Vol.2011-SE-173 No.5
2011/7/21

医薬品製造に関わるコンピュータ化システムの FMEA

高橋正和†

本論文では，医薬品製造に関わるコンピュータ化システム(DMCS)が有する共通故障モードを抽出し，それを用いて FMEA を実施する方法について述べる．医薬品は DMCS で制御された製造設備を使用して生産されるので，DMCS の機能は安全なものでなければならない．DMCS の安全性を検討するためには FMEA が使用される．FMEA を実施するには，全ての故障モードを漏れなくリストアップすることが重要であるが，その作業は困難なものである．この問題を解決するために，既存の DMCS の FMEA の結果を分析して，DMCS の FMEA で共通に使用可能な故障モードを洗い出した．そして，共通故障モード，故障，故障対策から構成される一覧表を作成した．この一覧表を使用することで，網羅的な FMEA を実施できるようにした．

A FMEA Method for Computerized Systems Regarding Drug Manufacturing

Masakazu Takahashi†

This paper shows common failure modes that drug manufacturing computerized system (DMCS) has and a method conducting FMEA with the common failure modes. Since drugs are manufactured in facilities controlled by DMCS, the functions must be safe. FMEA is used to investigate the safety. Conducting FMEA effectively, it is important to enumerate all failure modes. But it is difficult. To solve this problem, we enumerated the common failure modes that we could commonly use for conducting DMCS's FMEA. And we develop a list that consists of common failure modes, failures and countermeasures. Using this list, we can conduct FMEA exhaustively.

1. はじめに

医薬品は，人間の健康を維持するために必要不可欠なものである．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，医薬品はコンピュータ化システムが搭載された製造設備を用いて製造されている（以降， DMCS（Drug Manufacturing Computerlized System）と呼ぶ）．DMCSは製造設備の頭脳であるため，DMCSの機能と性能が不適切であると，医薬品の品質に悪影響を与える．このことが大きな社会問題となっている．

DMCSの機能と性能を適切で安全なものとするためには，DMCS設計段階において，十分な検討が必要となる．その際，国際医薬品エンジニアリング協会は，安全性を網羅的に検討する方法として故障モード影響解析（FMEA:Failure Mode and Effects Analysis)を使用することを推奨している[1)]．FMEAは適切な機能を有していた製品が，使用に伴う構成部位の変化により，製品の機能が不適切となる事象の原因や対策を検討するための手法である．このとき，部品の変化のことを故障モード，機能が不適切となる事象を故障と呼ぶ．

FMEAを用いたソフトウェアの安全化に関する研究としては，対象ソフトゥエアをブロックに分割し，それ毎に故障モードと推定原因を列挙してバグを発見する方法[2)]，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対策を行うことで信頼性を向上させる方法[3)]，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うことで信頼性を向上させる方法[4,5)] 等がある．しかし，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いるため，故障モードを漏れなく列挙できるとは限らない．そのため，網羅的な対策を施すことが困難となっている．加えて，ソフトウェアの故障モードとバグの識別があいまいであり，適切な FMEAの実施が困難となっている．

この問題を解決するため，複数の既存DMCSのFMEA実施結果を比較して，DMCSで共通に使用可能な故障モード，故障（システムへの影響），故障対策等をまとめた一覧表を作成した．DMCSのFMEAを実施する際に，この一覧表を使用することで，作業者の能力や経験の影響を受けないで，適切なFMEAを実施できるようにする．

2. 共通故障モードの導出

2.1 2.1 共通故障モードの考え方

本論文で取り扱う共通故障モードの考え方について述べる．DMCSは制御装置に搭載されて，標準作業手順書（SOP : Standard Operation Procedure）に則って運用される．

そのため，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，FMEAの方法は既に確立されているため，本論文では対象外とする[6]．

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．これらは，適切な設計とテストにより除去されるべきである．これらは，ソフトウェアの変化を伴わないので，本来の意味で故障モードではない．従って，本論文では対象外とする．一方，悪意を持つソフトウェアが侵入して，ソフトウェアを書き換えて，正常に動作しなくなる事例が発生している．これはソフトウェアの変化を伴うので，故障モードと考える．従って，本論文の対象とする．

運用については，SOPに則った作業が実施されていれば，運用の変化は伴わない．しかし，SOPやヒューマン・マシン・インターフェース（HMI:Human Machine Interface)の見間違い，想定外の運用等により，ソフトウェアが正常に動作しなくなることがある[7]．これらは運用の変化を伴うので，故障モードと考える．従って，本論文の対象とする．なお，運用の変化は操作員がDMCSの起動，停止，入力，出力，校正，バックアップ等を行う際に発生する．

