

CAST HANDBOOK:

How to Learn More from Incidents and Accidents

日本語版 Ver.0.1

Nancy G. Leveson

Translators

Seiko Shirasaka / KEIO Univ.
Masa Katahira, Naoki Ishihama, Keichi Wada, Yasushi Ueda, Hiroki Umeda, Naoko Okubo, Nico Watanabe / JAXA
Ai Noumi / Sophia Univ.
Tomoko Kaneko / National Institute of Informatics
Yuko Fukushima / Nihon Unisys

COPYRIGHT © 2019 BY NANCY LEVESON. ALL RIGHTS RESERVED. THE UNALTERED VERSION OF THIS HANDBOOK AND ITS CONTENTS MAY BE USED FOR NON-PROFIT CLASSES AND OTHER NON-COMMERCIAL PURPOSES BUT MAY NOT BE SOLD.

罪のない人々が殺される事故は悲劇的だが、そこから学ばない方が悲劇的である

An accident where innocent people are killed is tragic, but not nearly as tragic as not learning from it.

序文

約15年前、ある企業が所有する製油所の大事故を調査した際に、同社の別の大規模な製油所を訪れていました。安全エンジニアリンググループの責任者が、毎年何百件もの事故が発生している際に、どのインシデントや事故を調査するかをどのように決定できるかと私に尋ねました。私は彼に、それは間違った質問であると答えました：いくつかの事故をより深く調査していれば、何百もの事故は起きなかったでしょう。彼は私の提案を理解しなかったか、少なくとも受け入れてはいなかったと思います。このハンドブックの目的は、その答えを説明することにあります。つまり、私たちは、インシデント（incident）や事故（accident）から十分に学ぶことができていないということです。本当に損失（loss）を大幅に減らしたいのであれば、もっと学ぶ方法を理解する必要があります。

システム安全の分野で働き、いくつかの重大な事故（スペースシャトルコロンビア、ディープウォーター・ホライゾン、テキサスシティ）の事故報告書を作成した後、私は、すべての事故に共通する多くの要因を発見しました。驚いたことに、これらは公式の事故報告書に原因として含まれていないことがよくあります。CAST （システム理論に基づく原因分析（Causal Analysis based on System Theory））とこのハンドブックは、将来の損失を防ぐために、より良い仕事をするために、他の人々が事故からより多くのことを学ぶのを助けるために、私の経験を利用する試みです。

このハンドブックでは、事故調査中に尋ねる必要がある質問を識別し、事故が発生した理由を決定するためのCAST（システム理論に基づく因果分析）と呼ばれる構造化されたアプローチについて説明します。CASTは、非難しようとしないという点で、事故分析に対する現在のアプローチとは大きく異なります。分析の目的は、代表的な失敗（failure）の探索ということから、事象（event）を防止するためのシステムや構造（structure）が成功しなかった理由を探すことに変わります。推奨事項（recommendations）は、調査で学んだことに基づいて、これらの予防（コントロール（control））構造を強化することに焦点を当てています。

CASTを実行する最良の方法は、実際の事故についてこれらの分析を行った私の経験によって進化しました。私たち全員が、事故分析に対するこのシステムアプローチについて学ぶにつれて、ハンドブックは更新され、より多くのテクニックが提供されるようになるでしょう。

Acknowledgements:
I would like to thank several people who helped to edit this handbook: Dr. John Thomas, Andrew McGregor, Shem Malmquist, Diogo Castilho, and Darren Straker.

謝辞:
日本語版作成にあたり、以下の皆様のご支援に感謝申し上げます。

慶應義塾大学	白坂成功
宇宙航空研究開発機構	片平真史 石濱直樹 和田恵一 植田泰士 梅田浩貴 大久保梨思子 渡邉にこ
上智大学	能美亜衣
国立情報学研究所	金子朋子
日本ユニシス(株)	福島祐子

目次

第１章:序章 6
第２章：基本的な用語から始める 9
第３章：なぜ私たちは事故やインシデントから十分学べないのか？ 12
後知恵バイアス 14
非難は安全の敵 18
不適切な事故因果関係モデルの使用 23
改善された事故分析手法の目的 33
第４章：CAST分析の実施 34
CASTの基本コンポーネント 34
基本情報の収集 36
コントロール対象のプロセスにおいて発生したことの理解 42
安全コントロールストラクチャーのモデル化 46
各コンポーネントに対する分析：なぜコントロールが有効でなかったのか？ 55
全体としてのコントロールストラクチャーの分析 76
安全コントロールストラクチャーに対する推奨事項と変更の生成 90
CASTの結果を形式化するための提案 92
第５章：職場と社会的な事故におけるCASTの利用 98
職場の安全 98
社会的損失の分析へのCASTの利用 104
2008年の金融危機の例 115
第６章：組織や業界へのCASTの導入 118
付録Ａ：実際の事故に対するCAST分析の公開事例へのリンク 120
付録Ｂ：シェル ムールダイク損失の背景情報とCAST分析の概要 123
付録Ｃ：事故原因の腐ったリンゴ理論 134
付録Ｄ：損失における安全コントロールストラクチャーの役割を評価する際に考慮すべき要素 137
付録Ｅ：非エンジニアのための工学とコントロールの基本的概念 141

図目次

図 1：根本原因の誘惑はどこにもつながりません。 12
図 2：モグラ叩きゲーム 13
図 3：後知恵バイアスの図解 14
図 4：手順に従うジレンマ 17
図 5:事故説明の二つの相対する観点 20
図 6：ハインリッヒのDominoモデル、1932 24
図 7：リーズンのスイスチーズモデル 24
図 8：システム理論における創発特性 28
図 9：コントローラは、振る舞いに制約を強制する 28
図 10：一般的な安全コントロールストラクチャー 30
図 11：安全コントロールストラクチャーの基本コンポーネント 31
図 12：シェル ムールダイク爆発 36
図 13：シェル ムールダイクの非常に上位レベルでの安全コントロールストラクチャーモデル 48
図 14：シェル ムールダイクの安全コントロールストラクチャーの詳細 50
図 15：シェル ムールダイク化学プラントの安全コントロールストラクチャー 60
図 16：ユーバーリンゲン事故における理論的なコミュニケーションリンク 78
図 17：事故時の運用のコミュニケーションリンク 79
図 18：レキシントンでのコムエアーの誤った滑走路事故の安全コントロールストラクチャー。コントロールは上から下ではなく左から右に描画されます。点線は、損失の原因となったフィードバックとコミュニケーションの欠如を表しています[Paul Nelson, A STAMP Analysis of the LEX Comair 5191 Accident, Master’s Thesis, Lund University, June 2008.この論文へのリンクは付録Ａにあります。] 80
図 19：シャインの組織文化モデル 84
図 20：カナダ オンタリオにおいて水質をコントロールするために当初デザインされていたコントロールストラクチャー 96
図 21：水質汚染事象の際のコントロールストラクチャー 97
図 22：米国における製薬の安全コントロールストラクチャー 107

第１章:序章

このハンドブックはレシピ本のように手順を追って説明していくものではなく、専門家が事故原因を慎重に且つ深く考えるための方法を提供するものです。手順を追って説明するものからでは、残念ながら最良な結果は得られません。我々に必要なのは、通常より広くまた深く原因調査ができるようなツールなのです。

これまでも事故に対する表面的な調査は行われてきましたが、調査結果から得られることは少なく、同様の事故が発生しその度に表面的な調査が行われるということが繰り返されてきました。それよりも、各事故から十分に学ぶために必要な時間と労力を投資することにより、損失を大幅に削減し、将来の調査が少なくて済むようにすることを目的にする必要があります。

