Goal: G_6
システムが障害と確認した場合は、正常系に自動切り替えする

Evidence: E_1
ハードウェアは3重化し、動作は構築時に確認

Monitor: M_1
障害監視ログ

Evidence: E_2
システム構築時の試験は確実にした

下記の部分を点線記述とした意味合い
障害時の運用部門の対応ルールは定まっていたが、本障害時の対応模様から、結果的にD-Caseで重要となる実行可能性のエビデンスの確認が十分でなかったと思われるため。

Goal: G_16
夜間運用ベンダーはシステムが正常に動いているかどうか確認する

Goal: G_21
保守担当はシステムが正常に動いているかどうか確認する

Goal: G_18
運用ベンダーが診断結果を基に、切り替わりを確認する

Goal: G_19
影響が出る恐れがある場合、復旧処理を行う

Goal: G_20
結果を取引所保守担当に報告する

Goal: G_22
運用ベンダーが診断結果を基に、切り替わりを確認する

Goal: G_23
影響が出る恐れがある場合、復旧処理を行う

Goal: G_24
影響が出たら、経営陣に報告する

Monitor: M_18
切り替わりの確認の記録（ログ）

Evidence: E_4
ルールを作成

Evidence: E_5
ルールを作成

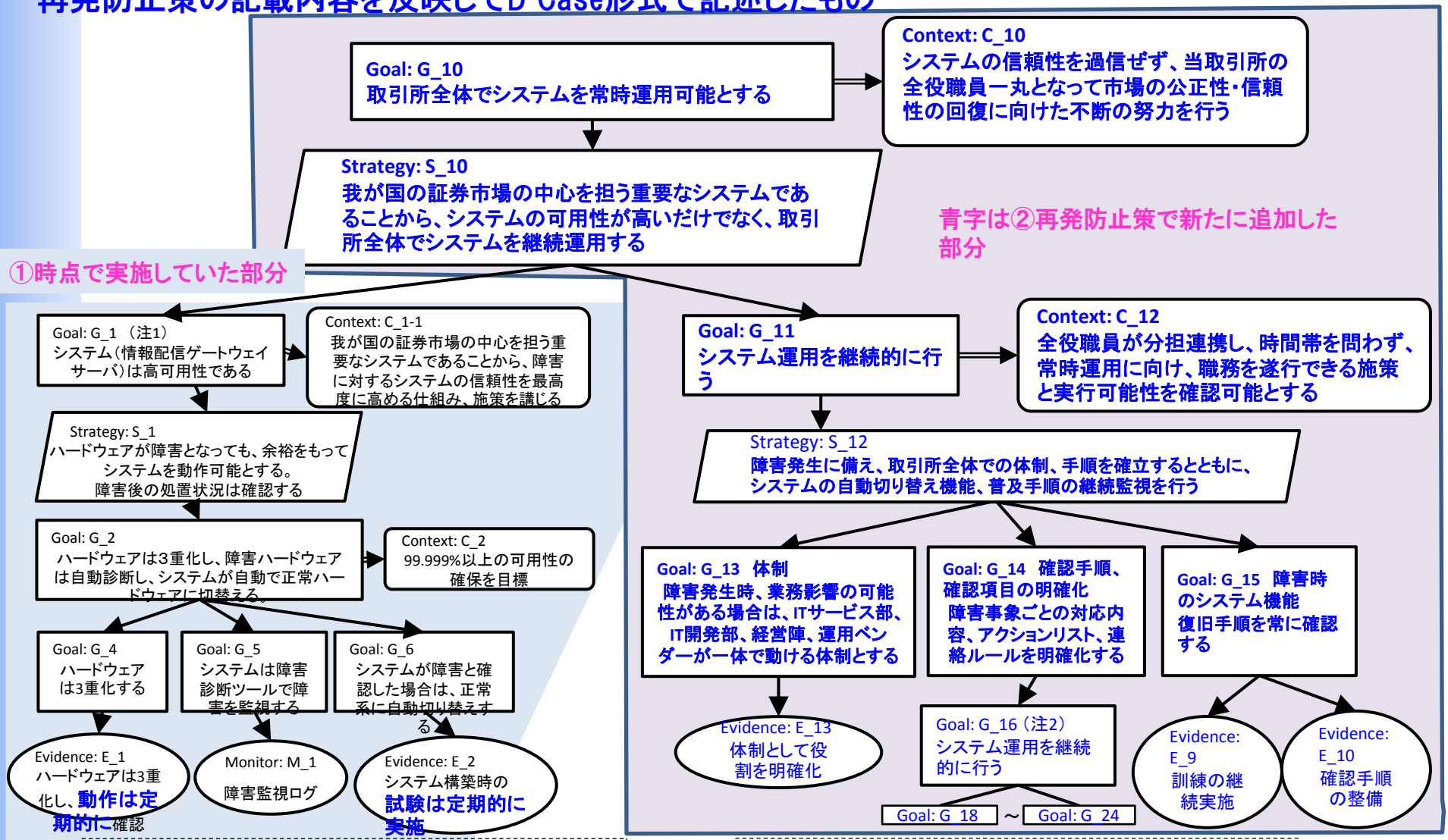
Monitor: M_6
切り替わりの確認の記録（ログ）

Evidence: E_7
ルールを作成

Evidence: E_8
ルールを作成

4. D-Case適用時の有効性
②初回（2012年2月2日）の障害発生後　防止策の常時運用のD-Caseで記述

再発防止策の記載内容を反映してD-Case形式で記述したもの

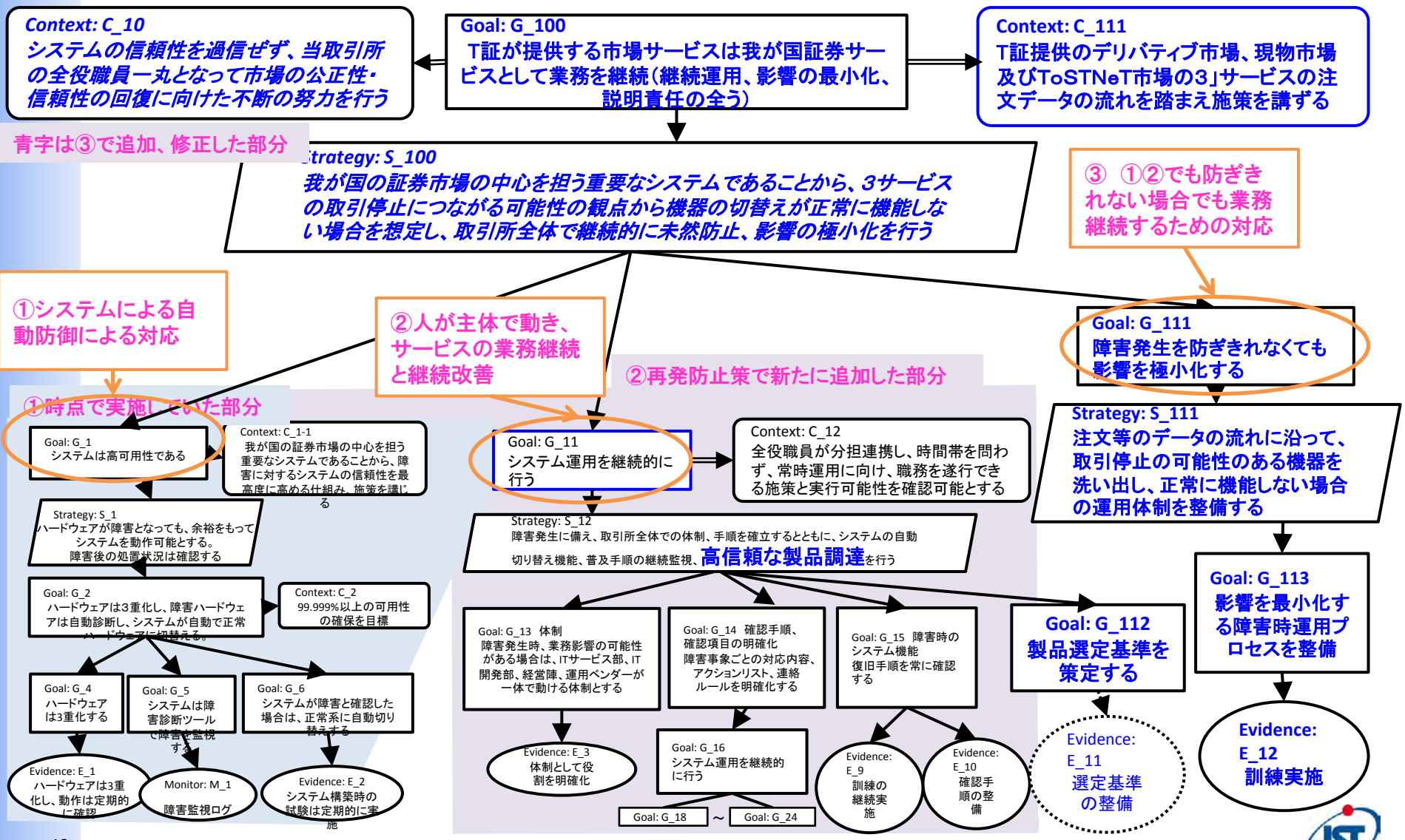


（注1）トップゴール（取引所全体でシステムを常時運用可能とする）を置くことにより、本ゴールをシステムの高可用性に拡張する

（注2）前頁の高可用性運用のD-CaseのGoal番号 G_16～G_24は、本ゴールと本ゴール以下のサブゴールとして記述される

4. D-Case適用時の有効性
③2012年8月7日の障害発生後の防止策　業務継続運用のD-Caseで記述

