2008－EVA－27 (2)
2008／12／1

CFIAを拡張した障害対策の検討方式の評価

佐藤 雅之† 大塚 亮†

あらまし CFIA(Component Failure Impact Analysis)は、障害対策の検討に用いられる。しかし、CFIAは、障害対策の範囲や、構成要素の分解能(サーバや、CPUやメモリといったデバイス、それらを構成する素子など)を適切に決定できないという課題があった。これらの課題を解決するために、障害履歴を活用した障害対策の検討方式として考案したAdvanced-CFIAについて、事例を用いてCFIAと比較評価を行った結果について報告する。

The Evaluation of a method of analyzing system failure with Advanced-CFIA

MASAYUKI SATO† RYO OTSUKA†

Abstract CFIA(Component Failure Impact Analysis) is used for analyzing system failure. But there is the issue that it's hard to determine the range of analyzing system failure and the range of classifying systems. We report about Advanced-CFIA which we devised as an examination method of the measure for troubles of system failure that utilized a system fault history, compared to CFIA.

1. はじめに

一般に、システムの障害対策は、CFIA(Component Failure Impact Analysis)を用いて検討される。CFIAは、システムの構成要素(S/W、H/W、N/W)の障害を想定し、障害が業務に与える影響の程度、大きさを評価し、障害の影響を最小化するための解決策の作成、改善を行い、システムの可用性の向上を図る手法である。しかし、CFIAは、実際にシステムを構築する上で、検討範囲が適正であるか、およびシステムの構成要素の分解能(例えば、ディスク装置として、複数のHDDを集約した装置一つを最小の構成要素とする、あるいは、ディスク装置をHDDごとに分割して、個々のデバイスを最小の構成要素とするなど)が十分であるかどうかが分からない、という課題を持つ。

Advanced-CFIAは、CFIAに対して、新たに障害履歴を入力に加えることで、課題の解決を試みる手法である。

本報告では、Advanced-CFIAについて、障害履歴例を用いて有効性の検証について示す。有効性の検証の方法は、CFIAとAdvanced-CFIAを用いて、システム例に対する障害対策を導き出し、障害履歴例に記載される障害が発生した場合に、障害を解決するかどうかに関する比較評価による。この結果、Advanced-CFIA技法による解決範囲が広いことを求めた。

2. CFIA

CFIAは、次のように実施する手法である。

- システムの構成要素(S/W,H/W,N/W)の障害を事前に想定する。
- 障害が業務に与える影響の程度、大きさ

† 三菱電機株式会社 情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation.

を評価する。
- 障害の影響を最小化するための解決策を作成する。
- システムの可用性の向上を図る

CFIA を図１のシステム例に適用する。システム例の動作は、次の通りである。

- ユーザは、クライアント１からインターネットを通じて、サーバにアクセスする。
- サーバは、画面表示プロセスにより、ユーザへのインターフェースを提供する。
- サーバは、ユーザ登録プロセスによりユーザ登録を行う。
- サーバは、ユーザ認証プロセスによりユーザ認証を行う。
- サーバは、業務プロセスにより処理を行い、ディスク上の DB に書き込む。
- サーバは、帳票作成プロセスにより、プリンタを通じて、一日の販売実績を帳票に出力する。
- サーバは、バックアッププロセスにより、テープドライブにバックアップを行う。
- サーバは、他システムから専用線を通じて、データを受け取る。
- サーバは、他システムに対し、専用線を通じて、実績データを送る。
- 監視システムは、一定の条件が満たされた場合に、障害通知を運用者に送る。
- 監視システムは、LAN を通じて、サーバなどを監視する。
- サーバは、スイッチにより、インターネット、LAN、専用線に接続する。
- 運用者は、作業指示書に従って、作業を行う。

図１のシステムは、次の運用ポリシに従うものとする。

- サービスを止めるような障害(重障害)となるシステムの構成要素は二重化し、監視システム(S/W 監視、H/W 監視、N/W 監視)により監視する。
- サービスに影響を与えない障害(軽障害)となるシステムの構成要素は修理、あるいは代替を試み、運用者は、障害が発生しているかどうかを確認する。

