医薬品製造にかかわるコンピュータ化システム向けの FMEA を用いた運用リスクマネジメント手法の提案

高橋 正和*・難波 礼治**・福江 義則***

A Proposal of Operational Risk Management Method Using FMEA for Drug Manufacturing Computerized System

Masakazu TAKAHASHI*, Reiji NANBA** and Yoshinori FUKUE***

This paper proposes operational Risk Management (RM) method using Failure Mode and Effects Analysis (FMEA) for drug manufacturing computerized system (DMCS). The quality of drug must not be influenced by failures and operational mistakes of DMCS. To avoid such situation, DMCS has to be conducted enough risk assessment and taken precautions. We propose operational RM method using FMEA for DMCS. To propose the method, we gathered and compared the FMEA results of DMCS, and develop a list that contains failure modes, failures and countermeasures. To apply this list, we can conduct RM in design phase, find failures, and conduct countermeasures efficiently. Additionally, we can find some failures that have not been found yet.

Key Words: risk management, failure mode and effects analysis, computerized system validation, GAMP, GMP

1. はじめに

医薬品は、人間の健康の維持に必要なものとなっている。そのため、適切な品質の医薬品の製造は、医薬品製造会社の責務となっている。近年、医薬品は Drug Manufacturing Computerized System (DMCS) で制御された設備で製造されているため、DMCS の不適切な機能と性能が医薬品の品質に悪影響を与えることが問題となっている。そのため、米国食品医薬局、日本国厚生労働省などの監督機関は、医薬品製造会社に対して、DMCS 開発時に、機能と性能の適切さを、文書または電子データによる証拠で立証することを義務付けた^{1), 2)}。これを Computerized System Validation (CSV) と呼ぶ。CSV 実施基準としては Good Automated Manufacturing Practice (GAMP5)³⁾ が国際標準となっている。

GAMP5 では、DMCS の機能と性能を適切なものとするた

め、開発ライフサイクルの各段階で、リスクアセスメントとリスク低減策を実施すること（これらを併せてリスクマネジメントと呼ぶ）を要求している。その際、Failure Mode and Effects Analysis (FMEA)⁴⁾、Fault Tree Analysis (FTA)⁵⁾、Hazard and Operability Analysis (HAZOP)⁶⁾ などを使用して網羅的かつ科学的な検討を行なうことを推奨している。しかし、具体的な手順が規定されていないため、担当者による差異が生じ、実施が困難となっている。加えて、各段階で実施されるリスクマネジメント結果の連携が困難となっている。

これらの問題を解決するため、DMCS 開発段階で利用可能な FMEA を用いたリスクマネジメント手法を提案する。FMEA を用いる理由は、FMEA は故障モードがシステムに与える影響を網羅的に分析するのに適しているためである。提案手法では、既存 DMCS の FMEA 結果を収集、分析して DMCS に共通に使用可能な故障モード、リスク低減策の一覧表を作成した。これを利用することで、適切なリスクマネジメントを実施できるようにした。

2. リスクマネジメントと FMEA の概要

2.1 DMCS の CSV とリスクマネジメント

Fig. 1 に GAMP5 の CSV 実施手順を示す。計画策定段階では、DMCS の概要を決定し、バリデーション計画を立案する。仕様作成段階では、DMCS の種類や機能の複雑さに応じて、User Requirement Specification (URS)、Functional Specification (FS)、Design Specification (DS)、Configuration Specification (CS)、Module Specification (MS) を作

* 山梨大学大学院医学工学総合研究部 甲府市武田 4-3-11

** 第一工業大学工学部 霧島市国分中央 1-10-2

*** 富士通 (株) 情報・サービス統括営業部
東京都新宿区西新宿 6-5-1 新宿アイランドタワー私書箱 1579

* Graduate School of Medical and Engineering, University of Yamanashi, 4-3-11 Takeda, Kofu

** Faculty of Engineering, Daiichi Institute of Technology, 1-10-2 Kokubuchuo, Kirishima

*** Sales Division, Information Services, Fujitsu Limited, P.O. Box 1579, Shinjuku Island Tower Bldg., 6-5-1 Nishishinjuku, Shinjuku-ku, Tokyo

(Received May 9, 2011)

(Revised February 21, 2012)

Fig. 1 Procedure of computerized system validation

成する^{7),8)}。構成/プログラミング段階では、DMCSの種類に応じて、パラメータ設定、部品構成の決定、プログラムの製作を行なう。検証段階では、DMCSに対して Requirement Test (RT), Functional Test (FT), Integration Test (IT), Configuration Test (CT), Module Test (MT)を行ない、機能と性能が適切であることを立証する。報告段階では、バリデーション結果を報告する。運用段階では、改修が生じた場合、変更と構成の管理を行なう。リタイアメント段階では、DMCSの保持、移行、破棄を決定し、データの保管や引渡しを行なう。

GAMP5で実施されるリスクマネジメント活動を Fig. 1の R1~R7に示す⁹⁾。R1とR2は計画策定段階で実施される。R1では、開発するDMCSがCSV対象になるか判定し影響度を判定する。R2では、サプライヤの評価とDMCSのカテゴリ分類を行なう。ここでカテゴリ1はOSなどの市販ソフトウェア、カテゴリ3はパラメータを与えて使用する市販ソフトウェア、カテゴリ4は構成を設定して使用する市販ソフトウェア、カテゴリ5は個別開発のソフトウェアである(カテゴリ2は存在しない。また、カテゴリ1に該当するDMCSはないので、以降記述しない)。カテゴリの数字が大きいく程、厳密な開発文書の作成と検証の実施が要求される。R3は仕様作成と構成/プログラミングの段階で実施される。仕様作成段階では、はじめにURSの内容にもとづいて、CSV対象機能を絞り込む。二番目に、Fig. 2のリスク評価行列を用いてCSV対象機能の重要性、障害発生確率、検出確率からリスク優先度を求める。三番目に、リスク優先度の高い順番にリスク低減策を検討していく。四番目にリスク低減策を反映させたURSの設計審査を行なう。そして、構成/プログラミング段階では、決定したリスク低減策をDMCSの設計の中に作り込んでいく。R4では、R2とR3の結果をもとに検証の範囲と厳密さを決定する。R5では、変更管理、構成管理などの方法を決定する。R6では、運用に伴う改修に対してR2からR4のリスクマネジメントを実施する。そして、R7では、データの保持、移行などの方法を決定する。

Fig. 2 Determining method of risk priority

2.2 FMEA

はじめにFMEAの定義を述べる。FMEAは適切な機能を有していた機器が、断線・短絡・特性の劣化などにより、機能を失う事象の原因や対策を検討する手法である。このとき、断線、短絡、特性の劣化などの変化のこと(故障状態の形式による分類)を故障モード、機能を失うことを故障と呼ぶ。

