ソフトウェア品質シンポジウム2018

FUJITSU
shaping tomorrow with you

マルチベンダー構成システムの信頼性向上を目的としたフェールセーフ設計に対する点検手法
～HAZOPを活用した例外事象を含む応答のモデル化～

2018年9月13日

富士通株式会社
品質保証本部　ソリューション品質推進統括部
発表　相澤 孝一
共同執筆　杉下 雄一、内藤 久志

目次

- 背景
  - システムのマルチベンダー化
  - 想定外事象でのトラブル
- 課題と対処方法
  - フェールセーフ設計に対する点検手法の確立
  - 適用効果
- 結論
  - 新手法まとめ
  - 今後の展開

FUJITSU

背景

背景　システムのマルチベンダー化

FUJITSU

社会的影響の大きいITシステムでも、最適な製品の組み合わせによるシステム構成が主流

☞　特定ベンダー依存からマルチベンダー化

利点：

要件に適合した製品を柔軟に選定可能

－ 機能面、コスト面、普及具合　等

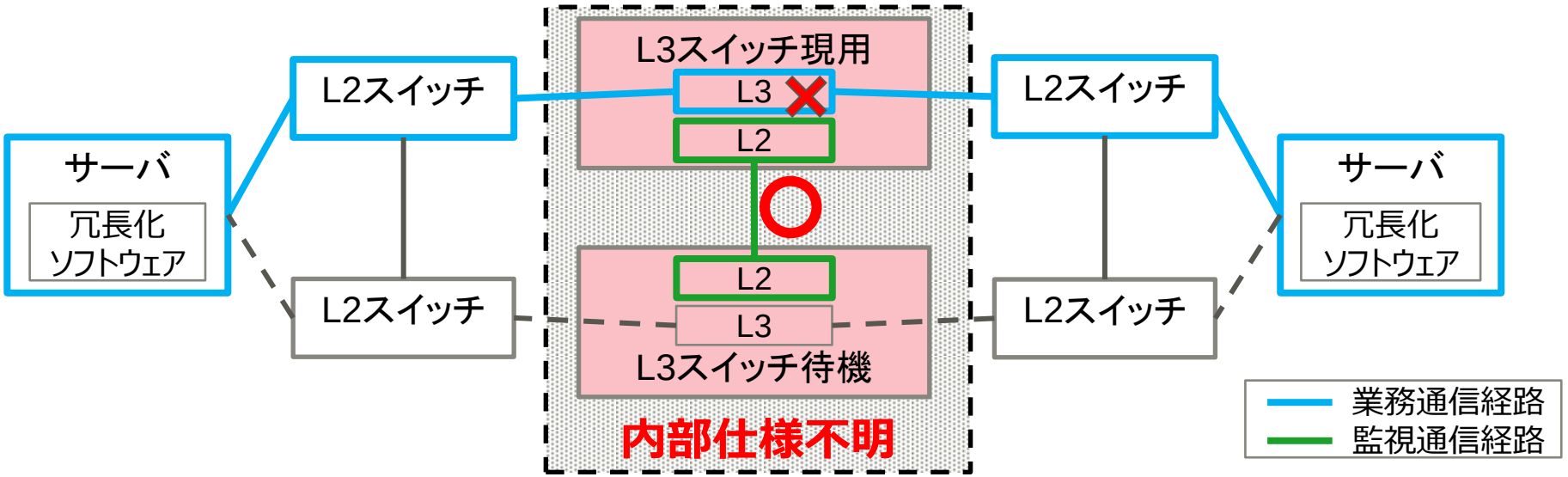
欠点：

製品の想定外事象でのトラブル発生リスクが高まる

製品の想定外事象により業務継続ができず
社会的影響が発生するリスクが有る
（事例を見ていきます）

背景　想定外事象でのトラブル事例

事例：冗長化されたL3スイッチの部品故障で切替え発生できず
サーバ間通信不可
原因：L3層の部品故障を、L2層の部品を使用した現用待機間の
生存監視では異常応答しない仕様で、切り替えできない