なぜ新しい事故分析ツールが必要なのか？

結論から先にお伝えすると、我々は損失やニアミスから思っていたほど学習できていないというのが現状です。これまで多くの事故分析ツールが作られてきましたが、大半が古いものを新しい表記方法で文書化することに焦点を当てているだけで、実際のシステムにおける事故を大幅に減少させたものや広く使用されているものはほとんどありません。

このテーマを学術的かつ哲学的に扱う場合には、私の論文「learning from events（事象から学ぶ）」[1]と、私の著書「Engineering a Safer World」[Leveson 2012]をお勧めします。Engineering a Safer Worldをお読みいただくことで、現在の事故分析手法とその前提（assumption）の限界、およびCASTの技術的・哲学的基盤をより深く理解することができます。

しかし、このハンドブックの目的はそこではなく、調査員や分析者が事故報告書を改善するのに役立つ実用的な手順を提供することです。事故調査は１～２つの要因、通常はオペレータのミスに焦点を当てすぎてしまい、最も重要な要因を見逃してしまうことが多々あります。このように因果関係を単純化し過ぎると、人を変えて同様の事故が繰り返されることとなります。損失ごとの症状が異なるように見えてしまい、共通の根本原因としていないがために、終わりの見えない消火活動のような状態が続いてしまいます。

学習内容

ハンドブックにより、事故調査と分析からより有益な結果を得る方法を学べます。このアプローチを使用し始めてしばらくは事故分析に時間を費やすことになるかもしれませんが、CASTの使用開始時にモデリングや分析に費やした労力の大半は、後の調査に再利用することが出来ます。短期的には、将来の事故調査に費やす時間短縮だけでなく、事故の減少、ひいては調査の減少においても正味の長期的利益を得ることで、努力の量は大幅に削減されるはずです。経験を積んだ事故調査担当者は、CASTの使用によって、早期にすべき質問が作成され、後戻りをしなくても済むようになるため、解析作業が迅速になることを発見しました。

長期的な目的は、事故を防止するために用いられるコントロールの全体的な有効性を高めることであるべきです。これらのコントロールは安全管理システム（Safety Management System（SMS））に組み込まれることが多々あります。事故を調査し、学んだ教訓を生かすことは効果的なSMSの重要な部分です。同様に、徹底した事故/インシデントの分析プロセスを通じて、SMS自体の現在の弱点が特定されます。このプロセスへの投資は莫大な収益をもたらします。対照的に、組織または業界で事故が発生している理由の表面的な分析は、主に

[1] Nancy Leveson, Applying Systems Thinking to Analyze and Learn from Events, Safety Science, Vol. 49, Issue 1, January 2010, pp. 55-64.

リソースの浪費であり、将来の事象にはほとんど影響しません。

事実、多様な産業においても事故の体系的な（systemic）要因は極めて類似している傾向があります。私は航空、石油・ガス、宇宙、その他の分野における事故の調査と原因分析に携わり、また、これらの業界やその他のほとんどの業界における数百件の事故報告書を調査してきました。産業によって症状こそ異なるかもしれませんが、基本的な事故の要因は著しく類似しており、また事故報告書の省略化と単純化のタイプも非常に似ています。要するに、意欲とツールがあれば、過去の学習から改善を図れるのです。共通する体系的な損失の要因を特定するCAST分析の結果を共有することで、自らが損失を受けることなく他者から学習することがでます。

STPA HANDBOOK [Leveson and Thomas、2018年]では、効果的な安全管理システムの構築など、事故を未然に防止するための取り組みを紹介しています。しかし、事故やニアミスが発生する可能性は依然としてあり、高度で包括的な事故/インシデント分析は、あらゆる損失防止プログラムの重要な要素です。SUBSAFEと呼ばれる米軍原子力海軍プログラム（*Engineering a Safer World* 第14章を参照）を除いて、いずれの安全プログラムも、長い間すべての事故を無くすことはできていません。SUBSAFEは、考慮されるハザードの種類を厳しく制限する（例えば、潜水艦の船体が損傷して浮上不能となり、港に戻ることができなくなる）、制限され、厳格にコントロールされた領域内で動作する、逆戻りや時間の経過とともにリスクを増大させるその他の要因を防ぐためにかなりのリソースと労力を費やす、といったいくつかのユニークな特徴があります。

しかし、たとえ完璧な損失防止プログラムを作ったところで、世界は絶えず変化しています。変化の中には、意図的で制御可能なものもあれば、そうでないものもあります。つまり、システム自体も経年変化し、利用行動、システム運用環境も変化していきます。うまくいけばハザードの増加を示す主な指標（STPA HANDBOOK 第6章を参照）を調べ、CASTを用いてニアミスやインシデントを徹底的に調査することによって非安全な（unsafe）変更を検出することで、損失が生じる前に計画外の変化を特定し、対処することが可能になります。

このハンドブックではいくつか提案が記述されていますが、使用しなければならない形式や表記があるというわけではありません。異なる事故の要因は、それぞれの方法で最もうまく説明され、解釈されているでしょう。しかし、結果の内容に違いがあってはいけません。このハンドブックの目的は、より包括的で有用な結果につながる因果関係について考えるプロセスを記述することです。これらのアイデアを適用することで、それぞれの目的や産業に最も効果的な結果を提示するためのフォーマットを作成することが可能です。

CASTとは何か？

このハンドブックで教示されている原因分析アプローチをCAST（システム理論に基づく原因分析）と呼びます。STPA[Leveson 2012, Leveson and Thomas 2018]と同様に、対象とする損失は、人命の損失や典型的な安全またはセキュリティ上の事故である必要はありません。実際、ステークホルダーが回避しようとする損失につながる望ましくない事象の原因理解のために使用することができます。例としては、経済的損失、環境汚染、ミッションの損失、企業の評判の低下、基本的に回避すべき資源の投資を正当化するようなあらゆる結果などがあります。また、学んだ教訓から、類似したあるいは同様の原因による将来の損失を防止することができる変更を加えることが可能です。

最終目的は将来の損失を回避する方法を学ぶことであり、特定された要因を恣意的な「根本原因（root cause）」に簡素化すべきではなく、あらゆる事故からできるだけ多くを学ぶことです。CASTはこの目的達成のために設計されています。事実、事故調査官の中には、CASTによって損失要因に関する情報が過多だと不満を述べる者もいますが、簡単な説明が最終目的なのでしょうか。それとも、全ての要因分析からできるだけ多くのことを学ぼうとすべきなのでしょうか。一度に一つの教訓だけを学び、事故が起きるたびに損失を被るこ

とは、合理的な行動ではありません。事故報告書では体系的な要因がしばしば省略されることがあり、その結果、最も重要で広範囲にわたる要因が無視され、修正が行われません。特定された要因を制限したり単純化し過ぎることは、事故調査における時間と経費の節約にはなりません。「根本原因」と「想定原因（probable cause）」の概念は、責任を負う誰かまたは何かを見つけて、次の事故まで生活とビジネスを続けるための一般的な方法です。最も重要なのは、今払うのか、つけを将来にまわすのかということです。

CASTとSTPAの関係

ハザード分析は、「事故が起こる前に調査すること」と言われています。STPA（システム理論プロセス分析）は、CASTと同様の強力な因果関係モデルに基づくハザード分析ツールですが、CASTとは異なり、発生したシナリオだけでなく、損失につながる可能性のあるすべての潜在的なシナリオを特定することができます。STPAによって作成されたこれらの潜在的なシナリオは、事故が発生する前に事故を予防するために使用することができます。これに対してCASTは、発生した特定のシナリオのみを特定するのに役立ちます。互いに目的は異なりますが密接に関係しています。

STPAは、事故の概念開発段階の初期（設計を作成する前）で使用できるため、システムの安全性とセキュリティを早期から行えることで、安全性とセキュリティの設計コストを大幅に削減することが可能です：潜在的な安全性やセキュリティの欠陥を設計の遅い段階で見つけると開発コストが非常に大きくなってしまいます。過去の事故のCAST分析は、更なる損失を防止するために除去または制御する必要があると思われるシナリオを特定することで、STPAプロセスを支援することができます。