二番目にソフトウェアに対するFMEAに関する先行研究について述べる。森田¹⁰⁾は対象ソフトウェアをブロックに分割し、それぞれに故障モードと推定原因を列挙してバグを発見した。丹羽¹¹⁾は対象ソフトウェアの外部設計単位で故障モードを列挙して信頼性向上対策を行なった。高井¹²⁾や山科¹³⁾は大規模ソフトウェアに対して構成要素単位で故障モードを列挙して対策を行ない信頼性を向上させた。これらの方法は、故障モードの抽出が作業者の能力に依存しており、故障モードを漏れなく列挙できるとは限らないため、網羅的な対策を施すことが難しい。Goddard^{14),15)}やSnooke¹⁶⁾はコードレベルのFMEAを提案した。Goddardは命令レベルでの故障モードを定義してFMEAを実施した。Snookeはソフトウェアを等価な回路に変換してFMEAを実施した。これらは、GAMP5で要求される機能レベルのFMEAには適用できない。

三番目に提案するFMEAの方法について述べる。DMCSは制御装置に搭載されて、Standard Operation Procedure (SOP)に則って運用されるので、ハードウェア、ソフトウェア、運用についてFMEAが必要となる。ハードウェアの場合、分析対象を構成要素に分割し、それぞれに故障モードを列挙して、分析対象の故障の検討、対応策の検討を行なう。この方法はすでに確立されているので、本論文では扱わない⁴⁾。ソフトウェアの場合、故障の多くは、テスト段階で除去できなかった誤りが、顕在化したものである。誤りはソフトウェアの変化を伴わないので故障モードではない。誤りは適切な設計とテストにより除去するものであり、故障モードはFMEAで分析・対策をするものである。したがって、本論文で扱うリスクマネジメントでは、誤りは対象外とする。一方、悪意をもつソフトウェアの侵入など、外部の脅威により、ソフトウェアが書き換えられ、正常に動作しなくなる事例が発生している。これらはソフトウェアの変化を伴い、故障モードと考えられるので対象とする。運用については、SOPに則った

作業が実施されていれば、変化は生じない。しかし、SOP や Human Machine Interface (HMI) の見間違い、想定外の運用などにより、DMCS の動作が異常となること、医薬品製造プロセスが不適切となることがある¹⁷⁾。これらは運用の変化を伴い、故障モードと考えられるので対象とする。これらは操作員が DMCS に対して起動、停止、入出力、校正、バックアップなどの操作をする場合、不適格な操作員が操作を行なう場合、不適切な DMCS 使用で想定外の負荷が生じた場合に発生する。

3. DMCS のリスクマネジメント実施上の問題

DMCS のリスクマネジメントの問題を述べる。

問題 1 実施者によるリスクマネジメント結果の差異

実施者の能力により、故障モードの見落としや不適切なリスク低減策の実施などが発生し、DMCS が不安全な状態となる。

問題 2 リスクマネジメントの実施手順と実施内容の不統一

GAMP5 では、リスクマネジメントの具体的な実施手順が明確となっていない。さらに、カテゴリに応じたリスクマネジメントの実施内容も明確でない。

問題 3 リスクマネジメント間での連携の不徹底

GAMP5 では開発の各段階でリスクマネジメント実施が要求されるが、前段階の結果が、後段階に適切に反映されているか不明確である。加えて、リスク低減策と検証との対応関係も不明確である。

4. DMCS のリスクマネジメント手法の提案

4.1 共通故障モードの導出

3 章の問題 1 を解決するために DMCS に共通に使用可能な故障モードを導出する。そのために、20 件の既存 DMCS の FMEA 結果を収集した。ここでは、医薬品の製造現場で用いられる標準的な装置や設備の DMCS を対象とした（品質、調達、生産の計画や管理などを行なう基幹システムは含まない）。収集したカテゴリ 3 の DMCS は遠心分離機、計量システム A、造粒装置、コーティング装置、データ計測装置 A と B である。これらは単純な製造装置の制御やそれにかかわるデータを収集する DMCS である。カテゴリ 4 の DMCS はデータ管理システム A、倉庫搬入出システム A、空調制御システム、監視制御とデータ収集システム A と B、データ収集システム A と B である。これらはやや複雑な制御やそれにかかわるデータの収集と蓄積を行なう DMCS である。カテゴリ 5 の DMCS はデータ管理システム B、倉庫搬入出システム B、計量システム B、医薬品製造プロセス制御システム A～E である。これらは複雑なプロセスの実行や大量なデータを収集・管理・抽出する DMCS である。

FMEA 結果に含まれる故障モードを 2.2 で述べた操作、想定外の負荷、外部の脅威にグループ分けした。Table 1 に結果を示す。そして同じグループの故障モードを分析して、DMCS で共通に使用可能な故障モード (Common Failure

Mode for DMCS: CFMD) と代表的なリスク低減策 (Risk Reduction Measure: TRRM) を導出した。以下にその過程を示す。

はじめに起動操作にかかわる故障モードについて述べる。「制御条件が設定できない」、「制御条件を通信できない」などの故障の内容を調べると、実行順序制約のある前処理が終了していない、優先順位の高い処理が終了していない、機器が所定状態になっていない、データが揃っていないなどが原因であった。したがって、これらを「機能の起動条件が揃わない」CFMD にまとめた。そして、RRM は「開始条件確認作業の SOP への追加」などとした。また、これらの故障は、「SOP を見間違う」、「HMI を見間違う」ことでも生じるので、これらも CFMD とした。そして、RRM は「開始条件を確認する作業の SOP への追加」、「SOP の二重確認」、「HMI の二重確認」などとした。

二番目に停止操作にかかわる故障モードについて述べる。「制御条件が設定できない」、「制御条件を通信できない」などの故障は、起動操作と同様に考え「機能の停止条件が揃わない」、「SOP を見間違う」、「HMI を見間違う」CFMD にまとめた。そして、RRM は「停止条件確認作業の SOP への追加」、「SOP の二重確認」、「HMI の二重確認」、「緊急停止機能の追加」などとした。停止操作にかかわる故障のうち「データを保管できない」、「入力データを設定できない」などは、旧データを新データで上書きしたり、新データを受けつけずに旧データを書き込んだりすることで生じる。これらは「過去のデータを損失する」、「最新のデータを損失する」CFMD にまとめた。そして、RRM は「過去データ損失警告機能の追加」、「最新データ損失警告機能の追加」などとした。

三番目にデータ入出力操作にかかわる故障モードについて述べる。「所定の回転数を逸脱する」、「所定の制御条件を逸脱する」などの原因は「SOP の回転数を見間違う」、「HMI の掻取回転数を見間違う」などであった。これらは、「SOP を見間違う」、「HMI を見間違う」CFMD にまとめた。そして RRM は「再確認機能の追加」、「SOP の書式の統一」、「HMI の表示形式の統一」、「SOP の二重確認」、「HMI の二重確認」などとした。また、これらの故障は誤ったデータを設定したり、ものを間違ったりしても発生する。前者は、「入力を間違う」CFMD にまとめ、RRM は「設定データの二重確認」とした。後者は、「ものを見間違える」CFMD にまとめ、RRM は「ものの二重確認」とした。

四番目に校正操作にかかわる故障モードについて述べる。「間違った時刻が記録される」故障の原因は、時刻の校正を行なう間隔が長く時刻がずれたためである。「測定結果の誤差が大きくなる」故障の原因も、測定機器の校正を行なう間隔が長く精度が悪化したためである。これらは、「校正を行なう間隔が長い」CFMD にまとめた。そして RRM は、「機能の校正を行なう間隔を短くする」などとした。