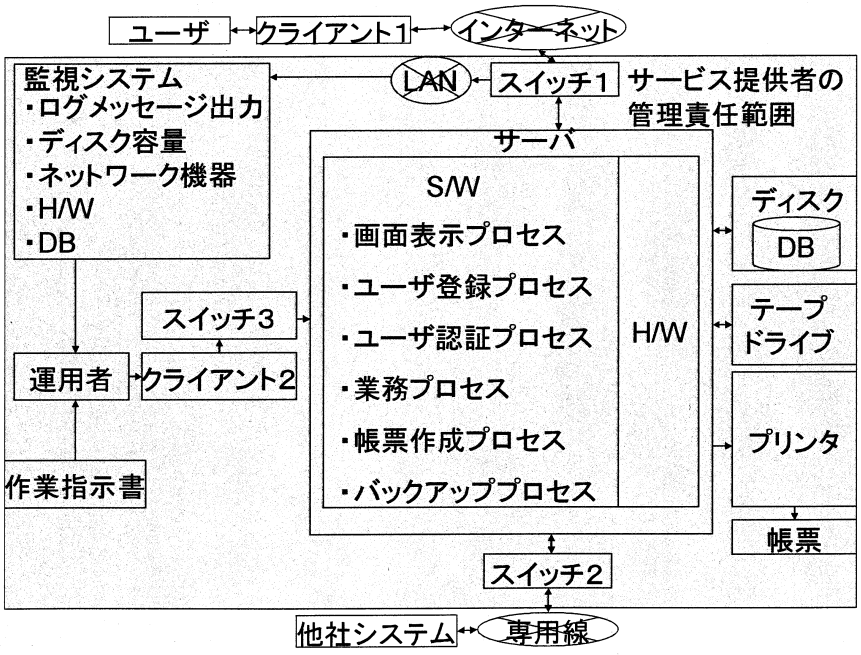

図１　システム例

こうした場合に、次の情報を持つ表１のCFIAマトリクスを作成することができる。

- 構成要素の分類、細分類、名称
- 構成要素の機能停止を意味するダウンなどの障害の種類
- 障害のサービスへの影響(重障害、軽障害)
- 障害を抑止するための対策、あるいは、障害が発生した場合の作業を示す障害対策
- 障害を検出するための障害検出手段

しかし、このCFIAマトリクスを用いて、実際に、システムを構築する上では、次の点が課題となる。

① [検討範囲]CFIA の対象となる検討範囲が適正であるかについては、検証する仕組みがなく、障害対策として不十分になっている可能性がある。

② [分解能]システムの構成要素の分解能(例えば、ディスク装置として、複数のHDD を集約した装置一つを最小の構成要素とする、あるいは、ディスク装置をHDDごとに分割して、個々のデバイスを最小の構成要素とするなど)が、十分かどうかが分からない。

表１　CFIAマトリクス

分類	細分類	構成要素	障害	影響	障害対策	障害検出手段
S/W	アプリケーション	画面表示プロセス	ダウン	X	サーバを二重化する。	S/W監視
		ユーザ登録プロセス	ダウン	X	サーバを二重化する。	S/W監視
		ユーザ認証プロセス	ダウン	X	サーバを二重化する。	S/W監視
		業務プロセス	ダウン	X	サーバを二重化する。	S/W監視
		帳票作成プロセス	ダウン	X	サーバを二重化する。	S/W監視
		バックアッププロセス	ダウン		サーバを二重化する。	運用者がバックアップテープに書き込まれていることを確認する。
	DB	DB	ダウン	X	ディスクをミラー構成にする。	S/W監視
H/W	サーバ	H/W	ダウン	X	サーバを二重化する。	H/W監視
	ディスク	ディスク	ダウン	X	ディスクをミラー構成にする。	H/W監視
	テープドライブ	テープドライブ	ダウン		修理を依頼し、完了後にバックアップを試みる。	運用者がバックアップテープに書き込まれていることを確認する。
	プリンタ	プリンタ	ダウン		修理を依頼し、完了後に印刷を試みる。	運用者が帳票を確認する。
	クライアント	クライアント	ダウン		代替機を用意する。	運用者がクライアントを確認する。
N/W	スイッチ	スイッチ１	ダウン	X	スイッチを二重化する。	N/W監視
		スイッチ２	ダウン	X	スイッチを二重化する。	N/W監視
		スイッチ３	ダウン		スイッチを二重化する。	N/W監視

凡例：X=重障害、空白=軽障害

3. 解決策

課題に対して、次の前提条件に示すように、障害履歴を用いた解決を示す。

① 検討範囲は、CFIA と同様のシステム構成に示される範囲に加えて、障害履歴に記載される障害の原因箇所を範囲とする。

② システムの構成要素の分解能は、CFIA と同様のシステム構成要素に加えて、障害履歴に記録される原因とされる箇所のうち、S/W、H/W、N/W に該当するものを加えたものとする。