このハンドブックの構成と使用方法

このハンドブックは、我々が事故からできる限りの多くの事を学べていない理由についての短い説明から始まり、次にCAST分析を行う目的とプロセスについて説明しています。説明のなかでは、オランダにおける化学プラント爆発の実例が、使用されていますが、この事故の要因は多くの事故と類似しています。CAST分析のその他の例は、*Engineering a Safer World*やPSASのWebサイト （http://psas.scripts.mit.edu）にあります。付録Ａには、さまざまな業界のCAST分析へのリンクがありますのでご参照ください。

エンジニアリング（engineering）の安全と職場の安全の世界は、関係する人々と安全性を高めるために用いられるアプローチの両方に関して、不必要に分離される傾向があります。実際はこの分離は不要であり、職場の安全性の向上を阻害しています。このハンドブックには、CASTを職場（個人）の安全に適用する方法に関する章が含まれています。

CASTおよび構造的な事故分析の方法は、主に物理的なシステムを含む事故に対して提案され、適用されてきましたが、CASTは、大きな混乱や人命の損失または金融システムの損失を伴う社会的なシステムの「事故」に対して非常に効果的に使用できます。第5章では、市場から撤退する前に深刻な身体的被害をもたらした処方疼痛管理薬（バイオックス（Vioxx））と、2008年の金融システム崩壊におけるベアー・スターンズ投資銀行（Bears Stearns investment bank）の破綻を例として挙げています。

まとめると、CASTの使用例や基礎となる哲学的な論文は発表されていますが、現状ではCAST分析を行う方法についての詳細な説明やヒントはありません。このハンドブックの目的は、その空白を埋めることです。

CASTは基本的なエンジニアリング概念に基づいています。エンジニアリングの経験がない読者のために、付録Ｅでは、このハンドブックを理解してCAST分析を実行するために必要な情報を提示していますので参考にしてください。

第２章：基本的な用語から始める

「私が言葉を使う時には、言葉は私の選んだとおりの意味になるのである―それ以上でも以下でもない。」と、ハンプティ・ダンプティはちょっと軽蔑的な口調で言いました。「問題は、言葉に様々な意味を持たせることができるかということよ。」アリスは言いました。ハンプティ・ダンプティは「問題は、どちらがご主人様かってことだ。単にそれだけの話。」と返しました。

ルイス・キャロル（チャールズ・ドジソン）

鏡の国のアリス　1872年初版

重要でエキサイティングな話題について話すには、定義から始めるのはかなりおもしろみのない方法ですが、さまざまな業界やグループで確立された共通の単語の異なる定義によって、コミュニケーションが妨げられることがしばしばあります。ですが、共通の用語は多少必要となるだけで、この章はとても短いので特に心配はありません。

ハンプティ・ダンプティ（正確にはチャールズ・ドジソン）がうまく表現しているように、ここで確立された定義は、世界を変えようとする試みではなく、このハンドブックの使用に適用するためのものとしています。共通の語彙なくしては、コミュニケーションは成り立ちません。

事故（*時にミスハップ（Mishap）と呼ばれる*）：損失につながる望ましくない（undesired）、許容できない（unacceptable）、計画外の（unplanned）事象。手短に言えば、単なる損失のこと。

望ましくない事と許容できない事とは、システムのステークホルダーが判断する必要があります。ステークホルダーが多くいる可能性があるため、一部の方にとっては損失事象が望ましくない、または許容できないものであった場合、その事象は事故（ミスハップ）とされます。損失が望ましく、許容できるものであると考える方々には、いずれにしてもそれを防ぐことには関心がないのでしょうから、このハンドブックはさほど重要ではないかと思います。

業界や組織によっては、事故をもっと狭く定義しているところもありますが、この定義はとても一般的なものであることということに注意してください。例えば、事故は、人の死亡または負傷のみに関連するものとして定義される場合があり、その他には機器や資産の損失などがありますが大半がそこまでとなっています。一方、上記の定義にはステークホルダーが含めることに同意した事象を入れることができます。たとえば、損失には、ミッションの損失、環境汚染、ビジネスへの悪影響（名誉の毀損など）、製品の発売の遅れ、法的な問題などが含まれる場合があります。定義を広く持つことによって、より大規模な問題に対処できるという利点があるので、本書で述べた事故分析のアプローチは、あらゆる種類の損失の原因分析に適用できます。

また、事象を意図しないものに限定する定義はないという点にも注意が必要です。意図的なものであった場合、安全性とセキュリティの両方が定義に含まれています。一例として、事象が、弁を開くことで損失につながる条件下で弁を開く人間のオペレータまたは自動コントローラーを含む原子力発電所を考えます。この損失は、アクションが意図的であったかどうかに関係なく同じ損失であり、CASTを使用すればその要因を特定することができます。

上記の事故定義の汎用性はシステムの目的（goal）と制約（constraint）の基本概念から導かれます。システムの目的は、化学物質の製造、乗客や貨物の輸送、戦争遂行、病気の

治療など、システムが作られた基本的な理由に由来しており、システムの制約は、それらの目的を達成するための許容可能な方法であると定義されています。例えば、輸送システムが移動中に乗客に怪我を負わせることは通常許容されない、といったことです。また、短期的な利益を上げながらも、企業の評判を損ねてしまうといった事象も、ステークホルダーに受け入れられないでしょう。

まとめると：

システム目的: システムを最初に作成した理由
システム制約: 目的を達成するための許容可能な方法

ここで、制約と目的とで矛盾が生じる可能性があるということに注意をしてください。システムエンジニアリング（system engineering）における重要な第一のステップは、システム設計と運用に関する意思決定に使用される目的と制約、および許容可能なトレードオフを特定することです。これらの定義を使用すると、システムの信頼性（reliability）は明らかにシステムの安全性やセキュリティと同義ではありません。システムは確実に目的を達成する一方で、危険であったり、不安定であったり、または逆であったりする場合があります。例えば、化学プラントは化学物質を生産すると同時に、周囲を汚染して人に害を与える毒素を放出することがあります。これらの定義は、信頼性が場合によっては安全性と矛盾する理由も説明しています。システムが「失敗（failed）」したというステートメントでは、何が起こったのか、あるいはどんな目的や制約に違反したのかを理解するのに十分な情報を示していません。

また、さらに２つの定義が必要とされます。一方は単純で、もう一方は少し複雑です。１つは、インシデントまたはニアミス（near-miss）の定義です。

インシデントまたはニアミス：損失にはならないが、異なる条件または異なる環境で発生する可能性のある、望ましくない、許容できない、計画外の事象

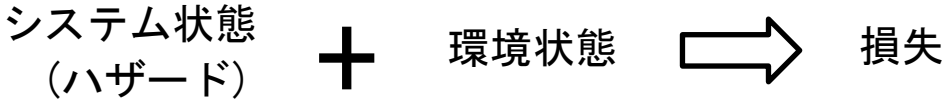
CASTで定義し、使用する必要がある最後の用語は、*ハザード*（hazard）または*脆弱性*（vulnerability）です。前者は安全性のために使われ、後者はセキュリティのために使われますが、基本的には同じことを意味します。簡単に言うと、脆弱性とは攻撃を受けやすい状態にあるシステムの欠陥（flaw）、ハザードとは事故や損失につながるシステムの状態（state）のことを言います。より正式で慎重な定義は、以下になります:

ハザードまたは脆弱性：特定の環境条件とともに、事故または損失につながる可能性のあるシステム状態または一連の条件.