五番目に操作員の資格確認作業にかかわる故障モードについて述べる。「アクセス権のない作業員が操作をする」、「無資

Table 1 Elicitation of common failure modes: abridgement

System	Function	Failure	Failure mode	Common failure mode	Representative risk reduction measures
Those associated with starting software functions:					
Measurement data management System B	Control conditions setting function	Control conditions cannot be set	The input window for control conditions does not open	Startup conditions are not prepared	Add the confirmation procedure for the startup conditions to the SOP
Automatic warehouse system B	Entering setting function	Entering data cannot be set	The input window for entering data does not open	SOP instructions misread HMI indications misread	Add the setting procedure for the conditions as to whether or not to start Add the function for displaying startup status
Those associated with terminating software functions:					
Measurement data management system B	Control conditions setting	Control conditions cannot be set	The input window for control conditions does not	Termination conditions are not prepared	Add the confirmation procedure for the termination conditions to the SOP
Automatic warehouse system B	Data save function	Data cannot be saved	Writing of data does not terminate	SOP instructions misread HMI indications misread	Add the setting procedure for the conditions as to whether or not to start
Automatic warehouse system B	Entering setting function	Input data cannot be set	Writing of data does not terminate	Past data lost Latest data lost	Add the emergency stop function Double checks on the SOP/HMI
Those associated with data input:					
Centrifugal separator	Acceleration function	Required revolutions deviated	A wrong revolution number entered	SOP instructions misread HMI indications misread Inputting error Mistake in checking products	Add the reconfirmation function
Measurement data management system A	Search conditions setting	Improper search conducted	Search conditions out of the specifications		SOP format integration
Automatic warehouse system A	Entering setting function	Wrong pallet entered	Wrong entering pallet data entered		Double checks on the SOP
Automatic warehouse system B	Entering setting function	Wrong products loaded on the	Wrong product ID		HMI format integration
Automatic warehouse system B	Entering setting function	Products loaded on a wrong pallet	Wrong pallet ID		Double checks on the HMI Double checks on the setting data Double checks on the products
Those associated with calibration:					
Automatic warehouse system A, B	Entering order control function	Wrong time recorded	Long time intervals for time correction	Long time intervals for function calibration	Long time intervals in structuring functions
Measurement system A, B	Measurement function	A significant error in measurement	Long time intervals for scale correction		
Those associated with operator qualifications:					
Measurement data management system A, B	Access control function	Unauthorized operator operates the device	Error in the operator authority	Error in the operator authority	Confirm operation authority before operation Review authority periodically
Measurement system A, B	Measurement amount calculation function	Unqualified operator operates the device	Error in the operator authority		
Those associated with backup:					
Measurement system B	Measurement amount calculation function	Data disappeared	Insufficient backup	Insufficient backup	Organize the backup procedures in the SOP and shorten backup intervals
Those associated with unexpected CPU load					
Automatic warehouse system B	Empty shelf control function	Empty shelves not updated	Empty shelves not updated	High update load	Add the restriction function for available data
	Prohibited shelf control function	Prohibited shelves not updated	Prohibited shelves not updated		Add the number of available data to the SOP
Measurement system B	Instruction reading function	Calculated with a wrong measurement amount	A wrong measurement value entered	Inputting error	Add the reconfirmation function
	Automatic raw-material sampling function	Wrong raw materials sampled	Wrong raw material input	SOP instructions misread HMI indications misread	SOP format integration
	Measurement calculation function	Calculated with a wrong measurement amount	Divided by zero	Improper data range	Double checks on the data/SOP/HMI HMI format integration
				Divided by a small divisor	Add the warning function for a small divisor
All category 5 system	All software functions	Abnormal program shutdown	Unexpected abnormal data processing	Unexpected abnormal data processing	Add the restriction function for available data
			Unexpected multiple interruption tasks occurred	Unexpected multiple interruption tasks occurred	Add the number of available data to the SOP
			Program does not response	CPU overload	CPU overload
Those associated with malicious operations or attacks:					
Entire system	All software functions	Data is brought out	No access control to data	No access control to data	Introduce DLP tools
		Data is falsified	No access control to the system	No access control to the system	Add the user access control function
			Data could be rewritten	Data could be rewritten	Add e-signature and time stamp
		Service rejection attack received	Vast amounts of fraudulent packets received	Vast amounts of fraudulent packets received	Disconnect from the external network or install fire walls
	Illegal access gained	Illegally accessed from the outside	Illegally access from the outside	Disconnect from the external network and	
	Access to a malicious website	Access to a harmful website	Access to a harmful website	Conduct access control to harmful websites	
	Infected with computer virus	Data with virus attached received	Data with virus attached received	Introduce antivirus software and IPS	
	Functions that uses USB	Infected with computer virus	USB with virus contained used	USB with virus contained used	Conduct virus checks on USB memory devices before connecting

格の作業員が作業をする」の原因は、資格確認が不十分なことで生じる。これらは、「作業権限の間違い」CFMDにまとめた。そして、RRMは「作業前の権限確認」、「定期的な権限の見直し」などとした。

六番目にデータのバックアップ操作にかかわる故障モードについて述べる。「操作員情報が消失する」、「データが消失する」の原因は、バックアップ不徹底である。これらは「バックアップの不備」CFMDにまとめた。そして、RRMは「バックアップ手順SOP化」、「バックアップ間隔短期化」などとした。

七番目に想定外の負荷にかかわる故障モードについて述べる。「空き棚数が更新されない」、「禁止棚が更新されない」などの故障の原因は、「想定数以上の更新が要求される」ためである。したがって、これをCFMDとした。そして、RRMは「更新処理の高速化」、「記憶装置の高速化」、「受付データ制限機能の追加」などとした。「誤った計量指図計算をする」、「誤った原材料を採取する」などの原因は、「計量値を間違えて入力する」、「誤った原材料を入力する」、「計量値を読み間違う」、「原材料を読み間違う」、「範囲外の計量値が入力される」、「指定外の原材料が入力される」などである。前の2つは「入力を間違う」、中の2つは「SOPを見間違う」と「HMIを見間違う」、後の2つは「ものを見間違う」CFMDにまとめた。RRMは、それぞれ「設定データの二重確認」、「SOP

の二重確認」と「HMIの二重確認」、「ものの二重確認」とした。それ以外に「誤った計量計算をする」の原因として、「計算範囲上限オーバー」、「計算範囲下限オーバー」、「ゼロ割をする」があり、CFMDとした。RRMは「倍精度型変数の利用」、「除数が小さいときの警告の追加」とした。「プログラムが異常停止する」は、大量のデータを受け取ったために記憶領域を使い切ることや、割り込みが多発してその情報がスタック領域からあふれ出して他のデータの記憶領域を破壊することなどで生じる。前者は「想定以上の大量データ受付」、後者は「想定以上の割り込みの発生」CFMDにまとめた。前者のRRMは「受付可能データ制限機能の追加」、「受付可能データ数のSOPへの追記」など、後者のRRMは「多重割り込みの制限」、「多重割り込み制限のSOPへの追記」などとした。「プログラムが反応しない」、「応答が遅くなる」は、プログラムの実行要求が頻発する、他のプログラムがCPUを占有することなどで生じる。これらは「想定以上のCPU負荷の発生」CFMDにまとめた。そしてRRMは、「CPU使用率表示機能の追加」、「CPU過負荷状態での実行要求受付制限機能の追加」とした。