2012年8月7日の再発防止策の記載内容を反映してD-Case形式で記述したもの

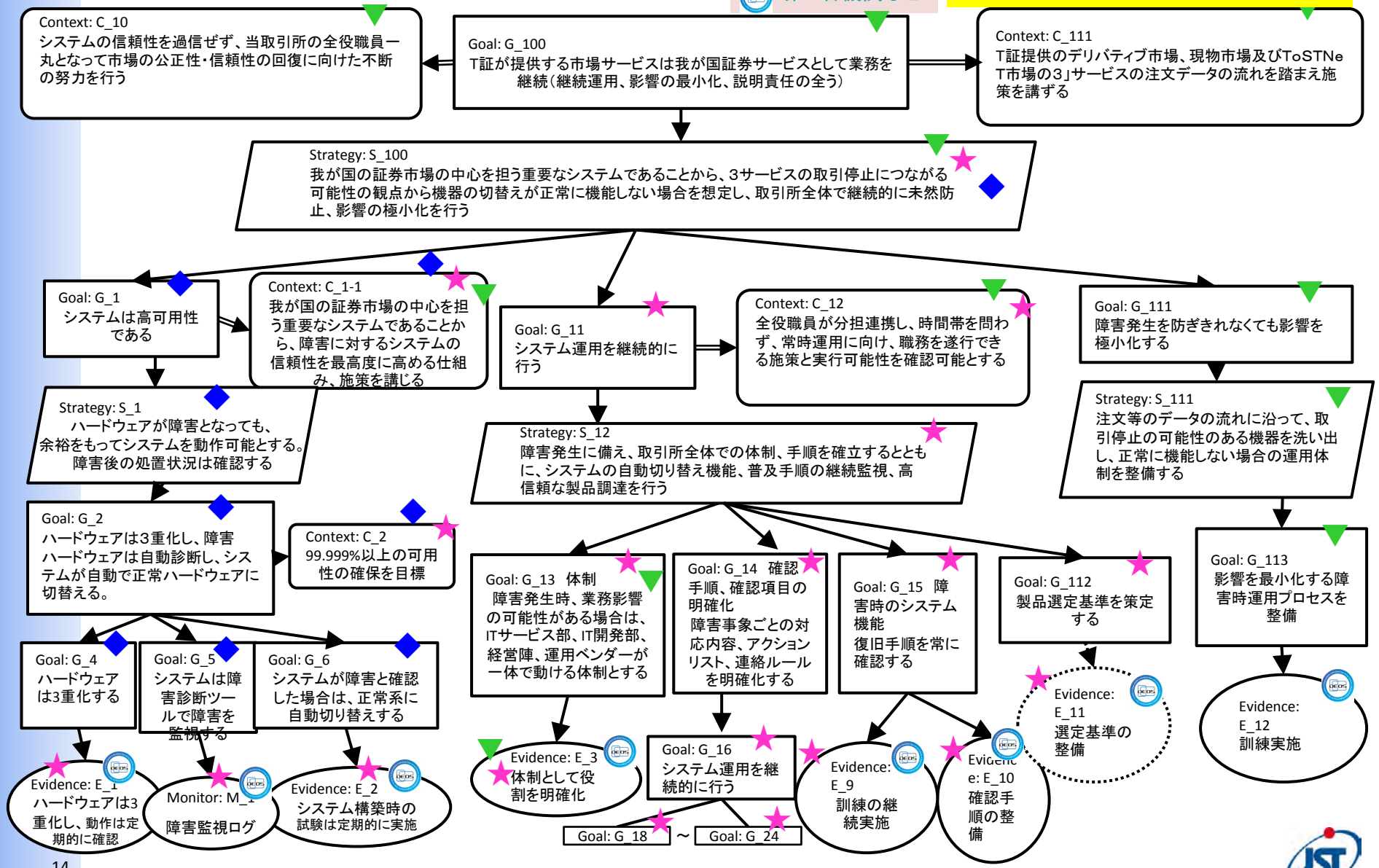


4. D-Case適用時の有効性

④運用対応（D-Caseで記述）

主管部門
▼：経営層
◆：IT開発部門
★：ITサービス部門
：第3者機関など

システム関係は開発部、
運用関係はサービス部門、
社会に対する責任の全う経営層が掌握する。
実行可能性の検証は、第3者機関などを想定した。



5. D-Case適用時のまとめ

再発防止策から段階的に
D-Caseを適用することにより

- 業務継続・影響最小化の実現： ハードウェアの高信頼化だけでなく、業務継続性や障害時での影響最小化を目指すケースを可視化できる
  - （適用事例での例）「システム運用を継続的に行う」、「障害発生を防ぎきれなくても影響を極小化する」場合のケース（ゴール）を追加
- 役割分担の明確化： D-Caseで記述された各ゴールの責任部署を明確化できる
  - （適用事例での例） 経営層、IT開発部門、ITサービス部門、第3者機関などの役割
- 運用の実行可能性の検証： 体制や復旧手順などの手順確認や訓練結果などをエビデンスとして確認・検証できる
  - （適用事例での例）「体制としての役割の明確化」、「訓練の継続実施」等のエビデンス

その結果

- **業務継続のためのすべてのゴールや各組織の役割を一つのD-Caseドキュメントで表すことができる**

5. D-Case適用時のまとめ

今回の事例分析からのD-Case記述・運用に関する気づき

- **気づき1**
  - 従来： 運用中に遭遇する出来事を抽出するモニターと、モニター結果に基づく判断、処置を行うアクションのセットで記述することを意識していた
  - 本事例： 再発防止策に対する新たな対策を実装する記述を追加することとした。これに伴い、モニター・アクションに加えゴールを記述するケースが出てきた。
- **気づき2**
  - 従来： 最終ゴールには運用中に必要な記述のみが書かれていたため、運用者は、D-Case記述を全て用いることで煩雑な部分はなかった
  - 本事例： D-Case記述に新たな実装記述が追加となり、運用時には必要ない記述が入ることとなる。煩雑さを避ける表記法が必要と考えられる。（記述例を4.④に示す。）