2.2 2.2 共通故障モードの抽出

DMCSに共通の故障モードを導出するために，20件の既存DMCSのFMEA結果を収集し，それらを故障の種類で分類した．その上で，故障を引き起こす故障モードの類似点を見つけ出し，共通化した．表1にFMEAの結果を故障種類で分類した結果を示す．

以下に，分類結果毎に共通故障モードを導出するための手順を記述する．

(1)機能の起動に関わる共通故障モード

「制御条件が設定できない」，「制御条件を通信できない」等の故障モードは，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ことで生じる．従って「機能の開始条件が揃わない」という共通故障モードにまとめられる．そして，リスク低減策は「開始条件確認作業のSOPへの追加」等となる．また，前述の故障は，SOPの記述やHMIの表示の見間違えでも生じる．これらは「SOPを見間違う」，「HMIを見間違う」という共通故障モードにまとめられる．そして，リスク低減策は「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」等となる．

(2)機能の停止に関わる共通故障モード

「制御条件が設定できない」，「制御条件を通信できない」等の故障は，起動と同様の考え方により「機能の終了条件が揃わない」，「SOPを見間違う」，「HMIを見間違う」という共通故障モードにまとめられる．そして，リスク低減策は「終了条件確認作業の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」等となる．機能の停止に関わる故障のうちデータ更新の適時性が要求される「データを保管できない」，「入力データを設定できない」等の故障は，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」という共通故障モードにまとめられる．そして，リスク低減策は「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」等となる．

(3)データの入出力に関わる共通故障モード

「所定の回転数を逸脱する」，「所定の制御条件を逸脱する」等の故障モードは，SOP記述やHMI表示の見間違えることで生じる．これらは「SOPを見間違う」，「HMIを見間違う」という共通故障モードにまとめられる．そして，リスク低減策は「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」等となる．また，これらは入力時に誤ったデータを設定したり，ものを間違ったりして生じる．前者は，「入力を間違う」という共通故障モードにまとめられ，リスク低減策は「設定データの二重確認」となる．後者は，「ものを見間違える」という共通故障モードにまとめられ，リスク低減策は「ものの二重確認」となる．

(4)プログラムの動作に関わる共通故障モード

「空き棚数が更新されない」，「禁止棚が更新されない」等の故障モードは，頻繁に空き棚や禁止棚に関する情報の更新が行われることで生じる．これらは「想定数以上の更新が要求される」という共通故障モードにまとめられる．そして，リスク低減策は「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」等となる．「誤った計量指図計算をする」，「誤った原材料を採取する」等の故障モードは，「計量値を間違って入力する」，「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」等となる．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「データの範囲が不適切」という共通故障モードにまとめられる．リスク低減策は，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」，「データ範囲の確認」となる．それ以外に「誤った計量計算をする」の故障モードとして，「ゼロ割をする」があり，リスク低減策は「除数が小さい時の警告の追加」となる．

(5)プログラムの以上に関わる共通故障モード

「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ったり，割り込みが多発して割り込みからの復帰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したりする等で生じる．前者の共通故障モードは「想定以上の大量データ受付」，リスク低減策は「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」等となる．後者の共通故障モードは「想定以上の割り込みの発生」となり，リスク低減策は「多重割り込みの制限」，「多重割り込