八番目に悪意のある操作や攻撃にかかわるものについて述べる。市販のUnified Threat Management (UTM) ツールの機能を参考としてデータの流出、データの改ざん、Denial

Table 2 List of common failure modes for DMCS

Group	Common Failure Mode	Failure Example	Countermeasure Policy	Representative Risk Reduction Measures
Startup	The startup conditions for functions are not prepared	Related operations cannot be conducted, an improper system status exists	Review the startup conditions Conduct multiple checks when startup Conduct the startup check	Add the confirmation procedure for the startup conditions to the SOP (3), set the conditions as to whether or not to start (4) Display the startup status (4)
Termination	The termination conditions for functions are not prepared	Related operations cannot be conducted, an improper system status exists	Review the termination conditions for Conduct multiple checks upon termination Conduct termination check Transit to the safe status for top priority	Add the confirmation procedure for termination conditions to the SOP, set the conditions whether or not to terminate (4), multiplex the termination confirmation procedure (4) Display the termination status (4) Add the emergency stop function (4) Conduct double checks on SOP (3)
Input/Output	Instructions on SOP misread	Improper drugs are manufactured, an improper	Conduct multiple checks on SOP Improve the visibility of SOP indications	Integrate the SOP format (3) Conduct double checks on HMI (3)
	Indications on HMI misread	Improper drugs are manufactured, an improper system status exists	Improve the visibility of HMI Check the content of HMI	Integrate the HMI format (4) Add the reconfirmation function (4)
	Mistake in checking products	Improper drugs are	Conduct multiple checks on products	Conduct double checks on products (3)
	Past data is lost	Data related to quality is lost	Notify when data is lost	Add the warning function for past data loss (4)
	Latest data is lost	Improper drugs are manufactured, an improper	Notify if there is a data loss risk	Add the warning function for the latest data loss (4)
	An inputting error	Improper drugs are manufactured, an improper	Multiple checks on input data	Conduct double checks on setting data (3)
Calibration	Long time intervals for function calibration	A wrong measurement is done, improper drugs are manufactured	Conduct periodic reviews	Shorten time intervals for function calibration (3)
Qualification	Wrong operation authority	Proper operations cannot be done, improper drugs are	Confirm the qualification before operation Do not set improper authority	Confirm operation authority before operation (3) Review authority periodically (3)
Backup	Insufficient backup	Data disappears, data related to quality is lost	Conduct proper backup operations Shorten backup intervals Realize faster processing	Organize the backup procedure in the SOP (3) Shorten backup time intervals (3) Realize faster update processing (5)
Unexpected CPU Load	Unexpected data update occurs	Data cannot be updated	Develop faster devices	Install faster memory devices (3)
	The upper limit of calculation precision is	Improper drugs are	Increase significant digits	Utilize double-precision variables (5)
	The lower limit of calculation precision is	Improper drugs are	Increase significant digits	Utilize double-precision variables (5)
	Divided by zero	Operation is suspended	Give a warning of division by zero	Add the warning function for a small divisor
	Unexpected amount of data is accepted	Abnormal program shutdown	Refuse data Do not input data	Add the restriction function for available data (4) Add the number of available data to the SOP (3)
	Unexpected interruption tasks occur		Restrict interruption tasks Prohibit interruption tasks	Restrict interruption tasks (5) Add the restriction function for interruption tasks to the SOP (3)
Malicious operations or attacks	Unexpected CPU load occurs	Program does not response, a slow response	Unexpected execution requests are not sent Refuse unexpected execution requests	Add the function of displaying CPU usage (5) Add the restriction function for accepting execution requests under CPU overload (5)
	No identification for important data	Data is removed	Take measures so that data is not removed	Introduce DLP tools (4)
	No access control for data	Data is falsified	Take measures so that data is not accessed	Add access control for data according to each user (4)
	Data could be rewritten	Related operations cannot be conducted	Take measures so that data is not falsified	Add e-signature (4), add time stamp (4)
	Vast amounts of data sent		Data acceptance is blocked	Disconnect from the external network (3)
	Vast amounts of requests sent		Data is selected	Install fire walls (3)
	Illegally accessed from the outside	System is invaded	Disconnect Discover illegal access	Disconnect from the external network (3) Introduce IDS (3), Introduce IPS (3)
			Remove computer virus	Introduce antivirus software (4)
			Take measures so that virus does not invade	Introduce virus protection software (4)
				Conduct virus check on USB memory devices connected (3)

of Service Attack (DOS), 不正アクセス, ウィルス感染などについて検討する。データの流出は, DMCS 内部のデータをコピーして持ち出すことなどで生じる。これらは, 「重要データの識別がない」, 「データへのアクセス制限がない」CFMD にまとめた。そして前者の RRM は「Data Loss Prevention (DLP) ツールを導入する」など, 後者の RRM は「ユーザの使用権限を設定する」などとした。データの改ざんは, 電子データを書き換えられることで生じる。この CFMD は「データの書き換えができる」とした。そして RRM は「電子書名を追加する」, 「タイムスタンプを追加する」などとした。DOS は, 大量の不正なパケットや要求を送りつけられサービス提供ができなくなることで生じる。これらは「大量データを送りつけられる」, 「大量要求を送りつけられる」CFMD にまとめた。そして RRM は「外部ネットワークから遮断する」, 「ファイアウォールを設置する」などとした。不正アクセスは, 社外から社内システムにアクセスされることで生じる。この CFMD は「外部からの不正アクセスができる」とした。そして RRM は「外部ネットワークから遮断する」, 「Intrusion Detection System (IDS) を導入する」, 「Intrusion Prevention System (IPS) を導入する」などとした。ウィルス感染は, ウィルスが付着したデータを受け取ることで生じる。したがって, CFMD は「ウィルスが付着したデータを授受する」とした。そして, RRM は「ウィルス除去ソフトを導入する」, 「IPS を導入する」などとした。また, 近年では, USB メモリを介して感染するウィルスやプログラマブル・ロジック・コントローラを用いた監視制御システムに感染するウィルスが出現している¹⁸⁾。これらの CFMD も「ウィルスが付着したデータを授受する」とした。そして, RRM は「使用

する記憶媒体の事前ウィルス確認の実施」, 「監視制御システム向けの UTM の導入」などとした。

Table 2 に上記の結果をまとめ直した共通故障モード一覧表を示す。RRM の後の括弧付数値は, その値以上のカテゴリで適用可能なことを表わす。DMCS は SOP に従って操作員が操作するため, 機能の種類はさまざまだが, 操作員の資格確認, 起動, データ入出力, 停止という作業の流れと定期的なバックアップや校正などの作業の流れは同様であったため, 上記の CFMD に集約できたと考えられる。