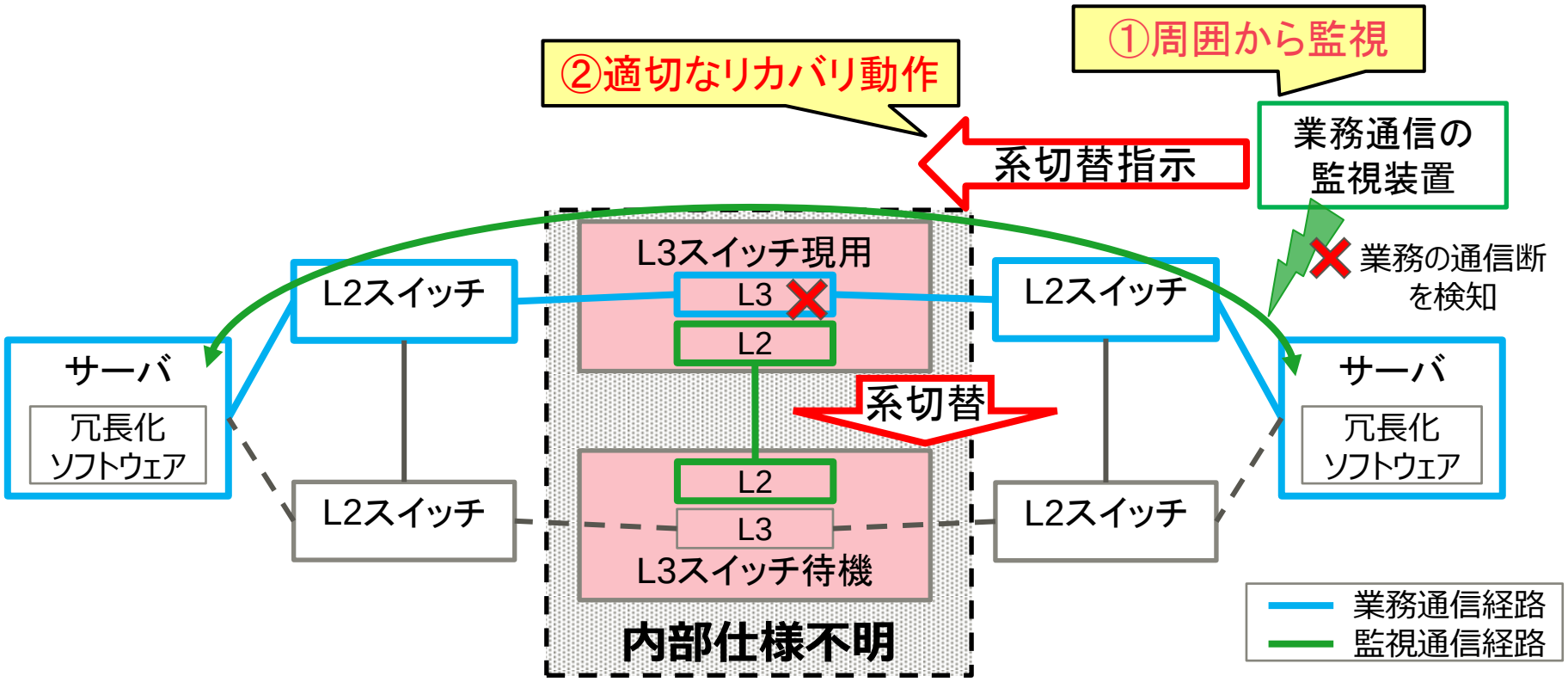


内部：　L2層とL3層が
仕様：　別ハードウェア部品で制御

背景　想定外事象でのトラブルへの対処

FUJITSU

社会的影響の大きいシステムでは、どの様な対処が必要だったのか



① 製品の周囲から監視する機構を実装し、常時監視
② 異常を検出した場合に適切なリカバリ動作をシステムとして実現

背景　想定外トラブルへの備え

FUJITSU

マルチベンダー化システムの欠点：
　製品の想定外事象でのトラブル発生リスクが高まる

欠点を排除するには
システム全体で『想定外トラブルへの備え』が必要

『想定外トラブルへの備え』の妥当性を
検証する手法の確立が必要

FUJITSU

課題と対処方法

課題

FUJITSU

課題：『想定外のトラブルへの備え』の妥当性を検証する手法の確立

検証手法		特定ベンダー依存	マルチベンダー化
ブラックボックステスト	外部仕様書により利用者・運用者向け機能を確認	①外部仕様に基づいた、故障検知と故障処理プロセスの確認	同左
ホワイトボックステスト	内部仕様書により故障モードと故障処理プロセスを網羅的に確認	①製品内部の故障モードを把握 ②故障処理プロセスをシーケンス化（FMEA）	検証不可 （内部仕様（特にRAS仕様）が未公開のため）