例えば、航空機を空中で保つのに十分な推進力を持たない航空機や、化学物質を環境中に放出している化学プラントなどがハザードとされます。どちらも事故は避けられないものではありません。航空機は地上にいるか、安全な着陸のために滑空できるかもしれませんし、化学物質は、居住地域に吹き込む風がない際に放出され、単に大気中に放散されるだけかもしれません。いずれの場合も、損失は発生していません。[2]

損失は、ハザードであるシステム状態と環境状態の組み合わせによって発生します。

[2] 化学物質の廃棄を化学プラントの損失の定義に含まれなければならず、つまりハザードは化学物質が放出され廃棄される状態にある化学プラントであると主張する方もいるかもしれません。



エンジニアリングでは「ハザード」という用語の導入が重要です。エンジニアやシステム設計者、システムオペレータは、システムをコントロール下に置くのであって、環境をコントロールするわけではありません。目的はハザードを防止することであるため、ハザードの発生が誰かのコントロール下にある場合にのみ目的達成が可能となります。設計者は、化学プラントを設計する際に、化学物質が環境に放出された時に風がどう吹くかをコントロールすることはできません。彼らとオペレータが唯一できることは、システムの設計またはオペレーションを通して、言い換えると、システムのハザードまたは状態をコントロールすることによって、放出自体を防止しようとすることです。航空交通管制システムは、航空機が潜在的に危険な気象状態にある地域に進入するかどうかをコントロールすることは可能ですが、航空機がその地域に進入した場合に落雷に見舞われるかどうかについてはコントロールできません。航空機の設計者は、航空機の設計に落雷からの保護を含めるかどうかのコントロールはできますが、航空機が落雷を受けるかどうかはコントロールできません。したがって、システムハザードを特定する際には、特定の環境条件において、自分たちのコントロール下で事故につながる可能性のあるものについて考えてみてください。もしそのような環境条件がなければハザードはないということです。[3]

それでは、さらに掘り下げていきましょう。

[3] ある分野では、システムエンジニアリングとは異なる「ハザード」を定義しています。例えば航空の場合、飛行機にとって山がハザードとされることがあります。エンジニアリングの目的は危険の排除や制御にあり、山はたいていの場合除去することは出来ないので、飛行機の設計者と操縦者が制御できるのは山から離れることです。そのため、ハザードは危険な地形での最小分離基準に反するものとして定義されます。

第３章：なぜ私たちは事故やインシデントから十分学べないのか？

“学習体験とは、『あなたは自分がやったことを知っていますよね？そんなことはしないでください』と言うものの一つです”

Douglas Adams, *The Salmon of Doubt*, William Heinemann Ltd, 2001.

私達が事故原因分析を行い、事象から学ぶ際の方法には、多くの制約があります。次の５つが最も重要になるでしょう：根本原因の誘惑（seduction）と原因説明の過剰な単純化、後知恵バイアス（hindsight bias）、ヒューマンエラーを表面的に取り扱う、非難に焦点を当てる、そして今日の世界に適合しない因果関係のモデルを利用すること。

根本原因の誘惑と原因の過剰な単純化

人間は、損失に対して簡単で単一の原因、または非常に数が限られた原因を探すという、心理的な要求があるように見えます。ジョン・キャロルはこれを「根本原因の誘惑」と呼んでいます。私達は、複雑な問題に対して、シンプルな回答を欲します。これは、損失に対する対応を容易に考案できるだけでなく、制御可能な感覚を提供します。もし私達が１つまたは数個の簡単に修正できる原因を識別できたなら、「問題解決」ができ、私達の注意を他の懸念事項に移すことができます。

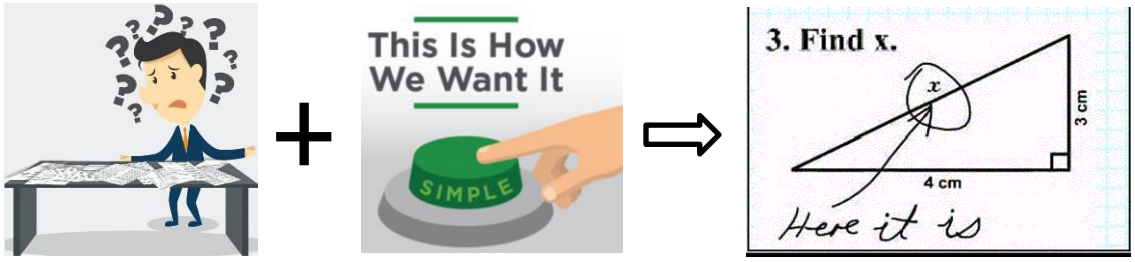


図 １：根本原因の誘惑はどこにもつながりません。

根本原因を探し当てたことに成功したという主張は、問題が解決されずに将来事故が発生する結果となります。我々は、症状や問題は修正するが、これらの症状が発生する体系的な原因やプロセスには取り組まないという、継続的な消化活動モードに結局行き着きます。我々はしばしば、洗練された「モグラ叩きゲーム」を行い、なぜ損失が継続的に起こるのかについて理解しません。膨大なリソースが費やされますが、投資の回収はほとんどありません。



図 2：モグラ叩きゲーム

ここでは、原因の過剰な単純化が不要な事故につながったいくつかの例を示します。1979年にシカゴ・オヘア空港におけるアメリカン航空DC-10の墜落では、米国の国家運輸安全委員会（NTSB）は、翼が破損した時にスラットが格納する設計誤りについては言及せず、「整備が誘発した亀裂」だけのせいにしました。この省略により、マクドネル・ダグラスは設計を変更するようには求められず、同様の設計誤りに関連するさらなる事故が引き起こされました。

1974年6月、英国フリックスボローでの化学プラントでの爆発は、化学反応炉が亀裂を修復するために取り除かれ、その代替として、一時的なパイプが使われました。亀裂自体は、あまり考えられていないプロセス変更による結果でした。（反応炉を）バイパスするパイプは適切に設計されておらず（ただ１つの図面は作業場でのスケッチだけ）、また適切に固定されていませんでした（足場にかかっていた）。応急処置のバイパスパイプは壊れ、死者28名、敷地を破壊した爆発となりました。事故調査官達は労力の大半を、２つのパイプのうちどちらのパイプが先に破裂したのかを決定することに使いました。英国調査委員会は、「この災害は、いくつもの不運な設計中の誤りと、修正の適用によって偶然引き起こされた。」（バイパスパイプのこと）そして、「このような誤りの組合せは、今後繰り返される可能性は極めて低い」結論づけました。[245]。

しかしながら、パイプの破裂はこの事故の原因の小さな一部だけであることは明らかです。完全な説明と、このような損失を将来防ぐには、理解が求められます。例えば、フリックスボローのプラントを稼働するための管理体制は、認定されたエンジニアがおらず、認定されていない者が適切に安全性を評価することなく、重要な技術的修正を加えることを許していました。そして同様に、大量の危険な化学物質をプラント内の潜在的に危険なエリアの近くに格納していました。事故を調査していた英国調査委員会は「安全手順に関する日常的な運用に欠点があったことは明らかだが、災害やその結果に影響を与えるものはなかった。我々はこれらのことに多くの時間をとらない。」と驚くような結論を出しました。幸運なことに、その他の者はこの過剰に狭い視野を無視したため、フリックスボローは、英国において危険な施設が運用される方法に、大きな変化をもたらしました。

多くのケースで、このモグラ叩きアプローチは、全てを深く調査できないほど多くのインシデントを発生させており、いくつかのうわべだけの分析が試みられます。もし代りに、いくつかが深く調査され、体系的な要因が修正されれば、インシデントの数は桁違いに減少するでしょう。