4.2 共通故障モードの FMEA への適用方針

4.1 節で導出した CFMD を各カテゴリの DMCS のリスクマネジメントに適用するための方針について考える。

(1) カテゴリ 3 の DMCS への適用方針

本論文で想定しているカテゴリ 3 の DMCS は, 市販品の製造装置, 計測装置, 計測機器などの小規模な装置である。これらは, SOP に従って, 外部から動作指示やパラメータを与え, 内部で処理を行ない, 結果を返す。処理内容はブラックボックスであり, 変更できない。DMCS によっては, 内部にデータを蓄積しているもの, ネットワーク接続しているものもある。なお, 1 つの DMCS の中に複数のカテゴリの DMCS が含まれる場合は, カテゴリ単位に分割してリスクマネジメントを行なう。上記特徴をもつカテゴリ 3 の DMCS に対して, Table 2 で示した CFMD の適用方針を述べる。

カテゴリ 3 の DMCS はボタンを押下したり, HMI をチェックしたりするだけなので, 操作員ができることはない。そのため, 機能の起動条件が揃わない CFMD の影響は検討しない (スイッチのスティックなどが考えられるが, ハードウェアに関するものなので扱わない)。機能の停止条件が揃わない

CFMD も、同様の考えにより検討しない。

入出力操作グループの CFMD について検討する。DMCS は SOP, HMI, ものを見ながら作業を行なう。これらの CFMD が生じると、医薬品の品質不良や提出データの不備が生じる。したがって、これらの CFMD の影響を検討する。一方、HMI が未装備、ものを扱わない場合は、検討しない。DMCS のデータ入出力の頻度はさまざまである。頻度が低い場合、上書きにより過去のデータを損失したり、書き込み不可で最新のデータを損失したりすることは生じないので、この CFMD の影響は検討しない。一方、頻度が高い場合、これらの事象が生じて提出データに不備が生じるので、この CFMD の影響を検討する。データの入力を誤ると医薬品の品質、提出データの不備が生じるので、この CFMD の影響を検討する。

校正を行なう間隔が長い CFMD が生じると、計測結果が不適切となり、医薬品の品質不良や提出データの不備が生じる。したがって、この CFMD の影響を検討する。

作業員の資格間違い CFMD が生じると、不適格な作業員の作業で医薬品の品質不良が生じる。したがって、この CFMD の影響を検討する。

バックアップの不備の CFMD が生じると、データを損失して提出データに不備が生じる。したがって、この CFMD の影響を検討する。

想定外の負荷グループの CFMD は機能の改造ができないので、原則として影響を検討しない。必要があれば、使用条件を SOP に追記する。

悪意のある操作や攻撃グループの CFMD の影響は、DMCS の構成に応じて検討する。基本方針を以下に示す。重要データの識別がない、データへのアクセス制限がない、データの書き換えができる CFMD は、機能がある場合は影響を検討し、ない場合は検討しない。大量データを送りつけられる、大量要求を送りつけられる、外部から不正アクセスされる CFMD は、ネットワーク接続がある場合は検討し、ない場合は検討しない。ウイルスが付着したデータを授受する CFMD は、記憶媒体やネットワーク経由のパラメータ入出力がある場合は影響を検討し、ない場合は検討しない。

上記 CFMD に対し、Table 2 から適切な RRM を選択する。

(2) カテゴリ 4 の DMCS への適用方針

本論文で想定しているカテゴリ 4 の DMCS は、データ管理システム、やや複雑な制御システム、監視制御とデータ収集システムなどであり、機能の構成設定が可能である。これらは、SOP に従って、ボタンや HMI から動作指示やパラメータを与え、内部で処理を行ない、結果を返す。機能の取捨選択は可能であるが、処理内容はブラックボックスであり、変更できない。カテゴリ 3 と同様に内部にデータを蓄積しているもの、ネットワーク接続しているものがある。上記特徴をもつカテゴリ 3 の DMCS に対して、Table 2 で示した CFMD の適用方針を検討する。

起動と停止の操作グループの CFMD は、カテゴリ 3 と同様の考え方で、影響を検討しない。入出力操作、校正作業、作

業員資格、バックアップのグループの CFMD は、カテゴリ 3 と同様の考え方で、影響を検討する。想定外の負荷グループの CFMD は、カテゴリ 3 と同様の考え方で、影響を検討しない。悪意のある操作や攻撃グループの CFMD は、カテゴリ 3 と同様の考え方で、影響を検討する。

上記 CFMD に対し、Table 2 から適切な RRM を選択する。

(3) カテゴリ 5 の DMCS への適用方針

本論文で想定しているカテゴリ 5 の DMCS は目的に特化して個別開発されたデータ管理システム、自動倉庫システム、設備制御システムなどである。これらは、SOP に従ってボタンや HMI から動作指示やパラメータを与え、内部で処理を行ない、結果を返す。カテゴリ 3, 4 と同様に、内部にデータを蓄積しているもの、ネットワーク接続しているものがある。上記特徴をもつカテゴリ 5 の DMCS に対して、Table 2 に示した CFMD の適用方針を検討する。

起動と停止の操作にかかわる CFMD は、独自に開発したものである。操作のための前提条件が個別に設定されている。これらの CFMD が生じると医薬品の品質が低下したり、製造作業が遅延したりするので、影響を検討する。

カテゴリ 3, 4 と同様の考え方により、入出力操作、校正作業、資格、バックアップの CFMD は影響を検討する。

カテゴリ 5 の DMCS は個別開発なので、想定外の負荷グループの CFMD はすべて検討する。想定以上のデータ更新が発生する CFMD が生じると、処理が遅延・中断したり、提出データの不備が生じたりするため、影響を検討する。計算範囲の上下限オーバーの CFMD が生じると、製造される医薬品の品質に影響が生じたり、提出データに不備が生じたりするので、影響を検討する。ゼロ割をする CFMD が生じると、処理が遅延・中断したり、製造される医薬品の品質に影響が生じたり、提出データに不備が生じたりするので、影響を検討する。想定以上の大量データ受付、想定以上の割り込み発生、想定以上の CPU の負荷発生、CFMD が生じると、処理が遅延・中断したり、データ記憶領域が壊れたりして提出データの不備が生じるので、影響を検討する。

悪意のある操作や攻撃のグループの CFMD は、カテゴリ 3, 4 と同様の考え方で影響を検討する。

上記 CFMD に対し、Table 2 から適切な RRM を選択する。

4.3 新規共通故障モード発見のための PDCA サイクル

適切な FMEA の実施には、最新の CFMD を反映した一覧表の維持が必須である。Fig. 3 に新しい CFMD を発見して、それらを一覧表に反映するための PDCA サイクルを示す。(a) は、4.1 節で述べた収集 FMEA の結果からの CFMD を導出する手順である。(b) は社会的要求や新たな脅威の出現に対応する CFMD を追加する手順である。前者は DMCS に対する規制や法令が変更となった場合、後者は新しい攻撃手法やウイルスが発見された場合などに実施する。この手順で追加した CFMD には「プログラマブル・ロジック・コントローラを用いた監視制御システムを標的としたウイルスの侵入」がある。これらは監督機関からの注意喚起により追加