表1 FMEA結果の分類
Table 1 Classification of FME results

	機能	故障	故障モード	共通故障モード
ソフトウェア機能の起動に関わるもの				
計測データ管理システム	制御条件設定機能	制御条件を設定できない	制御条件の入力画面が開かない	開始条件が揃わない，SOPを見間違う，HMIを見間違う
	通信機能	制御条件を通信できない	制御条件の通信が開始しない	
製品倉庫搬入出システム	入庫設定機能	入庫データを設定できない	入庫データの入力画面が開かない	
	搬送機能	搬送データを設定できない	搬送データの入力画面が開かない	
：	：	：	：	
ソフトウェアの機能の停止に関わるもの				
計測データ管理システム	制御条件設定機能	制御条件を設定できない	制御条件の入力画面が閉じない	終了条件が揃わない，SOPを見間違う，HMIを見間違う，過去のデータを損失する，最新のデータを損失する
	通信機能	制御条件を通信できない	制御条件の通信が終了しない	
	：	：	：	
計測データ管理システム	データ保管機能	データを保管できない	データの書き込みが終了しない	
自動倉庫	入庫設定機能	入力データを設定できない	データの書き込みが終了しない	
：	：	：	：	
データ入力に関わるもの				
遠心分離機	加速機能	所定の回転数を逸脱する	回転数の入力を誤る	SOPを見間違う，HMIを見間違う，入力を間違う，ものを見間違う
	：	：	：	
計測データ管理システム	検索条件設定機能	不適切な検索が行われる	仕様外の検索条件を入力する	
	：	：	：	
製品倉庫搬入出システム	入庫設定機能	誤ったパレットが入庫される	入庫パレットデータの入力を誤る	
	：	：	：	
製品倉庫搬入出システム	入庫設定機能	誤ったものを荷台に載せる	もののIDが間違っている	
	入庫設定機能	ものを誤った荷台に載せる	荷台のIDが間違っている	
：	：	：	：	
プログラムの動作に関わるもの				
製品倉庫搬入出システム	空棚数管理機能	空棚数の更新がされない	空棚数の更新がされない	更新負荷が高い
	禁止棚管理機能	禁止棚の更新がされない	禁止棚の更新がされない	
	：	：	：	
計量システム	指図読込機能	誤った計量指図料を計算する	計量値を間違って入力する	入力を間違う，SOPを見間違う，HMIを見間違う，データの範囲が不適切
	：	：	計量値を読み間違う	
	：	：	範囲外の計量地が入力される	
	原材料自動採取機能	誤った原材料を採取する	誤った原材料を入力する	
	：	：	原材料を読み間違う	
	：	：	指定外の原材料が入力される	
	計量計算機能	誤った計量指図料を計算する	ゼロ割をする	小さな徐数で割り算をする
：	：	：	：	
プログラムの異常に関わるもの				
全てのシステム	全てのソフトウェアの機能	プログラムが異常停止する	想定外の異常データ処理	想定外の異常データ処理
			想定外の割り込みの多発	想定外の割り込みの多発
		プログラムが反応しない	CPUが過負荷状態となる	CPUが過負荷状態となる
		応答が遅くなる	CPUが過負荷状態となる	
校正に関わるもの				
製品倉庫搬入出システム	入庫順序管理機能	間違った時刻が記録される	時刻の校正を行う間隔が長すぎる	機能の校正を行う間隔が長い
計量システム	計測機能	測定結果の誤差が大きい	はかりの校正を行う間隔が長すぎる	
：	：	：	：	
操作員の資格に関わるもの				
計測データ管理システム	アクセス制限機能	アクセス権のない操作員が操作をする	作業員の権限の誤り	作業員の権限の誤り
計量システム	計量指図量計算機能	無資格の作業員が操作をする	作業員の権限の誤り	
：	：	：	：	
バックアップに関するもの				
計測データ管理システム	利用者情報保管機能	操作員情報が消失する	記憶装置の故障	記憶装置の故障
計量システム	計量指図量計算機能	データが消失する	バックアップの不備	バックアップの不備
：	：	：	：	
悪意のある操作や攻撃に関するもの				
全てのシステム	全てのソフトウェアの機能	データを持ち出される	データへのアクセス制限がない	データのアクセス制限がない
			システムへのアクセス制限がない	システムのアクセス制限がない
		データを改ざんされる	データの書き換えができる	データの書き換えができる
		サービス拒絶攻撃を受ける	大量の不正パケットを受信する	大量の不正パケットを受信する
		不正にアクセスされる	外部からの不正アクセスができる	外部から不正アクセスができる
		悪意のあるサイトへアクセスする	有害サイトへアクセスする	有害サイトへアクセスする
		ウィルスに感染する	ウィルスが付着したデータを授受する	ウィルス付着データを授受する
	USBを使用する機能	ウィルスに感染する	ウィルスが付着したUSBを使用する	ウィルス付着USBを使用する

み制限のSOPへの追記」等となる．「プログラムが反応しない」，「応答が遅くなる」等などの故障は，プログラムの実行要求が頻発したり，他のプログラムがCPUを占有したりすることで生じる．これらは「想定以上のCPU負荷の発生」という共通故障モードにまとめられる．そしてリスク低減策は，「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」等となる．

(6)機能の校正に関わる共通故障モード

「間違った時刻が記録される」故障は，時刻の校正を行う間隔が長かったため時刻がずれたことで生じる．また，「測定結果の誤差が大きくなる」故障も，測定機器の校正を行う間隔が長かったために精度が悪化したことで生じる．これらの共通故障モードは「機能の校正を行う間隔が長い」となり，リスク低減策は，「機能の校正を行う間隔を短くする」となる．

(7)操作員の資格に関わる共通故障モード

「アクセス権のない作業員が操作をする」，「無資格の作業員が作業をする」故障は，作業員の資格の確認が不十分であることで生じる．これらは，「作業権限の間違い」という共通故障モードにまとめられる．リスク低減策は「作業前の権限確認」，「定期的な権限の見直し」等となる．