業界によっては、事故が継続的に発生している時、その事故は避けられないもので、事故を避けるためにリソースを提供することは良い投資でないという結論に行きつくことがあります。シーシュポス（Sisyphus）のように、再度底まで落下することが避けられないのに、最終的に諦めるまで大きな岩を丘に転がし上げるような気持ちになり、より良い事故統計を持つ他の業界よりも彼らの業界が危険である決断し、事故は生産性の代償だと結論づけています。悪循環に陥っている者と同様に、この場合は、原因説明の過剰な単純化をやめて、いくつかの根本原因を探すことを超えて答えの探索を拡大させることにより、循環を断ち切ることが解決策になります。

事故は常に複雑かつ多因子的です。ほとんどいつも、物理的な故障または設計に欠陥がある物理的な機器、損失を避けようとさえしないオペレータ、あるいはその振る舞いが危険な状態の原因となるオペレータ、欠陥のあるマネジメントの意思決定、不適合なエンジニアリング開発プロセス、安全文化の問題、規制の不備等があります。航空安全の父である、ジェローム・レデラーは下記のように書いています：

> 「システム安全は、リスクマネジメントのすべての範囲をカバーしています。これは、ハードウェアを超えて、システム安全エンジニアリングの手順と関連します。これは以下のものを含みます：設計者と製造者達の態度とモチベーション、従業員／マネジメント層の信頼関係、彼ら自身の業界団体と政府との関係、監査と品質管理の人的要因、設計と運用に関する企業と公衆安全のインターフェースに関する文書、経営トップの関心事と態度、事故調査に関する法制度と意見交換の影響、重要な作業員の認定、政治的配慮、資源、国民感情とその他非技術的だが許容可能なレベルのリスク制御が達成されていることに対する生々しい（感覚的な）影響。これらは、システム安全が決して無視できない非技術的な側面であります。」[4]

私達の事故調査は、これら全ての要因かそれ以上を潜在的に含める必要があります。このハンドブックではそれをどう行うか示します。

後知恵バイアス

後知恵バイアスの概念について書いたものはたくさんあります。リスクの過剰な単純化において、後知恵バイアスとは、事故が起きたことを知り、その理由を考えた後では、事前に事象を予測できなかったことを理解することが、人にとっては心理的に不可能である、という意味です。事実の後では、人は因果関係を理解し、全てのことが明らかなように見えます。私達は、行動に対する結果を見ることが叶わなかった関係者の精神状態に身を置くことが大変難しいです（図3参照）。

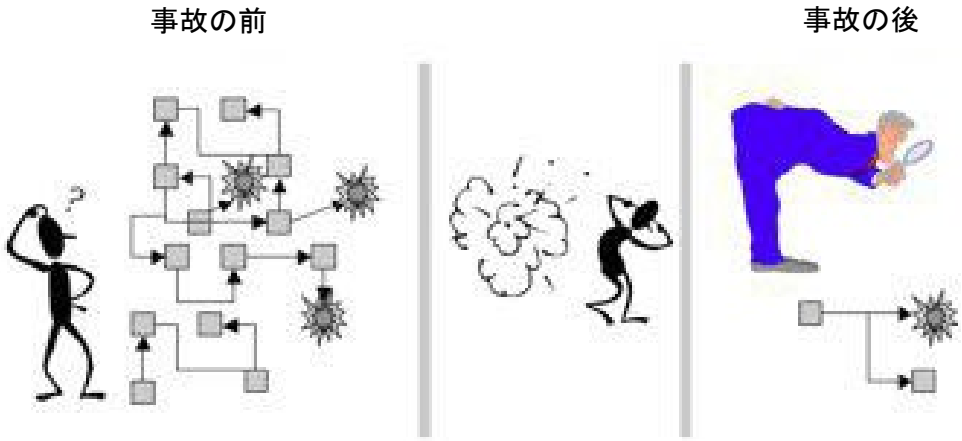


図 3：後知恵バイアスの図解
[本図はリチャード・クックまたはシドニー・デッカーに帰属]

後知恵バイアスは、通常、事故報告書で見受けられます。後知恵バイアスの明白な手がかりは、「彼／彼女はしなければならなかった・・」、「彼／彼女が出来たならば」または「もし彼／彼女が・・さえしていれば」という言葉が現れた時に含まれています。ここではいくつかの例を示します。１つは化学プラント、もう１つは航空機です。

---

[4] Jerome Lederer, How far Have we come? A look back at the leading edge of system safety eighteen years ago, *Hazard Prevention*, page 8, May/June 1986.

化学プラントにおいて、SO2（二酸化硫黄）のオーバーフローを伴う事故の後では、調査報告書は、「*ボードオペレータは、タンク内部の液面上昇を通知すべきであった*」［強調追加］と結論づけました。良くないですよね？結果を調べてみましょう。

オペレータは、液体をタンクに流入させる制御バルブをオフにし、バルブが閉じたことを示す光が点灯しました。オペレータが制御室で得ることが出来た、流量計を含む他全ての手がかりは、バルブは閉じたと示していました。タンク内の高位置警報機は18ヶ月間故障していて、修理がされたことがなかったため鳴りませんでした。レポートからは、オペレータがその警報機が稼働しないことを知っていたかは分かりませんでした。空気中のSO2の存在を検知するはずの他の警報機も、もうしばらく後になるまで鳴りませんでした。

１つの警報は鳴りましたが、それは月に１回程度誤動作し、過去に一度も実際の問題を警告したことがなかったので、オペレータはその警告を信用しませんでした。彼らは、警報は単純に、タンク内の液体がセンサーを揺らした結果だと思いました。オペレータはプロセス制御システム内の特別なツールを使用して逐次液体の水位を調査する（そして水位が上昇していることが分かる）ことができましたが、非標準的なツールを使うための、自動システムの中のページに行くためには、特別な労力が要求されました。そのようなことをする理由はありませんでしたし（それは標準的な作業ではありません）、その時には問題があるという証拠はありませんでした。同時に、潜在的に非常に深刻な警報が発電所の別の部分で発生したので、オペレータは代りそちらの調査をしました。結果として、事故報告書の中では、オペレータがSO2放出の主な原因として識別されました。

SO2放出後の丁寧な調査の後にも関わらず、報告書ではなぜバルブが閉じず、また流量計に流入がなかったかを説明できていないことは興味深いです。別の言葉で言うと、なぜそうしてはならない時にタンクが満たされていったのでしょうか？しかし、オペレータは、当時目に見える手がかりなしで、かつ彼らの注意への競合する要求がある中で、（タンクの水位を）知ることが期待されています。これは、調査官が後知恵バイアスに屈している古典的な例です。事実の後であるから、報告書作成者はSO2が放出されたことを知っており、オペレータもどうにかしてそれを知るべきと想定しています。

「すべきである」やそれに相当する言葉はあまり報告書には現れないかもしれませんが、後知恵バイアスはまだ働いている場合があります。例えば、1995年コロンビアのカリに向かう途中に墜落したアメリカン航空B757の事故報告書に引用された４つの想定原因のうち１つは、「*多数のシグナルが（カリへの）アプローチを継続することの不適切さを警告したにも関わらず、カリに向かうことを中止しなかった乗務員の失敗*」でした。事実、「シグナル」は墜落が起こったことを既に知っているからこそいえる、後知恵でのシグナルです。

まとめると、事故の後は人がどこを誤ったのか、そして彼らは何をすべきだったか、または避けるために何をすべきだったかが簡単に見えるため、後知恵バイアスは起こります。また、事故がどう起こったかの因果関係が明らかになった後にだけ、危機的状況に陥る欠落した情報を判断することも容易です。（事故が起きたときに）戻って、後の結果についての知識を持たない人が世界をどのように見ていたかを理解することはほとんど不可能です。

「事後の」推論の自然な結果であるとすれば、後知恵バイアスはどのように避けられるのでしょうか？これには、多少の労力と、因果関係についての私達の考え方を変える必要があります。事故の原因を分析する際に、誰が誤ったことをしたのかの識別に焦点を当てることに時間を費やす代わりに、オペレータが故意に損失を起こそうとしているのではなく、正しいことをしようとしていたという前提から始める必要があります。私たちが、人がどう間違ったかではなく、*彼らがしたことに対して、なぜその時に彼らにとって理にかなっていたか*を特定することに着目した時、学びは起こりえます。[5] CASTはこのようなタイプの質問に答えることを求め、このような振る舞いを将来防ぐための更に有用な方法を特定させます。

[5] さらに知りたい場合はこちらを参照してください。Sidney Dekker, The Field Guide to Understanding Human Error, Ashgate Publishers, 2002.