Fig. 3 Procedure of CSV and risk management tasks

した¹⁹⁾。このCFMDは最終的に「ウィルスが附着したデータを授受する」CFMDにまとめた。(c)は、DMCS使用中に故障が発生した場合に、その原因となる新しいCFMDを発見した場合の手順である。この手順で発見したCFMDは「想定以上の大量データ受付」、「想定以上のCPU負荷の発生」がある。これらは動作不良の原因を分析して、発見・追加した。(d)は、共通故障モード一覧表を用いてFMEAを実施した結果、新しいCFMDを発見した場合の手順である。この手順で発見したCFMDは「想定以上のデータ更新発生」である。これは、「想定以上の大量データ受付」CFMDの影響を検討中に、データの更新頻度が高くなると動作不良になることが判明して追加した。

4.4 リスクマネジメントの実施方法

3章の問題2を解決するためにリスクマネジメント実施手順を定める。Fig.1の構成設定とプログラミングの枠内に詳細なCSVとリスクマネジメントの流れを示す。この内容を明確にするためR3をR3-0～R3-4、R4をR4-1～R4-4に細分した。なお、下記作業の実施には、DMCS開発、FMEA、CSVに関する知識と数件の実施経験が必要と考えられる。

(1) R3-0の実施内容

R3-0では、CSV対象のDMCSのリスクマネジメントの実施方針を決定する。はじめに、CSV対象機能を洗い出す。CSV対象機能は、各種マスタ、指図、実績、検査、原材料、ロット番号、個数、分量、有効期限などの医薬品の品質に係るデータの生成にかかわるものとする。URSの機能とデータに関する情報を参考に、CSV対象機能を判定する。

つぎに、CSV対象機能に対してリスクアセスメントを実施する。一番目に、CSV対象機能に対し、4.2節で述べたCFMDの適用方針に沿って、共通故障モード一覧表の中から適用するものを選ぶ。二番目に、重要性、発生確率、発見確率を決定し、リスク優先度を決定する。三番目に、リスク優先度に従って、RRMを検討する。RRMはTable 2から、DMCSのカテゴリとリスク優先度を考慮して選択する。

Fig. 4 DB structure of design and verification information

(2) R3-1～R3-4 および R4-1～R4-2の実施内容

カテゴリごとにリスクマネジメントの実施内容を述べる。

ア. カテゴリ3のDMCSに対するリスクマネジメント

URS (R3-1)の作成とRT (R4-1)を実施する。R3-1では、R3-0で選んだTable 2のカテゴリ3向けのRRMをURSとSOPに追記する。R4-1では、URSに追記されたRRMが正しく行なわれたことを確認するRTを実施する。

イ. カテゴリ4のDMCSに対するリスクマネジメント

URS, FS, CS (R3-1～R3-3)の作成, RT, FT, CT (R4-1～R4-3)の実施を行なう。Table 2のカテゴリ3向けのRRMを適用した場合、作業はカテゴリ3の場合と同様となる。カテゴリ4向けのRRMを適用した場合、R3-1ではRRMをURSとSOPに、R3-2では要求を展開した機能をFSに、R3-3では機能の構成をCSに追記する。そして、R4-3では機能構成を確認するためのCTを、R4-2では複数の機能で実現される機能を確認するためのFTを、R4-1では機能を組み合わせる要求を確認するためのRTを実施する。

ウ. カテゴリ5のDMCSに対するリスクマネジメント

URS, FS, DS, MS (R3-1～R3-4)の作成, RT, FT, IT, MT (R4-1～R4-4)の実施を行なう。Table 2のカテゴリ3向けのRRMを適用した場合、作業はカテゴリ3の場合と同様となる。カテゴリ5向けのRRMを適用した場合には、R3-1ではRRMをURSとSOPに、R3-2では要求を展開した機能をFSに、R3-3では機能を展開した詳細機能をDSに、そして、R3-4では詳細機能を展開した処理ロジックをMSに追記する。R4-4では処理ロジックを判定条件/条件網羅の基準で作成したテストケースを用いてMTを、R4-3では複数モジュールからなる詳細機能を確認するためのITを、R4-2では複数詳細機能からなる機能を確認するためのFTを、そして、R4-1では複数機能からなる要求を確認するためのRTを実施する。

4.5 リスクマネジメント情報の連携

著者らはDMCSの設計と検証の情報を一元的に管理するデータベース(DB)を開発して、トレーサビリティを確保で

Fig. 5 Data sharing between FMEA

きるようにした²⁰⁾。この DB で本論文で扱うリスクマネジメント情報を追加した。Fig. 4 に DB の構造を示す。

カテゴリ 5 の DMCS を例に、リスクマネジメント結果の DB への反映方法を述べる。はじめに、Fig. 5(i) に示すように R3-0 で抽出した CSV 対象機能の RRM に関する設計情報を URS テーブルに記入する。つぎに、(ii) に示すように URS を複数の FS に展開し、URS と FS との間の対応関係を DB に設定する。そして、選択した RRM に関する設計情報を FS テーブルに記入する。以降、(iii), (iv) に示すように FS と DS, DS と MS との対応関係、設計情報、RRM に関する情報を DB に設定する。三番目に、(v) に示すように MS の内容に従ってモジュールを製作し、その設計情報をモジュールテーブルに記入する。四番目に、(vi) に示すようにモジュールを確認するための MT を設計し、MT テーブルに入力し、モジュールと MT との対応関係を DB に設定する。以降、(vii)~(ix) に示すように DS と IT, FS と FT, URS と RT との対応関係とテストの情報を DB に設定する。なお、カテゴリ 3 と 4 の場合は、必要のない文書と検証の情報を省略する。

5. 提案手法の適用と評価

カテゴリ 3, 4, 5 の DMCS に対して、Table 2 と 4.2 節の適用方針に従ってリスクマネジメントを行ない、提案手法を評価した。評価方法は、5 件の CSV の経験を有する技術者 A が提案手法で、20 件以上の CSV の経験を有する技術者 B が経験の手順 (DMCS 開発時に実施) で、リスクマネジメントを実施して、結果を比較することとした。経験的な手順では、CSV 対象機能に対する CFMD の列挙と RRM の開発文書への反映を経験に基づいて行なう。それ以外は同様である。

なお、リスクマネジメントを実施するに当たり、機能の重要性、発生確率、検出確率は以下の基準で決定した。重要度は (a) 最終製品の品質を損ねるか、(b) 患者および消費者の安全性を損ねるか、(c) 規制当局に提出するデータを不確実にするか、(d) 最終製品の製造を遅延する原因となるか、の観点で評価した。各観点には、複数のリスクに関する質問がある。(a) から (c) は、1 つでもリスクがあれば、重要性を「高」とした。(d) は、リスクがあれば「中」、ない場合は「低」と

した。発生確率は、1/100 回程度の発生を「高」、1/1000 回程度の発生を「中」、それ以下を「低」とした。検出確率は、毎回検出できる場合は「高」、2 回に 1 回程度検出できる場合は「中」、それ以下の場合は「低」とした。