(8)データのバックアップに関わる共通故障モード

「操作員情報が消失する」，「データが消失する」故障は，記憶装置の故障，バックアップの不徹底で生じる．前者は「記憶装置の故障」共通故障モードに，後者は「バックアップの不備」共通故障モードにまとめられる．前者のリスク低減策は「記憶装置の多重化」，「定期的なバックアップ実施」，後者のリスク低減策は「バックアップ手順のSOP化」，「バックアップ間隔の短期化」等となる．

(9)悪意のある操作や攻撃に関わる共通故障モード

市販の統合脅威管理（UTM:Unified Threat Management)ツールの有する機能を参考としてデータの流出，データの改ざん，サービス停止攻撃（DOS:Denial of Service Attack)，不正サクセス，ウィルス感染　等の故障について検討する．

(a)データの流出

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等で生じる．この共通故障モードは，「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」となる．前者のリスク低減策は「情報漏えい防止（DLP:Data Loss Prevention)ツールを導入する」等となり，後者のリスク低減策は「ユーザのアクセス制限機能を追加する」等となる．

(b)データの改ざん

データの改ざんは，電子データを書き換えることで生じる．この共通故障モードは「データが書き換えられる」となる．対策は「電子書名を追加する」，「タイムスタンプを追加する」等となる．DOSは，外部から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．共通故障モードは「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」となる．そしてリスク低減策は「外部ネットワークから遮断する」，「ファイヤーウォールを設置する」等となる．

(c)不正アクセス

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．共通故障モードは「外部から不正アクセスされる」となる．そしてリスク低減策は「外部ネットワークから遮断する」，「侵入検出システム（IDS:Intrusion Detection System)を導入する」，「侵入防止システム（IPS:Intrusion Prevention System)を導入する」等となる．

(d)ウィルス感染

ウィルス感染は，ウィルスが付着したデータを受け取ったり，ウィルスが入り込んだりすることで生じる．共通故障モードは「ウィルスが付着したデータを授受する」となる．そして，リスク低減策は「ウィルス除去ソフトを導入する」，「IPSを導入する」等となる．また，近年では，USBメモリを介して感染するウィルスやPC以外のコンピュータを用いた監視制御システムを標的としたウィルスも出現している[8]．これらの共通故障モードはネットワークに接続している機器と同様である．リスク低減策は，「接続するUSBメモリ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」等となる．

悪意のある操作や攻撃は，新たなものが続々と現れるため，後述する新しい共通故障モードを発見するための手順に従って，定期的に見直す必要がある．

表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．

2.3 新しい共通故障モードを発見する手順

適切なFMEAを実施するためには，新しい共通故障モードを反映した一覧表を維持する必要がある．図１に新しい共通故障モード発見手順を示す．発見手順は，図１中の(a)～(d)の4種類がある．

(a)の手順は，実績ベースで共通故障モードを抽出する手順である．この手順では，蓄積されたFMEAの結果を故障グループ毎に分類し，それらの共通故障モードを導き出す．(a)の手順は，共通故障モードの漏れを防ぐために定期的に実施する．

(b)の手順は，社会的な要求や新たな脅威の出現に対応する共通故障モードを抽出する手順である．前者はDMCSに対する規約や法令が変更となった場合，後者は新しい攻撃手法やウィルスが発見された場合に実施する．これらは，予防的な観点から共通故障モードの検討を実施する．