なお、ここでいう障害履歴は、検討対象であるシステムが、旧システムから新システムへの移行により導入されるシステムである場合、旧システムに関する障害履歴である。検討対象システムが、新規のシステムである場合、障害履歴は、導入を行う SE が同種のシステム開発を行った際の同種のシステムに関する障害履歴などである。表 2 に例を示す。

障害履歴には、次の情報が記載される。

- どのような不具合であったかを示す現象
- どのように対応したのかを示す対応
- どこに原因があったかを示す原因

他に、障害を検出した人、原因の所在を示す分類、障害の影響程度を示す影響を記載する。

このような前提を導入することで、次のように課題を解決することを仮定する。

① [検討範囲]障害履歴に記載される障害について、解決しうる範囲にまで、CFIA の検討範囲を設定する。すなわち、表 2 のような障害履歴に記載された障害を解決しうる範囲を検討範囲とする。

② [分解能]障害履歴にある障害を解決しうる範囲に、CFIA の分解能を設定する。すなわち、表 2 のような障害履歴に記載された障害を解決しうる程度にまで、分解能を高める。

しかし、障害履歴は、単純にシステムの構成要素に関する障害のみではなく、システムにより解決しえない障害を含む。これらの障害は、CFIA の考え方の中では、対応方法が検討されないが、網羅的に対策を検討する上では、除外できない。

このため、これらの要素についての対策を併せて検討するための技法として、Advanced-CFIA を次のように定義する。

- システムの構成要素(S/W, H/W, N/W)の障害を事前に想定する。
- 障害が業務に与える影響の程度、大きさを評価する。
- 障害履歴を用いて、検討範囲および分解能を設定する。
- 障害の影響を最小化するための解決策を作成する。
- システムの可用性の向上を図る

表 2　障害履歴例

検出者	現象	対応	原因	原因箇所分類	レベル
運用者	ディスクフルになった	スケジューラの再実行	業務プロセスにバグがあり、ログファイルのローテートが実施ざれなかった。	S/W(業務プロセス)	軽
S/W 監視	運用手順中の異常認識	運用者画面が出力されない	ディスプレイ故障	H/W	軽
…	…	…	…	…	…
S/W 監視	業務プロセスのタイムアウト	業務プロセスの再実行	サーバ上のデータ増大により、業務処理も遅延したためタイムアウトになった。	S/W(業務プロセス)	重

4. Advanced-CFIA

Advanced-CFIA のプロセスは、次の通りである(図 2)。

① 検討…CFIA により、障害対策および障害検出手段を検討する。

② 検証…障害履歴に記載される障害が、検討対象のシステムでも発生することを仮定し、その場合にも、検討ステップで決定した障害対応手段により障害が検出できるか、障害対策が有効かを検証する。

③ 修正…検証ステップにおいて、障害検出ができなかった、あるいは障害対策が適当ではなかった場合に、障害検出手段やコンポーネント、パーツ分割を見直す。1～3 の繰り返し適用により、検討範囲と分解能について、検証、修正が行われた Advanced-CFIA マトリクスを作成する。

④ Advanced-CFIA マトリクスでは解決しない障害の対策…運用方法の改善などによる障害の対策を行う。

修正の結果から、検討に戻ることを繰り返し、障害対応手段を得る。

5. Advanced-CFIA の評価

Advanced-CFIA の有効性について、事例を用いて評価を行う。評価方法は、障害履歴例を用い、解決する障害の割合が多い技法が有効であると評価する。以下では、表 2 の障害履歴例を用いて評価を行う。表 2 の障害履歴例は、あるシステムの障害履歴を参考に次のように作成している。

- システム規模を図 1 のシステム構成例に対応させる。
  - サーバの集約
  - ネットワークの集約
- 同一の障害を集約する。

5.1 CFIA により解決する障害

CFIA により解決する障害の割合を求める。表 2 の障害履歴例と、表 1 の CFIA マトリクスを照らし合わせ、障害対策を行い、障害履歴例に記載される障害のうち、解決する障害件数を求めた。本事例の場合、障害履歴例の 37 件中、9 件(24%)の障害について解決しうることが分かった。