マルチベンダー化システムではホワイトボックステストが不可

☞故障モードに対する処理プロセス確認の網羅性が不足

課題への対処

FUJITSU

課題：『想定外のトラブルへの備え』の妥当性を検証する手法の確立

検証手法		特定ベンダー依存	マルチベンダー化
ブラックボックステスト	外部仕様書により利用者・運用者向け機能を確認	①外部仕様に基づいた、故障検知と故障処理プロセスの確認	同左
ホワイトボクステスト	内部仕様書により故障モードと故障処理プロセスを網羅的に確認	①製品内部の故障モードを把握 ②故障処理プロセスをシーケンス化（FMEA）	①製品の故障が業務処理に返す応答をモデル化 ②故障応答に対する処理プロセスをシーケンス化

マルチベンダー化システムでも故障に対する処理プロセス確認の網羅性を確保するために・・・

製品の故障が業務処理に返す応答をモデル化

施策　応答のモデル化１

FUJITSU

①製品の故障が業務処理に返す応答をモデル化

故障発生時の製品の異常状態をグルーピングし、応答をモデル化

自社開発システムの点検より
蓄積した障害情報　661件

故障によって起こる
製品の異常状態　13種類

×

応答は、時間・情報の違いにより
業務への影響が変化

影響種別	ガイドワード	
時間	即応答	要件値以内
	要件値	要件値オーバー
情報の量	情報無し	情報量不足
	情報量適切	情報量過剰
情報の質	正常情報	誤情報

異常状態とガイドワードの組合せにより応答をモデル化！

施策　応答のモデル化２

FUJITSU

①製品の故障が業務処理に返す応答をモデル化

モデル化の手法としてHAZOPを選択

☞ **１つの異常状態に対して複数の影響種別（ガイドワード）を掛け合わせることが可能な手法**

異常状態	ガイドワード			モデル化した応答
	時間	情報の量	情報の質	
異常状態①	即応答	情報量適切	正常情報	応答A
異常状態②	要件値	情報量適切	誤情報	応答B
	要件値オーバー	情報無し	正常情報	応答C
・・・	・・・	・・・	・・・	・・・
異常状態⑬	・・・	・・・	・・・	応答XX

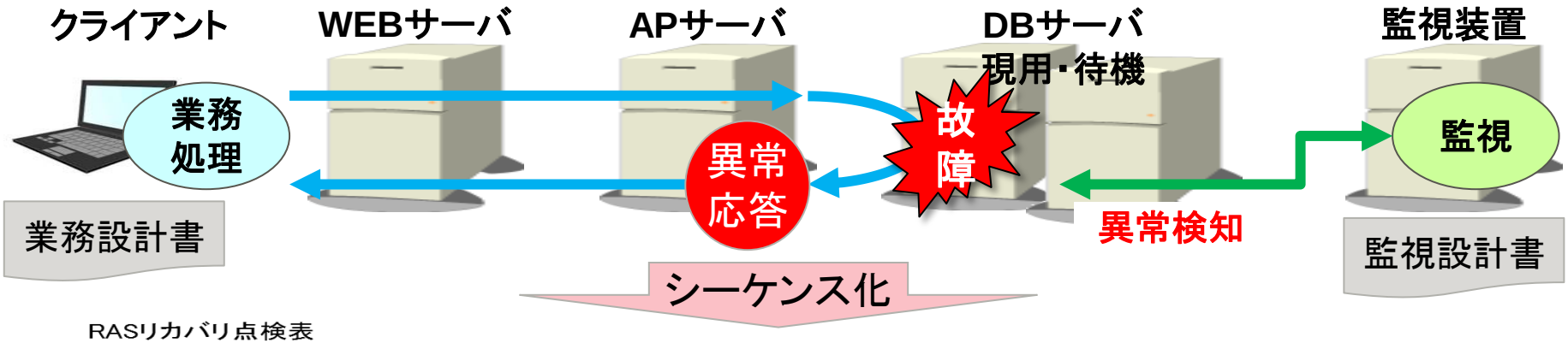
さらに、故障がシステムの業務処理にどのように影響を及ぼし応答するかの観点でグルーピング