(c)の手順は，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故障モードを発見した場合の手順である．

(d)の手順は，共通故障モード一覧表を用いてFMEAを実施した結果，新たな共通故障モードを発見した場合の手順である．

表2 共通故障モードの一覧
Table 2 List of Common Failure Modes

グループ	共通故障モード	代表的な故障の例	対策の方針	代表的なリスク低減策
起動	機能の開始条件が揃わない	該当する作業ができない，システムが不適切な状態になる	起動条件の見直し	開始条件確認作業のSOPへの追加(3)，起動可／不可条件設定(4)
			起動時の多重確認	開始条件確認作業のSOPへの追加(3)，起動確認の多重化(4)
			起動確認	起動状態の表示(4)
停止	機能の終了条件が揃わない	該当する作業ができない，システムが不適切な状態になる	機能の停止条件の見直し	終了条件確認作業のSOPへの追加，停止可／不可条件設定(4)
			停止時の多重確認	終了条件確認作業のSOPへの追加，停止確認の多重化(4)
			停止確認	停止状態の表示(4)
			最優先での安全状態への移行	緊急停止機能の追加(4)
入出力	SOPを見間違う	不適切な医薬品が製造される，システムが不適切な状態となる	SOPの多重確認	SOPの二重確認(3)
			SOPの標記を見やすくする	SOPの書式統一(3)
	HMIを見間違う	不適切な医薬品が製造される，システムが不適切な状態となる	HMIの多重確認	HMIの二重確認(3)
			HMIの表示を見やすくする	HMI表示形式の統一(4)
			HMIの内容を確認する	再確認機能の追加(4)
	ものを見間違う	不適切な医薬品が製造される	ものの多重確認	ものの二重確認(3)
	過去のデータを損失する	品質に関わるデータが失われる	データが失われることを知らせる	過去データ損失警告機能の追加(4)
	最新のデータを損失する	品質に関わるデータが失われる	データが失われることを知らせる	最新データ損失警告機能の追加(4)
	入力を誤る	不適切な委託品が製造される，システムが不適切な状態となる	入力データの多重確認	設定データの二重確認(3)
プログラム	想定以上のデータ更新が発生する	データ更新ができない	処理を高速化する	更新処理の高速化(5)
		データ更新ができない	装置を高速化する	記憶装置の高速化(3)
	計算精度の上限確認	不適切な医薬品が製造される	有効桁を増やす	倍精度型変数の利用(5)
	計算精度の下限確認	不適切な医薬品が製造される	有効桁を増やす	倍精度型変数の利用(5)
	ゼロ割をする	作業が途中で停止する	ゼロ割発生を警告する	割り算の除数が小さい場合の警告機能の追加(5)
	想定以上の大量データ受付	プログラム異常停止	データを受け付けない	受付データ制限機能の追加(4)
			データを入力しない	受付可能データ数のSOPへの追記（3）
	想定以上の割り込み発生	プログラム異常停止	割り込みを制限する	多重割り込みの制限（5）
			割り込みを禁止する	多重割り込み制限のSOPへの追記（3）
	想定以上のCPU負荷の発生	プログラムが反応しない，プログラムの反応が遅くなる	想定以上の実行要求をしない	CPU使用率表示機能の追加(5)
			想定以上の実行要求を拒否する	CPU過負荷状態での新規実行要求受付制限機能の追加(5)
校正	機能の校正を行う間隔が長い	誤った計測が行われる，不適切な医薬品が製造される	定期的な見直しを行う	機能の校正を行う間隔を短くする(3)
資格	作業権限の間違い	適切な作業が実施できない，不適切な医薬品が製造される	作業前に確認する	作業前の権限確認(3)
			不適切な権限を設定しない	定期的な権限の見直し(3)
バックアップ	記憶装置の故障	データが消失する，品質に関するデータが失われる	データ保存を多重化する	記憶装置の多重化(3)
			バックアップ間隔を短くする	定期的なバックアップ実施(3)
	バックアップの不備	データが消失する，品質に関わるデータが失われる	適切にバックする	バックアップ手順のSOP化(3)
			バックアップ間隔を短くする	バックアップ間隔の短期化(3)
悪意のある操作や攻撃	重要データの識別がない	データが持ち出される	データを持ち出されないようにする	DLPツールの導入(4)
	データへのアクセス制限がない		データにアクセスできないようにする	ユーザ毎のデータへのアクセス制限を追加する(4)
	データの書き換えができる	データを改ざんされる	データを改ざんできないようにする	電子署名を追加する(4)，タイムスタンプを追加する(4)
	大量データを送りつけられる	該当する作業ができない	データが来ないようにする	外部ネットワークと遮断する(3)
	大量要求を送りつけられる		データを取捨選択する	ファイヤーウォールを設置する(3)
	外部からの不正アクセスされる	システムに侵入される	アクセスできないようにする	外部ネットワークと遮断する(3)
			不正アクセスを発見する	不正侵入検知システムを導入する(3)
				不正侵入予防システムを導入する(3)
	ウィルスが付着したデータを授受する	システムが想定外の動作をする，不適切な医薬品が製造される	ウィルスを除去する	ウィルス除去ソフトを導入する(4)
			ウィルスが侵入しないようにする	ウィルス侵入防御ソフトを導入する(4)
				接続するメモリのウィルス確認の実施(3)