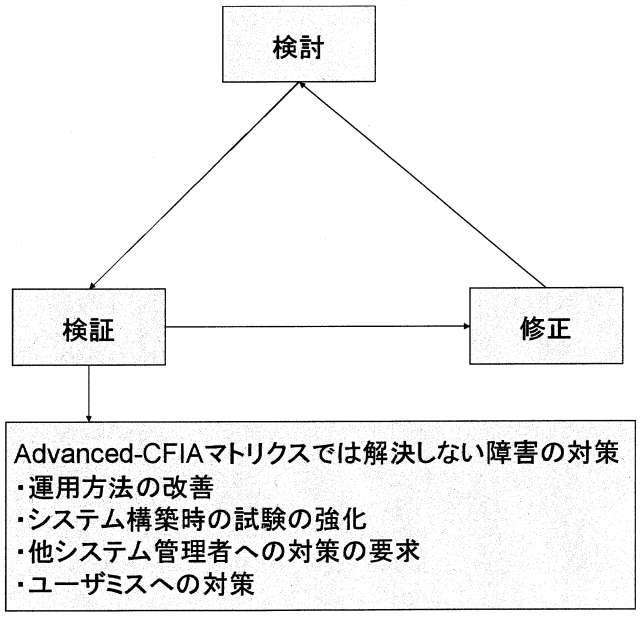

図 2　Advanced-CFIA のプロセス構成

5.2 Advanced-CFIA により解決する障害

まず、Advanced-CFIA のプロセス 1 である検討により、表 1 を得る。さらに、Advanced-CFIA のプロセス 2 およびプロセス 3 を実施することにより、解決する障害件数を求めた。この際に、Advanced-CFIA マトリクス上では、検討範囲の拡大は不要であったが、次の構成要素および構成要素の障害現象について、分解能を高める必要があった。

- 業務プロセスの処理遅延時間
- DB のデータ領域
- DB のエクステント領域
- DB のエクステント回数
- ディスプレイ
- ディスクの容量

結果、本事例の場合、障害履歴例の 37 件中、16 件(43%)の障害について解決しうることが分かった。さらに、プロセス 4 により、障害履歴例上の各障害について、次の方法による解決を検討した。

- 運用方法の改善
- システム構築時の試験の強化
- 他システム管理者への対策の要求
- ユーザミスへの対策

この際に、検討範囲を、ユーザ、クライアント 1、インターネット、他社システム、専用線を含むところまで拡大する必要があった。

5.3 CFIA と Advanced-CFIA の比較

CFIA に関する検討範囲と分解能に関する問題点について、事例により検証を行い、CFIA マトリクスと Advanced-CFIA マトリクスを比較した結果は、次のことを示す。

- Advanced-CFIA マトリクスの方が、障害履歴に記載される障害について、解決する障害の割合が多い。
- Advanced-CFIA マトリクスによる検討範囲は、CFIA マトリクスよりも広い。
- Advanced-CFIA マトリクスによるシステムの構成要素の分解能は、障害履歴に記載される障害について、CFIA マトリクスよりも高く設定される。
- Advanced-CFIA は、障害履歴に記録された障害について、Advanced-CFIA マトリクスを用いる以外に、次の障害対策を検討する方法を持つ。
  - 運用者および作業指示書
  - システム構築時の試験
  - 他システム
  - ユーザ行動

6. おわりに

CFIA は、障害対策の検討手段として、広く用いられる。CFIA は、検討範囲や構成要素の分解能に関し、ノウハウなどを用いて定めている。これに対し、障害履歴を用いて検討範囲や構成要素の分解能を定めて障害への対策方法を検討する Advanced-CFIA を考案し、システム例、障害履歴例を用いた CFIA との比較評価を行い、次の結果を得た。

- Advanced-CFIA は、障害履歴例に記載される障害をより多く解決しうる範囲に、検討範囲を設定し、結果、CFIA よりも多くの障害を解決しうる。
- Advanced-CFIA は、障害履歴例に記載される障害をより多く解決しうる程度に、分解能を設定し、結果、CFIA よりも多くの障害を解決しうる。

以上により、Advanced-CFIA は、障害への対策の検討に有効である、といえる。

Advanced-CFIA の課題は、適用事例が本評価を含め、現時点で、2 例であり、様々なシステムにおいて検証を行っていない点にある。今後は、様々なシステムへの適用を試み、Advanced-CFIA の検証を行う。

参 考 文 献

[1] N.Joshi 他、“Integration of domain-specific IT processes and tools in IBM Service Management”、 IBM Systems Journal vol.15、No.3、 2007.

[2] ソフトウェア品質知識体系ガイド-SQuBOK Guide-, SQuBOK 策定部会, 2007.

[3] 金 翰局,“システム統合における障害発生に対する分析枠組みの提案”, 経営情報学会 2003 年春季全国研究発表大会予稿集, pp. 408-411, 2003.

[4] 日経コンピュータ編集、『動かないコンピューター情報システムに見る失敗の研究』、日経 BP、2003.