5.1 カテゴリ 3 の DMCS への適用と評価

提案手法を赤外分光光度計へ適用した。この DMCS は、物質から放射されるスペクトルを解析するメーカー標準品である。試料データ入力、スペクトル解析、解析データ出力の機能を有し、すべて CSV 対象機能となっている。これらの機能はボタン押下により起動される。データ記憶装置とネットワーク接続はない。試料データ入力機能に対して実施したリスクマネジメント結果を以下に記述する。

作業者が SOP やものを見間違ふ CFMD が生じると不適切な医薬品が製造されるので、影響を検討した。重要性は高、発生確率は中、検出確率は高とした。したがって、Fig. 2 よりリスク優先度は中となった。RRM は Table 2 から、SOP の二重確認と入力時の試料データ二重確認を採用した。その結果、発生確率が低となり、リスク優先度は低となった。

校正を行なう間隔が長い CFMD が生じると提出データ不備が生じるので、影響を検討した。重要性は高、発生確率は中、検出確率は高なので、リスク優先度は中となった。RRM は Table 2 から、使用前の校正実施を採用した。その結果、発生確率が低となり、リスク優先度は低となった。

作業員の資格間違い CFMD が生じると不適切な医薬品が製造されるので、影響を検討した。重要性は高、発生確率は低、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 から作業前後の作業員の資格確認を採用した。この結果、リスク優先度は変わらないが、発生確率が低下した。

ウィルスが付着したデータを授受する CFMD が生じると機能や計測結果が不適切となり、不適切な医薬品の製造、提出データ不備が生じるので、影響を検討した。重要性は高、発生確率は低、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 から入力に用いる記憶媒体の事前ウィルスチェックを採用した。この結果、リスク優先度は変わらないが、発生確率が低下した。

上記リスク低減策を実現するために、Fig. 4 のカテゴリ 3 の手順に従い、URS と SOP の修正と RT を実施した。ほかの機能についても、同様に検討を行なった。

A と B の結果を比較した結果、B はウィルスが付着したデータを授受する CFMD の検討がなかった。これは、FMEA 実施時に制御機器に感染するウィルスが現れていなかったためである。それ以外は同様の対策がとられていた。これらの結果より、4.2(1) の方針に従えば、カテゴリ 3 の DMCS に対して適切なリスクマネジメントができることがわかった。

5.2 カテゴリ 4 の DMCS への適用と評価

電子文書管理 DMCS への適用を行なった。この DMCS は構成を設定して使用する市販ソフトウェアであり、機能の取捨選択は可能であるが、機能の改造はできない。この DMCS は電子データの登録、承認、検索、取出し、バックアップ、

印刷などの機能を有している。その中で文書の登録、承認、検索、取出し、バックアップの機能が CSV 対象となっている。この DMCS は HMI の操作で上記機能を起動する。この DMCS はデータ蓄積機能を有しているが、ネットワークは未接続である。文書の登録機能に対して実施したリスクマネジメント結果を以下に記述する。

SOP, HMI, ものを見間違ふ CFMD が生じると不適切な医薬品が製造されるので、影響を検討した。重要性は高、発生確率は中、検出確率は高なので、リスク優先度は中となった。RRM は Table 2 から SOP, HMI, 文書データの二重確認を採用した。この結果、発生確率が低となり、リスク優先度が低となった。

校正を行なう間隔が長い CFMD が生じると、作成時刻がずれて、提出データ不備となるので、影響を検討した。重要性は高、発生確率は中、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 から、使用前の時刻校正実施を採用した。この結果、リスク優先度は変わらないが、発生確率が低下した。

作業員の資格間違い CFMD は、カテゴリ 3 と同様の理由で検討した。リスクマネジメント内容も同様とした。

バックアップの不備 CFMD が生じると、登録データが損失して、提出データ不備となるので、影響を検討した。重要性は高、発生確率は低、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 からバックアップを行なうモジュールの追加を採用した。

データへのアクセス制限がない CFMD が生じると、不適切な者が入手する可能性があるので、影響を検討した。重要性は高、発生確率は低、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 から使用権限の設定を採用した。この結果、リスク優先度は変わらないが、発生確率が低下した。データの書き換えができる CFMD が生じると、文書の改ざんにより提出データ不備となるので、影響を検討した。重要性は高、発生確率は低、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 から電子署名とタイムスタンプの追加を採用した。この結果、リスク優先度は変わらないが、発生確率が低下した。ウィルスが付着したデータを授受する CFMD は、カテゴリ 3 と同様の理由で検討した。リスクマネジメント内容も同様とした。

上記のリスク低減策のうち、バックアップモジュール追加は、Fig. 4 のカテゴリ 4 の手順に従い、URS, FS, CS, SOP の修正と CT, FT, RT を実施した。それ以外は、カテゴリ 3 の手順に従い、URS と SOP の修正と RT を実施した。ほかの機能についても、同様に検討を行なった。

A の結果と B の結果を比較したところ、同様の対策がとられていた。これらの結果より、4.2(2) の方針に従えば、カテゴリ 4 の DMCS に対して適切なリスクマネジメントができることがわかった。

5.3 カテゴリ 5 の DMCS への適用と評価

計量装置の DMCS への適用を行なった。この装置は製造

指図データを読み込み、所要量を算出し、手計量し、計量結果を印刷する機能を有している。手計量以外が CSV 対象機能である。この DMCS はデータ蓄積機能を有しているが、ネットワークには未接続である。製造指図データ読み込み機能に対して実施したリスクマネジメント結果を以下に記述する。

起動と停止の操作に関する CFMD が生じると、作業が遅延・中断するので、影響を検討した。重要度は中、発生確率は中、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 から機動と停止の条件の確認を採用した。この結果、リスク優先度は変わらないが、停滞する時間が短縮された。

SOP, HMI, ものを見間違ふ CFMD が生じると、医薬品の品質に影響を与えるので、影響を検討した。重要性は高、発生確率は中、検出確率は高なので、リスク優先度は中となった。RRM は Table 2 から入出力画面に表示された製造指図の二重確認、入力製造指図の二重確認を採用した。この結果、発生確率が低となり、リスク優先度が低となった。入出力データを誤る共通故障モードは、医薬品の品質に影響を与えるので、影響を検討した。重要性は高、発生確率は中、検出確率は高なので、リスク優先度は中となった。RRM は Table 2 から入力製造指図の二重確認、計量結果に印刷された製造指図と元の製造指図との二重確認を採用した。この結果、発生確率が低となり、リスク優先度が低となった。

校正を行なう間隔が長い、作業員の資格間違い CFMD は、カテゴリ 3, 4 と同様の理由で、検討した。リスクマネジメント内容も同様とした。

バックアップ操作の不備 CFMD が生じると、提出データ不備となるので、影響を検討した。重要性は高、発生確率は低、検出確率は高なので、リスク優先度は低となった。RRM は Table 2 から製造指図データ読み込み直後のバックアップを採用した。この結果、リスク優先度は変わらないが、発生確率が低下した。