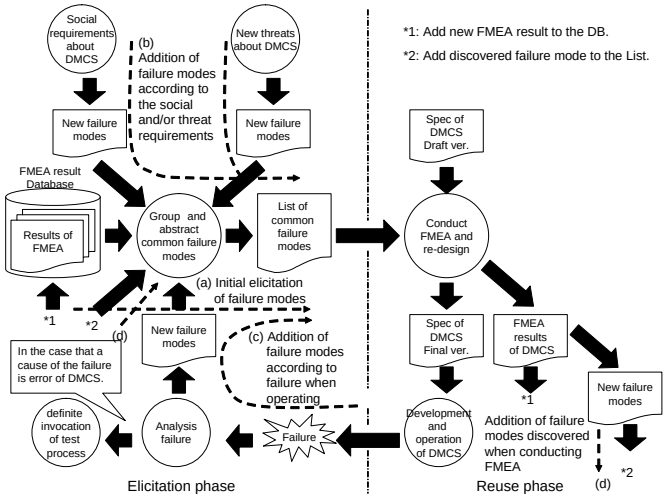

図.1 共通故障モードの発見手順
Fig.1 Detection Process of Common Failure Modes

3. 導出した共通故障モードの適用と評価

作成した共通故障モード一覧表を評価するために, 既存の DMCS に対して試行を行った. 評価は技術者 A が共通故障モード一覧表を用いて FMEA を実施した結果と技術者 B が手順を決めずに FMEA を実施した結果（DMCS 開発時に実施した FMEA の結果）を比較することで行う．なお，技術者 A は 5 件の DMCS の FMEA 実施経験を有する中堅技術者であり，技術者 B は 20 件以上の FMEA 実施経験を有する熟練技術者である．

3.1 赤外分光光度計の DMCS への適用

共通故障モード一覧表を赤外分光光度計のDMCSのFMEAに適用した．このDMCSは，物質から放射されるスペクトルを解析するために用いられる．このDMCSは試料データ入力，スペクトル解析，解析データ出力の機能を有している．DMCSを含めた赤外分光光度計は，メーカーの標準品であり，改造はできない．

以下に技術者AのFMEAの実施結果を示す．

試料データ入力機能の起動と終了の条件が揃わない共通故障モードについては，標準品で改造ができない．さらに, 使用実績も豊富かつ不具合の報告がない．そのため，対象外とした．

SOPを見間違うとものを見間違う共通故障モードについては，不適切な医薬品が製造される可能性がある．従って，重要性は高，発生確率は中，検出確率は高で，リスク優先度は中とした．そしてリスク低減策は，夫々，入力時に試料データを複数回チェックすることとした．これにより，発生確率が低となり，リスク優先度は低となるので，このリスク低減策を採用した．それ以外の入出力に関わる共通故障モードは該当しなかった．

プログラムに関わる故障モード群は，標準品で使用実績が豊富かつ不具合もなく，使用頻度も低いので，対象外とした．校正に関する共通故障モードについては，不適切な医薬品が製造される可能性がある．従って，重要性は高，発生確率は中，検出確率は高で，リスク優先度は中とした．そして，リスク低減策は，使用前に校正を行うこととした．これにより，発生確率が低となり，リスク優先度は低となるので，このリスク低減策を採用した．

作業権限を間違う共通故障モードは，不適切な医薬品が製造される可能性がある．従って，重要性は高，発生確率は低，検出確率は高で，リスク優先度は低とした．そしてリスク低減策は, 作業の前後で作業員の資格を確認することとした. これにより，リスク優先度は変わらないが，発生確率が低下するので，このリスク低減策を採用した．

バックアップに関する共通故障モードは，この赤外分光光度計には内部にデータを保存しておく機能がないため，対象外とした．

ウィルスが付着したデータを授受する共通故障モードについては，機能や計測結果が不適切となる可能性がある．従って，重要性は高，発生確率は低，検出確率は高で，リスク優先度は低とした．そして，リスク低減策は，入力するデータを事前にウィルスチェックすることとした．これにより，リスク優先度は変わらないが，発生確率が低下するので，このリスク低減策を採用した．他の悪意のある操作や攻撃に関する共通故障モードは該当しなかった．

他の機能についても，同様に検討を行った．

表3に赤外分光光度計のDMCSのFMEAの結果（抜粋）を示す．技術者Aの結果とBの結果を比較したところ，Bの結果にはウィルスが付着したデータを授受する共通故障モードに関する検討がなかった．これは，BがFMEAを実施した時点では，制御機器に感染するウィルスが現れていなかったためだと考えられる．それ以外は同様であった．このことから，共通故障モード一覧表は上記DMCSのFMEAに適用できると考えられる．加えて，リスク低減策の漏れ防止に役立つと考えられる．

表3　赤外分光光度計のFMEA結果―抜粋―
Table 3　FMEA Results of Infrared Spectrophotometer　-Extracted-