ヒューマンエラーに対する非現実的な見解

人的要因の学術論文は、ここではふさわしくありません。このような本は沢山存在します。しかし、多くの事故分析は、オペレータのエラーが多くのインシデントや事故の原因であるという信条からはじまっています。[6]従って、調査はオペレータに主に焦点を当てるべきということになります。オペレータが原因であるに違いないという想定（assumption）がなされ、そして当然のことながら、オペレータは事故分析において注目の的となり、原因として識別されます。オペレータが関与した途端、推奨事項はオペレータについて何かすることを強調します（彼らを罰する、解雇する、同じことを二度としないように特定のオペレータまたは全てのオペレータの再教育）。事故原因としてのヒューマンエラーの強調の一部は、100年前に発生し、約70年前に科学的に完全に信用できないとされた「腐ったりんご」理論によるものです。残念ながら、今でもそれは存在しています。付録Ｃは、その理論について詳細な情報を提供します。ハインリッヒもまた、この理論を同じ時期に公表しました。

一般的にオペレータに対しては、代替的、または追加的に何かがなされることがあります。彼らの仕事は、彼ら自身が事故を導いてしまうような、または彼らが常に従うことが不可能または非現実的な多くのルールや手順を作成されることにより、制限されているかもしれません。あるいは、自動化をさらに追加することにより、オペレータを重要視しなくなるかもしれません。自動化をさらに追加すると、彼らが制御しているプロセスからオペレータをさらに遠ざけることにより、より多くのタイプのエラーを発生させることになるかもしれません。最も重要な点は、オペレータに着目することによって、事故調査では、オペレータの振る舞いと事故の間の体系的な要因を、無視するか重要視していないということです。

一例として、多くの事故調査では、オペレータは過去の同様の事象についての事前知識があったものの、インシデントの報告システムで報告したことがないことが分かっています。多くのケースで、オペレータは問題を解決できると思った技術者には報告していましたが、公式のインシデントの報告システムは利用していません。この事故報告書の結論としては、事故の原因は、オペレータが公式のインシデントの報告システムを利用していないこととし、常にそのシステムを使用することを強制するために新しい規則を作ることとシステムの使用のための追加の訓練の提供を推奨することになります。

しかしながら、これらのほとんどのケースでは、なぜオペレータが公式の報告システムを使用しなかったのかの調査はありませんでした。しばしば、彼らの振る舞いはシステムを利用することが難しいこと、オペレータに扱いづらいインターフェースでめったに使わない且つ見つけるのが困難なウェブサイトを探すことが要求されることから来ています。このような方法で事象を報告させるのは、多量の時間がかかります。オペレータは決して結果を見るまたは聞くことはなく、まるで報告がブラックホールに吸い込まれるように思います。彼らが問題に対して何か出来ると思う人に、（システムの）かわりに報告することは不思議ではありません。報告システムの設計により問題を修正することは、オペレータにそれを利用しろと強調するよりも、より容易で効果的です。

システムによるヒューマンエラーの見方は、全ての振る舞いはそれが発生するコンテキスト（システム）により影響を受けるという前提からはじまります。従って、人の振る舞いを変える最善の方法は、それが発生するシステムを変えることです。これは、オペレータが利用している機器の設計を調べる、オペレータが従うように与えられた手順の有用さと適切

[6] 多くの研究では、事故の70-90%の原因はオペレータであると結論づけて公表しています。この研究は、事故報告書を参照していることが問題です。この結論が導かれたのは、オペレータが真の主たる原因だからでしょうか？事故報告書でよく非難されるからでしょうか？多くの場合、後者が真実です。どの道、単に事故報告書を見ているだけでは、そのような結論は正当化されません。

さを慎重に分析する、目的の矛盾と生産に対する圧力を特定する、振る舞いについての組織の安全文化の影響を評価する、等を含みます。

安全ルールや手順に違反することは、オペレータによるエラーが事故の原因である明白な証拠として一般的に考えられることは興味深いです。調査がなぜルールは破られたかという方向に行くことはほとんどありません。事実、ルールや手順は、オペレータや作業者を「手順に従う」ジレンマに直面させるような容認できない状況にします。図4のモデルを考えてみましょう。

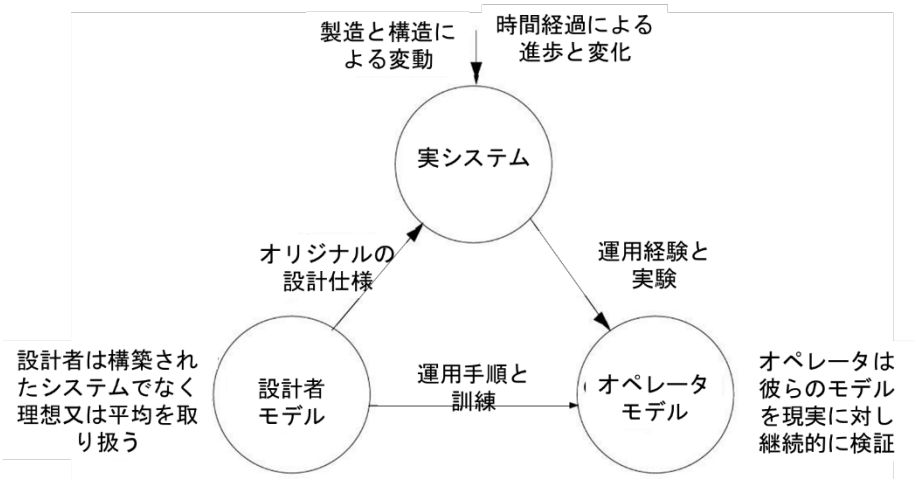


図 4：手順に従うジレンマ

実システムには常に、少なくとも２つのメンタルモデル（mental model）が存在します：設計者モデルとオペレータモデルです。設計者は、オリジナルの設計仕様、運用手順、訓練ガイドについて提供を行うか従います。設計者は、理想または平均値（理想的な材料や平均的な材料）を扱い、実システムは当初の設計仕様を満たしながら開始し、時間が経過してもそれが保たれていると想定します。操作手順と訓練はその想定に基づいています。しかしながら現実は、初期の構築中に、製造上および構築上の差分があるかもしれません。加えて、システムは進化し、その環境は時間とともに変化します。

対照的にオペレータは、元々設計者の頭の中か当初仕様にあるシステムではなく、どんな時でも実在する実システムを扱う必要があります。オペレータはどうやってシステムの今の状態が分かるのでしょうか？彼らは、フィードバック（feedback）と運用経験を活用して、この状態を判断し、設計者による誤った想定を明らかにします。多くの場合、オペレータは、「実験（experiments）」または非公式のテストを行うことによって、実システムに対する自身のメンタルモデルを検証します。彼らはシステムの振る舞いと、実在の状態に対する自身のモデルを継続的に検証しています。

システム設計者によりオペレータに提供された手順は、オペレータ（または設計者）の期待からシステムが異なる振る舞いをした時には適合しないかもしれません。例えば、スリーマイル島のオペレータは、プラントが期待の振る舞いとは異なった振る舞いをしていることを認識していました。彼らは、提供された実手順に従い続けることも、自分たちの手順を打ち出すことも出来ました。彼らは、事実として後に間違っていることが判明した手順に従うことを選びました。オペレータは、これらの手順に従ったことにより、インシデントに対する多大な非難を受けました。一般に、オペレータは下記の中から選択しなくてはいけません：