想定以上のデータ更新発生、想定以上の大量データ受付、想定以上の CPU 負荷の発生 CFMD は、DMCS はスタンドアロンで、記憶媒体経由のデータ手入力なので、影響を検討しなかった。想定以上の割り込み発生は、割り込みを使用していないので、検討しなかった。計算範囲の上下限オーバー、ゼロ割の CFMD が生じると、作業の遅延・中断、医薬品の品質に影響が生じるので、影響を検討した。重要度は中、発生確率は低、検出確率は高なので、リスク優先度は低となった。計算範囲の上限と下限のオーバーに対する RRM は Table 2 から倍精度型変数の使用を採用した。ゼロ割に対する RRM は除数が小さい場合の警告機能を採用した。それぞれ、リスク優先度は変わらないが、検出確率が向上した。

データへのアクセス制限がない CFMD は、カテゴリ 4 と同様の理由で検討した。リスクマネジメント内容も同様とした。ウィルスが付着したデータを授受する CFMD は、医薬品の品質に影響を与えるので、影響を検討した。重要度は高、発生確率は低、検出確率は高とし、リスク優先度は低となった。RRM は Table 2 から入力データの事前ウィルスチェッ

クを採用した。この結果、リスク優先度は変わらないが、発生確率が低下した。

上記のうち、倍制度型変数の使用と計算精度とゼロ割り警告機能の追加は、Fig. 4 のカテゴリ 5 の手順に従い、RRM を URS, FS, DS, SOP に反映させて、MT, FT, RT を実施した。それ以外は、カテゴリ 3 の手順に従い、RRM を URS と SOP に反映させて、RT を実施した。ほかの機能についても、同様に検討を行なった。

A の結果と B の結果とを比較したところ、B の結果にはウィルスが付着したデータの授受 CFMD に関する影響の検討が行なわれていなかった。これは、カテゴリ 3 と同様の理由による。また、RRM の FS への記述漏れ、FT 未実施の事項が 2 つあった。それ以外は同様の対策がとられていた。これらの結果より、4.2(3) の方針に従えば、カテゴリ 5 の DMCS に対して適切なリスクマネジメントができることがわかった。

6. おわりに

本論文では、DMCS のリスクマネジメント手法を提案し、その標準化を図った。提案手法を DMCS に試行した結果、従来のリスクマネジメント手法と同等の結果を得ることができ、故障対策の漏れを防止する効果も確認できた。したがって、提案手法は今回想定した DMCS に対して適用できることがわかった。一方、今回作成した共通故障モード一覧表は医薬品製造に直接関係するシステムを対象としたため、生産管理システム、Material Resource Planning システムなどの基幹系システムへは未対応である。今後の課題としたい。さらに、提案手法をさまざまな DMCS へ適用していきたい。

謝辞 本研究は日本学術振興会科学研究費補助金基盤研究(c)、課題番号 21500439「医薬品製造に関わるソフトウェアの統合的なコンピュータ・バリデーション手法の研究」の助成による。

参考文献

- 1) Food and Drug Administration: Software Development Activities, Food and Drug Administration (1997)
- 2) 厚生労働省：医薬品・医薬部外品製造販売業者等におけるコンピュータ化システム適性管理ガイドライン，厚生労働省 (2010)
- 3) GAMP forum: GAMP 5 A Risk-Based Approach to Compliant GxP Computerized Systems, International Society for Pharmaceutical Engineering (2008)
- 4) 塩見，岡島，石山：FMEA, FTA の活用，日科技連 (1983)
- 5) W.E. Vesely, F.F. Goldberg, H.H. Roberts and D.F. Haasl: Fault tree handbook, Technical Report NUREG-0492, U.S. Nuclear Regulatory Commission (1981)
- 6) H. Ozog: Hazard identification, analysis, and control, Hazard Prevention, 6/13 (1985)
- 7) 萩原，他：コンピュータバリデーション，FDA・厚生省 ER/ES 指針とその適用事例，情報機構 (2006)
- 8) 高橋，津田：医薬品製造設備における制御ソフトウェアの効率的コンピュータ・バリデーション，情報処理学会論文誌，45-12, 2869/2879 (2004)
- 9) ISPE GAMP Japan Forum：リスクベースアプローチ実施ガイド，ISPE 日本支部 (2006)
- 10) 森田雅弘：FMEA を活用したソフトウェアのバグの低減，ソ

- フトウェア品質管理事例集，日科技連，461/486 (1990)
- 11) 丹羽雅春：FMEA を用いたシステム設計の信頼性向上，ソフトウェア品質管理事例集，日科技連，467/475 (1990)
- 12) 高井，田村，森崎，松本：Web アプリケーションを対象とした故障モード影響解析の試行，情報処理学会研究報告，2009-SE-166-12 (2009)
- 13) 山科，森崎：大規模ソフトウェアの保守開発を対象とした故障モード解析 (FMEA) 適用の試み，Unisys Technology Review, 99-Feb., 107/121 (2009)
- 14) P.L. Goddard: Validating The Safty of Embedded Real-Time Control Systems Using FMEA, Proc. Annual Reliability and Maintainability Symposium 1993, 227/230 (1993)
- 15) P.L. Goddard: Software Safty Techniques, Proc. Annual Reliability and Maintainability Symposium 2000, 119/123 (1993)
- 16) N. Snook: Model-based Failure Modes and Effects analysis of Software, Proc. 15th International Workshop on the Principles of Diagnosis, 221/226 (2004)
- 17) K.G. Johnson and M.K. Khan: A study into the use of process failure mode and effects analysis (PFMEA) in the automotive industry in the UK, Journal of Materials Processing Technology, 139-1-3, 348/356 (2003)
- 18) E. Luijijf: SCADA Security Good Practices for the Drinking Water Sector, TNO Report, TNO Defense, Security and Safty (2008)
- 19) 情報処理推進機構：Stuxnet (スタックスネット) をはじめとした新しいサイバー攻撃手法の出現，<http://www.ipa.go.jp/about/technicalwatch/20101217.html> (2010)
- 20) 高橋，福江：改造を考慮した医薬品製造にかかわるソフトウェアの回顧的コンピュータ化システムバリデーションの一手法，計測自動制御学会論文誌，45-12, 731/740 (2009)

[著者紹介]

高橋 正和 (正会員)

1988 年立教大学理学部物理学科卒業。同年 IHI 入社。98 年筑波大学大学院経営システム科学専攻修了。2002 年同博士課程修了。博士 (システムマネジメント)。2005 年島根大学総合理工学部助教授，2008 年山梨大学大学院医学工学総合研究部准教授。情報処理学会，電気学会などの会員。

難波 礼治

1999 年第一工業大学工学部土木工学科卒業。2003 年島根大学大学院教育学研究科教科教育専攻修了。2008 年同総合理工学研究科博士課程電子機能システム工学専攻修了。博士 (工学)。2008 年第一工業大学工学部社会環境工学科助教，2011 年同講師。日本機械学会，土木学会の会員。

福江 義則

1990 年関西学院大学経済学部卒業。同年富士通入社。2004 年筑波大学大学院経営システム科学専攻修了。2008 年徳島大学大学院工学研究科情報システム工学専攻修了。博士 (工学)。情報処理学会，人工知能学会の会員。