機能	故障モード	システムへの影響	採択	機能重要性	発生確率	検出確率	リスク優先度	対策
試料データ入力	SOPを見間違う，ものを見間違う	不適切な品質の医薬品の製造	○	高	中	高	中	試料データ複数回チェック(URS・SOP)，RT
				高	低	高	低	
試料データ入力	機能の校正を行う間隔が長い	不適格な者が医薬品を製造	○	高	中	高	中	使用前に校正を行う(URS,SOP)，RT
				高	低	高	低	
試料データ入力	作業権限を間違う	不適切な品質の医薬品の製造	○	高	低	高	低	作業前後に作業員の資格確認(URS,SOP)，RT
				高	低	高	低	
試料データ入力	ウィルスが付着したデータの授受	計測結果が不適切	○	高	低	高	低	入力するデータを事前にウィルスチェック(URS,SOP),RT
				高	低	高	低	

表 4　計量装置の FMEA 結果―抜粋―
Table 4　FMEA Results of Measuring Equipment – Extracted -

機能	故障モード	システムへの影響	採択	機能重要性	発生確率	検出確率	リスク優先度	対策
製造指図データ読み込み	機能の開始条件が揃わない	計量作業が停滞	○	中	中	高	低	開始条件を確認する作業の追加(URS・SOP)，RT
				中	中	高	低	
製造指図データ読み込み	機能の終了条件が揃わない	計量作業が停滞	○	中	中	高	低	終了条件を確認する作業の追加(URS・SOP)，RT
				中	中	高	低	
製造指図データ読み込み	SOPを見間違う，HMIを見間違う，ものを見間違う	不適切な計量，不適切な品質の医薬品の製造	○	高	中	高	中	指図データ複数回確認(URS・SOP)，RT，画面表示結果との比較(URS・SOP)，RT
				高	低	高	低	
製造指図データ読み込み	入力を誤る	不適切な品質の医薬品の製造	○	高	中	高	中	指図の比較(URS・SOP)，RT，計量結果と指図の比較(URS・SOP)，RT
				高	低	高	低	
製造指図データ読み込み	計算精度下限確認	不適切な計量，不適切な品質の医	○	中	低	高	低	除数が小さい場合の警告機能の追加(URS・FS・DS・MS)，(RT・FT・IT・MT)
				中	低	高	低	
製造指図データ読み込み	機能の校正を行う間隔が長い	計測結果に誤差が生じる	○	高	中	高	中	使用前に機器の校正を行う(URS・SOP)，RT
				高	低	高	低	
製造指図データ読み込み	作業権限を間違う	不適切な品質の医薬品の製造	○	高	低	高	低	作業前後に資格の確認を行う(URS・SOP)，RT
				高	低	高	低	
製造指図データ読み込み	バックアップの不良	データ損失	○	高	低	高	低	データ読み込み直後のバックアップ実施(URS・SOP)，RT
				高	低	高	低	
製造指図データ読み込み	ウィルスの付着したデータの授受	不適切な計量	○	高	低	高	低	入力データの事前ウィルスチェック(URS・SOP)，RT
				高	低	高	低	

3.2 計量装置の DMCS への適用

共通故障モード一覧表を原材料の計量装置のDMCSのFMEAに適用した．このDMCSは個別開発されたものである．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，計量結果印刷をする機能を有している．

以下に技術者AのFMEAの実施結果を示す．

製造指図データ読み込み機能の開始と終了の条件の揃わない共通故障モードについては，計量作業が停滞する可能性がある．従って，重要度は中，発生確率は中，検出確率は高で，リスク優先度は低とした．そして，リスク低減策は開始と終了の条件を確認することとした．これにより，リスク優先度は変わらないが，停滞する時間が短縮するので，この対策を採用した．

SOP/HMI/ものを見間違う共通故障モードは，不適切な指図に基づいた計量が行われると医薬品の品質に影響を与える可能性がある．従って，重要性は高，発生確率は中，検出確率は高で，リスク優先度は中とした．そして，リスク低減策は，入力する製造指図データを複数回チェックすること，入力された製造指図データと装置の画面に表示された製造指図データを比較チェックすることとした．これにより，発生確率が低となり，リスク優先度は低となるので，このリスク低減策を採用した．

入力を誤る共通故障モードは，製造指図データを間違えることで誤った作業が行われて医薬品の品質に影響を与える可能性がある．従って，重要性は高，発生確率は中，検出確率は高で，リスク優先度は中とした．そして，リスク低減策は，入力する製造指図を複数回チェックすること，計量結果に印刷された製造指図と元の製造指図との比較チェックすることとした．これにより，発生確率が低となり，リスク優先度が低となるので，このリスク低減策を採用した．それ以外の入出力に関する共通故障モードは該当しなかった．