製品の故障モードを「１２種の応答事象」でモデル化

施策　シーケンス化

②故障応答に対する処理プロセスをシーケンス化

モデル化した応答に対してリカバリ設計されているかを可視化



RASリカバリ点検表

業務	Input元	Input先（異常発生元）	モデル化した応答	端末	WEBサーバ			APサーバ				DBサーバ			DB待機		ストレージ		監視装置		点検結果
					OS	MW		OS	MW		APL	OS	MW		MW		HW		OS	MW	
					Linux	業務	監視	Linux	業務	監視		Linux	DB	監視	DB		DB領域	バックアップ領域	Linux	監視	
				業務画面	7.2	–	3.2	7.2	–	3.2	業務アプリ	7.2	–	3.2	–				7.2	3.2	QA/リスク内容
					–	–	Agent	–	–	Agent		–	DB	冗長化 Agent	DB	冗長化			–	Manager	
業務処理A	APサーバ	DBサーバ	応答A		□	□		□	□		□	×									異常により応答Aが返ってきたときのリカバリ設計を可視化し、設計不足、漏れをリスクとして抽出 ↓ 対処案を提示

応答A発生

アプリでのリカバリ設計確認

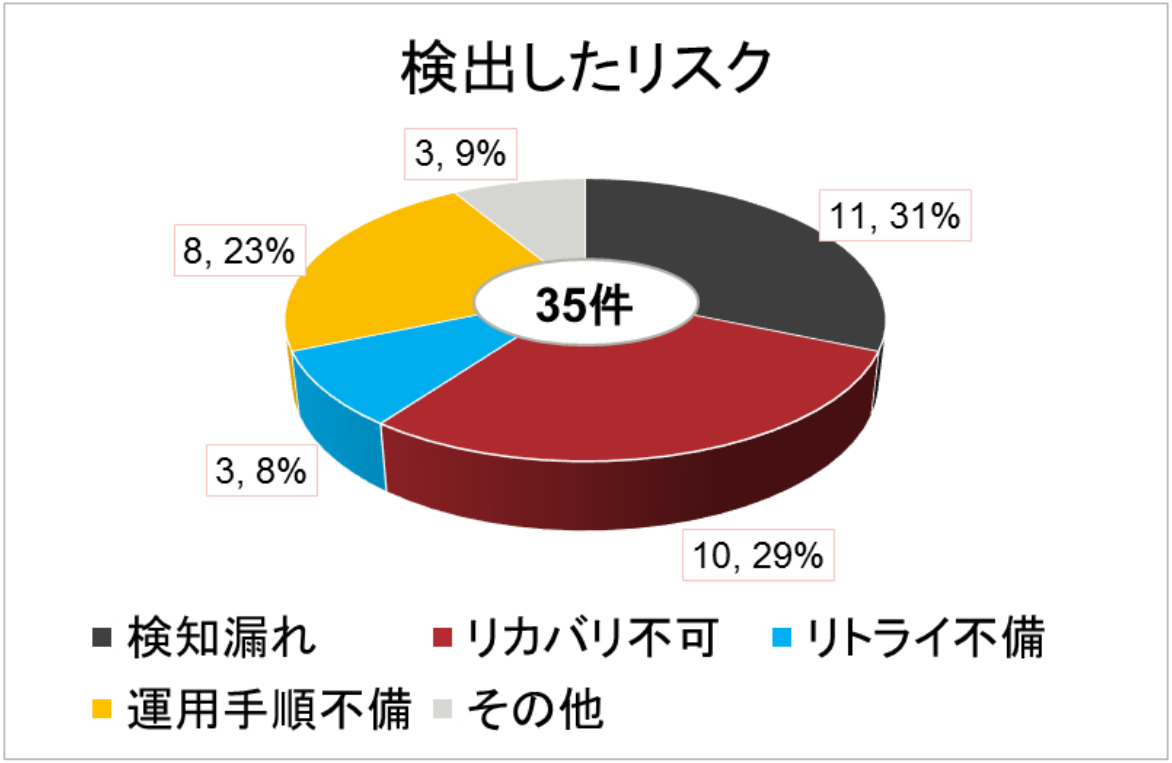
【点検図凡例】 ×：異常発生箇所、□：経由する機器、○：検知箇所、★：リカバリ箇所、点線：リカバリ・異常通知ルート、実線：業務ルート