1. 周辺状況が適応や変更の必要を示唆しているにも関わらず、厳密に手順に従う。または、

2. 予期しない状況に直面したときに手順を適応させるまたは変更する。

彼らが従うように訓練された手順に従うという最初の選択は、訓練された手順が当面の状況に対して間違っている場合、危険な結果につながる可能性があります。彼らは、柔軟性に欠けることと、設計者や手順では予期していないシステムや状況についての状態を理解せずにルールを適用したことについて非難されます。もし彼らが手順を適応または変更するという２つ目の選択をした時、彼らは起きている事象とシステムの状態、そして書かれている手順を破ることによって何が起こるのかに対する完璧な知識がない場合、事故やインシデントを引き起こす行動を取ることになります。彼らは、逸脱したことやルールに違反したことについて非難されます。

ルールや手順に従うことは常に安全性を保証するものではありません。代りに安全性は、それらをいつどうやって適用するのか判断力のある人によってもたらされます。安全性に対する伝統的なアプローチは、安全性の向上は、組織が人々に手順を守るように指示し、それらを強制し、事故が発生しまたルールや手順違反があったときに、人にその責任を割り当てることによりもたらされると主張しています。対照的に、安全に対するシステム的アプローチは、安全性の向上は、組織が書かれている手順と実績（振る舞い）の間のギャップを監視、理解し、それに従い手順やルールを更新することであると想定します。文書化された手順やルールに違反した事故やインシデントが発生した後は、その手順や規則を無視する必要があるとオペレータが判断した理由を決定することに重点が置かれるべきです。単純に、オペレータが失敗に陥ったのは、彼らが文書化されたルールに従わなかったからという結論では、有用な情報が提供されません。

一般に、近代的なシステムでのオペレータの役割は変化しています。人間は、直接システムを制御するよりも、ますます自動化（実際に、ほとんどの詳細な制御タスクを実装している）を監督するようになっています。それと同時に、ソフトウェアは非常に複雑なシステムを作成することを可能にしています。これが、そのシステムを理解する人間の能力を拡張させ、ある条件下では危険であるかもしれない人間の振る舞いにつながります。加えて、システムは時々、適切な人間中心または人的要因の原則を使わずに設計されることがあります。その結果として、我々はオペレータのエラーが避けられないシステムを設計し、そして事故について設計エラーよりもオペレータのエラーについて非難します。

*ヒューマンエラーは症状であって、原因ではありません。*アメリカン航空のカリの事故の事故報告書で引用された４つの想定原因の中の、他の原因を考えてみましょう。：「FMS支援ナビゲーションが混乱し、飛行のクリティカルなフェーズで過剰な作業量を要求されたときに、乗務員は基本的なラジオナビゲーション（radio navigation）に戻らなかった」。ここでは、混乱を招き、過剰な作業量を要求したソフトウェアのせいではなく、混乱しそして、貧弱に設計されたソフトウェア（FMSまたはFlight Management System）を使用することを選択した乗務員のせいであると見なされていることに注意してください。このように事故報告書が原因に言及している時に、学びは妨げられ、事故シナリオの悪い側面に注意が向きます。

事故原因のシステムアプローチは、ヒューマンエラーは再設計が必要なシステムの症状であるという前提から始まります。事故分析は、設計の欠陥とどのように修正できるかの推奨事項を識別すべきで、これらの設計の欠陥による影響であるオペレータを非難すべきではありません。

非難は安全の敵

非難は法的または道徳的なコンセプトであり、工学的なものではない

非難（blame）に焦点を合わせることは、私達が事故から学ぶことを著しく妨げます。裁判所の目的は、責任と負債を確立することです。対照的に、エンジニアリングの目的は、*な*

*ぜ*避けられたかもしれない事故が起こったのかを理解することで、避難することや誰に責任があるのか決めることではありません。

事故分析で非難に焦点を当てることは、事故から学べることを減らし、将来の事故の防止を妨げるという多くの不幸な側面があります。一つの結果としては、多くの場合、大事な情報が隠れることです：これらには、他人に非難が向くようにする、非難すべき他の人を探すということが含まれています。原因の探索は、事象連鎖の直接的なアクターを識別することに陥ります。通常は、明らかに事象に登場し、他の人達に注意をそらす理由がない、人間のオペレータや下級のマネージャです。すると焦点は、将来の事故を防止するための重要な情報を提供する可能性が最も低い損失の側面に置かれます。

C.O.ミラーとジェリー・ブルギンクは、原因分析の非難的（accusatory）アプローチと説明的（explanatory）アプローチを区別しました。ここで、このハンドブックの読者への短い演習です。下記の事故報告書の結論を考えてみて下さい：[7]

演習 その１ 事故原因の説明:

WHO（誰が）

事故調査委員Ａはこの事故の想定原因は、下記だと判断しました：

1. 地上運用と離陸時にエンジンの防氷装置を使用しなかった乗務員の失敗（failure）。
2. 乗務員たちが行った、航空機の翼の表面に雪／氷がある状態での離陸判断。機長の注意がエンジン異常に関する計器に向いている時に、早期の離陸を取り下げなかった機長の失敗。

WHY(なぜ)

寄与した要因:

1. 航空機が継続的な降雪にさらされる中、除氷と離着陸の管制承認に関わる長時間の地上での遅延。
2. たとえ少量の雪や氷であっても前縁にコンタミネーション（contamination）があった時に発生する、B-737航空機固有の既知のピッチアップ特性。
3. 冬季のジェット旅客機のオペレーションに対して、経験の少ない乗務員。

上述の事故原因の記述を用いると、この損失に対する責任はどこに割り当てられるのでしょうか？どのような推奨事項を結果として提供しますか？調査中に聞きたい追加の質問はあるでしょうか？

あなたの答えに対する考察：

あなたは、乗務員に責任を割り当てましたか？なぜですか？あなたが作った推奨事項の焦点は何でしたか？推奨事項には、乗務員の訓練や手順が含まれていましたか？その他にはどのような事故要因や推奨事項を作成しましたか？あなたは、地上の遅延やそれを避けることについて述べたかもしれません。しかし、多くの場合あなたの事故要因や推奨事項は乗務員に関するものが含まれているでしょう。乗務員達の振る舞いが想定要因であると分析されることは、驚くことではありません。

[7] C.O. Miller, “Down with ‘Probable Cause’!” International Society of Air Safety Investigators
Seminar, Canberra, Australia, November 1991 から適用。

演習　その２：ここでは同じ事故について述べた２つめの要因の記述について考えて下さい。

WHAT（何が）

有効な証拠にもとづき、事故調査委員Bは、両エンジンの推力不足は、コンタミネーションがある翼と相まって、航空機の離陸性能を著しく低下させ、その結果、離陸直後に飛行経路内の障害物との衝突を引き起こしました。

WHY（なぜ）

推力不足の理由：

1. エンジンの防氷装置が離陸時に使用されず、また航空機の運用マニュアルにもとづくと「湿った雪」の際は使用することが求められていませんでした。
2. エンジンのインレット（吸気口）のプローブが氷で詰まり、その結果、誤って高い推力が読み取られました。
3. １人の乗務員がコクピット内の計器の異常に気付いたが、エンジンインレットのプローブが凍結したことと関連付けませんでした。
4. 冬季の推力計器の誤りを含むインシデントが以前にあったにも関わらず、規制当局と企業は、エンジンインレットのプローブが塞がれることによる影響について対処しませんでした。