計算精度の下限確認とゼロ割をする共通故障モードは，計量値が小さい場合に発生する可能性がある．従って，重要度は中，発生確率は低，検出確率は高，リスク優先度は低とした．そして，前者のリスク低減策は倍精度型変数を使用すること，後者のリスク低減策は除数が小さい場合の警告機能を追加することとした．前者は既に倍精度型変数が用いられていたため，採用しなかった．後者は，リスク優先度は変わらないが，検出確率が向上し，原因分析に役立つので，採用した．これ以外のプログラムに関する共通故障モードは該当しなかった．

機能の校正に関する共通故障モードについては，計量結果に誤差が生じると不適切な医薬品が製造される可能性がある．従って，重要性は高，発生確率は中，検出確率は高で，リスク優先度は中とした．そして，リスク低減策は，使用前に機器の校正を行うこととした．これにより，発生確率が低となり，リスク優先度は低となるので，このリスク低減策を採用した．

作業権限を間違う共通故障モードについては，不適切な医薬品が製造される可能性がある．従って，重要性は高，発生確率は低，検出確率は高で，リスク優先度は低とした．そしてリスク低減策は，作業前後に作業員の資格を確認することとした．これにより，リスク優先度は変わらないが，発生確率が低下するので，このリスク低減策を採用した．

バックアップに関する共通故障モードは，入力された指図データが損失して医薬品の品質に影響を与える可能性がある．従って，重要性は高，発生確率は低，検出確率は高で，リスク優先度は低とした．そして，リスク低減策は製造指図データ読み込み直後にバックアップをとることとした．これにより，リスク優先度は変わらないが，発生確率が低下し，検出確率も向上するので，このリスク低減策を採用した．

ウィルスが付着したデータを授受する共通故障モードについては，計測結果が不適切となり，医薬品の品質に影響を与える可能性がある．従って，重要性は高，発生確率は低，検出確率は高で，リスク優先度は低とした．そして，リスク低減策は，入力

するデータを事前にウィルスチェックすることとした．これにより，リスク優先度は変わらないが，発生確率が低下するので，このリスク低減策を採用した．他の悪意のある操作や攻撃に関する共通故障モードは該当しなかった．

他の機能についても，同様に検討を行った．

表4に計量装置のDMCSのFMEAの結果（抜粋）を示す．技術者Aの結果とBの結果とを比較したところ，Bの結果にはプログラムの動作とウィルスが付着したデータを授受する共通故障モードに対する検討がなかった．前者はBの検討漏れ，後者は赤外分光光度計のDMCSと同様の理由であった．それ以外は同様であった．このことから，共通故障モード一覧表は上記DMCSのFMEAに適用できると考えられる．加えて，検討すべき故障モードの漏れを防止する効果があると考えられる．

3.3 総合評価

上記の適用の結果，中堅技術者Aが実施したFMEAの結果は，熟練技術者Bが実施したFMEAの結果とほぼ同じであった．このことから，作成した共通故障モード一覧表を使用してFMEAを実施することで，経験の多くない技術者であっても，熟練技術者と同等のFMEA結果を導くことができることが分かった．さらに，共通故障モード一覧表を用いてFMEAを実施することで，FMEA時に故障モードの列挙し忘れを防止する効果があることが分かった．

また，2.3で述べた新しい故障モードを発見する手順を定期的に実行することで，最新の共通故障モード一覧表を維持することができる．最新の故障モード一覧表を用いてFMEAを実施することで，より安全なDMCSを実現できるようになるものと考えられる．

4. おわりに

本論文では，DMCSに共通で適用できる故障モードの一覧を作成し，それを用いてFMEAを実施することで，技術者の能力や経験に左右されずにFMEAを実施できるようにした．さらに，故障モードを列挙し忘れるといったトラブルを防止できるようにした．この結果，DMCSの網羅的な安全化の対策を実現できるようになった．

今後は，プログラムレベルまで一貫して実施することのできるFMEA手法について検討する．併せて，提案手法を様々なDMCSに対して適用し，その結果をもとに共通故障モード一覧表を充実させていく．

謝辞

本研究は日本学術進行会科学研究費補助金基盤研究(C)，課題番号21500439「医薬品晴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) IPSE GAMP Japan Forum: リスクベースアプローチ実施ガイド, IPSE 日本支部 (2006)
2) 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，pp.461-486 (1990)
3) 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，pp.467-475 (1990)
4) 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, Vol.2009-SE-166No.12 (2009)
5) 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, Vol.99, Feb, pp.107-121，日刊工業新聞社(2009)
6) 塩見，岡島，石山, FMEA, FTA の活用，日科技連(1983)
7) 原子力安全基盤機構, JNES の人的・組織的要因分析について,原子力安全委員会事故・故障情報活用 WG(第 7 回) (2006)
8) Eric Luiijif, SCADA Security Good Practices for the Drinking Water Sector,TNO Report, TNO Defense, Security and Safety (2008)