『想定外トラブルへの備え』の妥当性を検証する手法（フェールセーフ設計に対する点検手法）を確立！

施策適用効果

FUJITSU

２０１７年度
マルチベンダー構成の１０システムを対象に点検を実施し、
３５件のリスク（想定外トラブルへの備えの不備）を検出

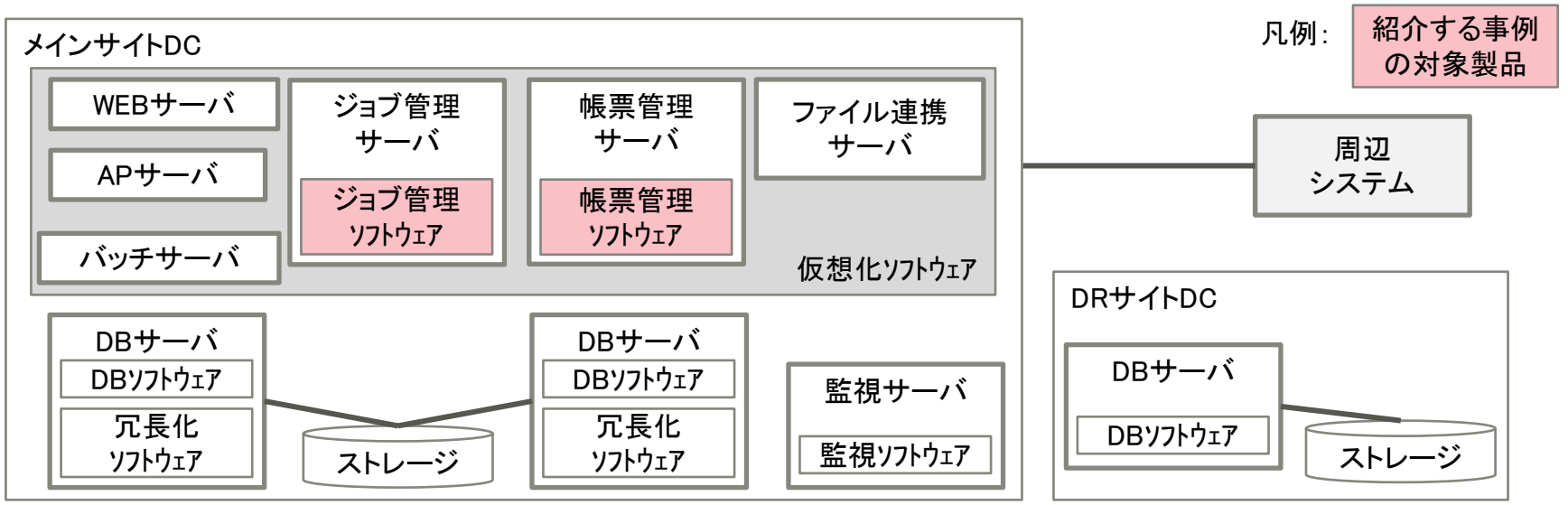


✓ 稼働前にリスクヘッジを図り、システムトラブル発生回避へ

検出障害事例　概要

FUJITSU

金融系基幹システムに対して、フェールセーフ点検を実施

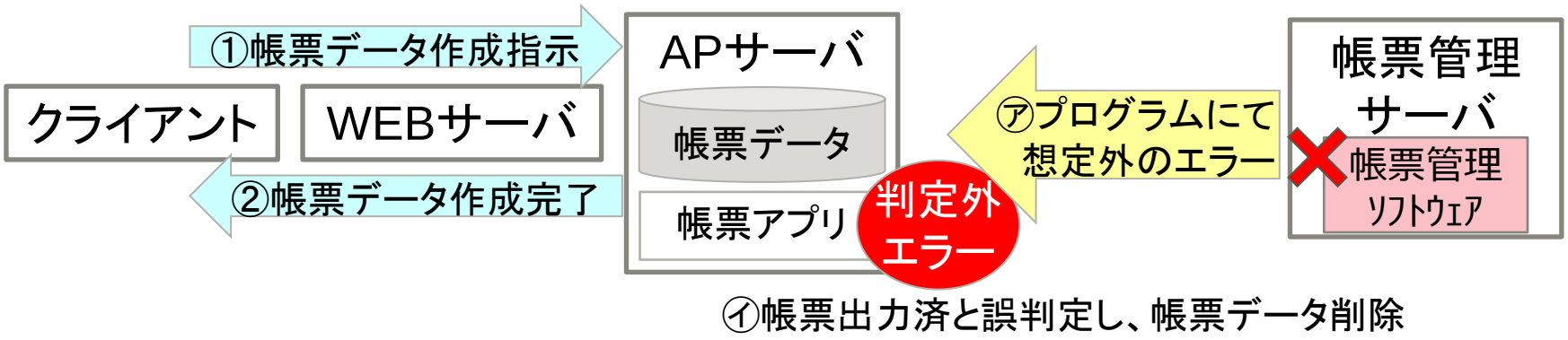


- 主な点検対象製品　：DBソフトウェア、帳票管理ソフトウェア、ジョブ管理ソフトウェア、監視ソフトウェア
- 対象とした主要業務　：オンライン業務、バッチ処理、帳票出力処理など7業務を選定
- 点検項目数　：主要7業務に対し12種の応答事象を適用し、128項目を可視化

✓ システムダウンに至る重要なリスク：2件を検出
✓ 稼働前にリスクヘッジを図り、業務影響を最小化へ

検出障害事例１

帳票出力業務処理中に帳票管理サーバの異常発生時、
帳票データ消失のリスク有り



- 応答事象　　：プログラムにて例外となるエラー応答を受信
- 対象の製品　：帳票管理ソフトウェア
- リスクの原因　：例外発生時のリカバリ設計が未実施。
  帳票出力完了と誤判定され、帳票データが消失する影響あり。

提案したリスクヘッジ方法（リカバリ動作の実装）
- **APサーバにて帳票出力処理のステータス監視を実施**
- **監視結果をもとに帳票アプリ上で帳票処理の完了を判定**

検出障害事例２

バッチ業務処理中にバッチサーバのジョブ管理にて異常発生時、
異常検知が遅れ、翌日の業務運用に影響を及ぼすリスク有り

- 応答事象　　：業務通信のみタイムアウト
- 対象製品　　：ジョブ管理ソフトウェア
- リスクの原因　：バッチ処理の手動実行時に対するタイムアウト設計が未実施。
  バッチ未完了のままとなり、翌日のオンライン業務に影響あり。

提案したリスクヘッジ方法（周囲から監視する機構の実装）

- **監視サーバよりバッチ処理時間の監視を実施**
- **異常検知時には、手動にてバッチサーバを切り離す運用を整備**

ＳＥの声

FUJITSU

システム担当者（SE）からの意見

○　評価できる点

- ☞ **点検の結果を通して**フェールセーフな設計の考えが**必要なポイントがわかり、システム品質が向上した**
- ☞ **過去に稼働中システムでも、点検で**検出されたリスクに**合致する障害も出ていて、点検の有効性を感じた**

×　改善を必要とする点

- ☞ **お客様の要望でIoT機器やクラウド基盤の利用も増加しているので、点検で対応していってほしい**

FUJITSU

結論

新手法まとめ

FUJITSU

新手法まとめ

マルチベンダー化した社会的に影響の大きいシステムにおいて、製品の内部仕様が不明確な場合でも、製品故障が業務処理に返す応答をモデル化する事で、特定ベンダー依存システムと同等な信頼性を向上させる点検を実現した

波及効果

- ✓ 内部仕様に依存しない点検を可能としたことで、特定ベンダー依存システムでも活用できる
- ✓ 業務応答に着眼した点検としたことで、アプリ、運用まで含めた、リカバリ設計全体の点検を実現

今後の展開

FUJITSU

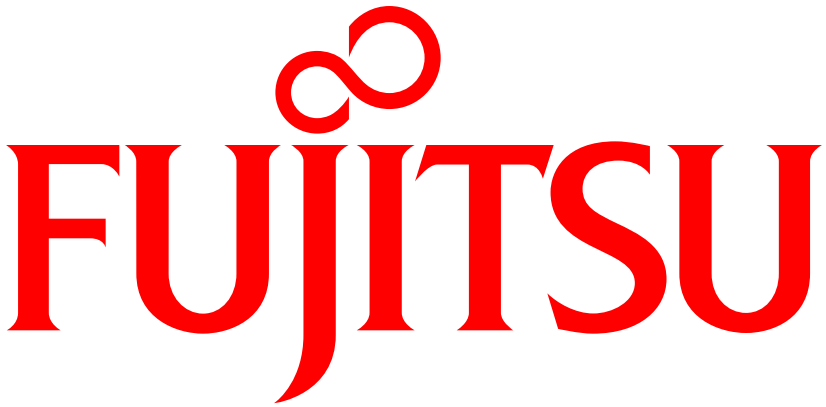
今後の展開

近年のシステムでは、ミッションクリティカルな領域だけではなく、
IoTや他社クラウドの使用も増加

☞ これらに対応可能なよう点検範囲の拡大を図るため、
点検手法のさらなる改善を続ける

見えてきた課題

- 業務の種類が多いと点検項目が膨大になる
  - ☞ 点検対象とする業務を絞り込む技術・理論の開発
- IoTシステムなど中・小規模システムへの対象の拡大
  - ☞ 点検依頼の増加に対応するための効率化の実現
  - ☞ システムレベルに合った点検手法の改革



shaping tomorrow with you