翼のコンタミネーションの理由：

1. 除氷／防氷装置の手順。
2. 飛行マニュアルのガイドに反したテクニックを乗務員が使用することによる、翼のコンタミネーションの悪化。
3. ゲートからの出発と離陸許可の間に49分の遅れをもたらしたATC手順。

さて、この事故であなたは誰または何に責任を割り当てますか？あなたのリストは、演習その１で作成したものより、大きくそして異なるものでしたか？あなたが調査したい追加の疑問はありますか？事故要因は「乗務員の失敗」以外のものがあると今は思いますか？他の要因は識別しましたか？この分析からどのような推奨事項を作成しますか？推奨事項は演習その１で作成したものと比較してどう異なりますか？なぜですか？設計上の推奨事項や、乗務員以外のグループや人々を含む推奨事項を作成しましたか？

はじめの事故の説明（演習その１）は、*非難的*でした。 損失に係るオペレータや彼らの役割、つまり誰に責任があったかに焦点を当てています。２つ目の説明（演習その２）は、*説明的*でした。誰が（Who）ではなく、何が（What）どうして（Why)に焦点を当てています。両者は同じ事故を説明していますが、とても違う推奨事項となります。非難的なものよりも、説明的なアプローチを用いる、つまり誰がではなく何が、どうしてということに焦点を置くことで、私達はより多くの原因因子を探し、学ぶことができます。

非難的:	VS.	**説明的:**
Who（誰が）		What（何が）
Why（なぜ）		Why（なぜ）

図 5:事故説明の二つの相対する観点

この２つの演習でもう１つ注意すべきことは、「失敗（failure）」という言葉が１つ目では使用され、２つ目では使用されていないことです。失敗は悲観的な言葉です、すなわち、それは判断と責任の割り当てを含みます。「失敗（failure）」という言葉の使用だけが異なる、以下の２つの記述を考えて下さい:

1. 機長の注意がエンジン異常に関する計器に向いているときに、早期の離陸を取り下げなかった機長の失敗（failure）。
2. 機長は、彼の注意がエンジン異常に関する計器に向いているときに、早期の離陸を取り下げなかった。

最初の記述は、機長が何か誤りを行ったことを示唆する結論になっています。結論があるので、さらなる追求は推奨されません。機長の行動についての判決がなされています。原因は特定され、その原因は機長の失敗によるものです。２つ目の記述は、機長が何を行ったかの単純な記述で、判決は入っていません。なぜ機長の注意が異常なエンジン計器の測定値に向けられたのか、そしてさらに重要である、なぜ異常な測定値が出されたのかについて、さらなる追求が推奨されます。

これ（誰かの「失敗（failure）」と結論づけること）は、複数の事故報告書において実際にある問題なのでしょうか？もっとはっきり言えば、「失敗（failure）」と結論づけることは多くの事故報告書で浸透しています。ここにバーミングハム=シャトルズワース国際空港で起きた航空機のCFIT（シーフィット。操縦可能状態での地表へ墜落）事故[8]の、典型的な結論の例があります。NTSBは下記のように結論づけました：

「この事故の想定原因は、乗務員の継続的な不安定な進入と、彼らが進入中に航空機の高度を監視することに失敗したことであり、不注意な降下により最低進入高度を下回り、その後地表に墜落した。」

また、報告書はこの事故へ寄与したものは下記と結論づけました：

(1) 進入のためのフライトマネジメントコンピュータを適切に設定および検証しなかった乗務員の失敗
(2) 縦方向のプロファイルが把握されていないことが明らかになった時に、意図を副操縦士とコミュニケーションしなかった機長の失敗。
(3) 不完全な気象情報から、地上1,000フィードで雲を抜けられると思っていた乗務員の想定
(4) 必要だった最低高度のコールアウトをしなかった副操縦士の失敗
(5) 疲労、注意散漫、または混乱を含むがこれらに限定されない要因による、機長の能力不足。これは訓練中に示された能力不足と一致する。
(6) 勤務時間外のタイムマネジメントの乏しさと体内時計に関する要因による急性の睡眠障害による副操縦士の疲労

[強調追加]

この事故の想定原因と寄与する要因に関する結論は、乗務員に関する振る舞いと乗務員の「失敗」を反映した事象のみが識別されているということに注意して下さい。*なぜ*乗務員がそのような行動を取ったのかの理由は含まれていません（疲労を除き、十分な説明にはなっていません）。１つの寄与因子は理由を述べています（例：（3）不完全な気象情報か

[8] National Transportation Safety Board, Crash During a Nighttime Nonprecision Instrument Landing, UPS Flight 1354, Birmingham, Alabama, August 14, 2013, Accident Report NTSB/AAR-14/02, 2014.

ら、地上1,000フィードで雲を抜けられると思っていた乗務員の想定）。しかし、ここでは乗務員の行動と想定のみが強調され、なぜ不完全な気象情報が乗務員に提供されたかについては強調されていません。気象情報を提供し、かつ修正が必要なシステム設計の欠陥については、事故原因の要約では言及されていません。

一方、システムアプローチを用いるCASTでは、事故に寄与したパイロットの行動に着目するだけでなく、より重要な、*なぜ*その時にその行動が正しいと信じたかについて着目します。[9] 公式な結論は、将来同様の事故を防ぐために有用な多くの情報を省略しています。「失敗」という結論によって説明が止まってしまうため、なぜ乗務員がそのように行動したのかが学べません。加えて、パイロットの行動だけではなく、CFIT（何年にも渡って事故回避のために焦点が当てられていた）を防止するための全てのシステムが検証させるべきです。この事故での多くの寄与因子は自動化の設計にありました。例えば、計器着陸システムなしでの滑走路への着陸、航空機が低すぎることを示す航空交通管制の警報の欠如、空港での保守、手遅れになるまで警告を提供しない地上接近警報システム（航空会社が警報システムを新しく提供されているソフトウェアで更新していないことが一部の原因）、そして単に乗務員の「失敗」と特定するよりも有用な推奨事項につながる可能性が高い、多くの要因です。

「失敗（failure）」という単語の使用は、ほとんどの事故報告書の原因の説明として浸透しています。人間に対してだけでなく、ソフトウェア、オペレータそしてマネジメントの意思決定にも誤って適用されています。

ソフトウェアは「失敗（fail）」しません。単に書かれているロジックを実行するだけです。なぜ安全でないソフトウェアが作成されたのか（通常、要求の欠陥に帰着します）、安全でないソフトウェアを作成したプロセスの改善に関する推奨事項の検討が必要です。「ソフトウェアの失敗」という結論は、技術的に意味がなく、有用な情報を提供しません。

人もまた「失敗」しません（心臓が止まるまでは）。彼らは、彼ら自身が見つけた状況に対して単に反応するだけです。後知恵により、彼らが行ったことは間違ったことだったかもしれません。しかし、なぜその時に彼らにとって正しいことだと思ったのかを調べることは、有用な推奨事項を作成するために必要です。繰り返しますが、単に人が間違ったことをしたと言うことは有用な情報を提供することはなく、事故に対する便利なスケープゴートを作るだけです。なぜ彼らがそのような行動を取ったのかについて理解することは、事故分析を有用な方向に集中させることになるでしょう。

そして最後に、企業も倒産するまで失敗しません。事故報告書で見られる典型的な例として、「企業Xは過去の事象から学ぶことに失敗した」という記述があります。企業とは法人を表す紙切れのことです。紙切れは学ぶことはなく、失敗することもありません。企業は、何百、千、万の従業員によって作られています。より有用にするには、学びがなぜ起こらなかったか次のような質問から判断することです。「学びが発生するような過去の異常事象を捉える安全情報システムはありますか？もし存在するとしたら、過去の事象は安全情報システムに記録されていましたか？記録がなければ、なぜしないのですか？突発的に誤っただけなのか、これらを含めるプロセスがなかったのか、プロセスが守られなかったのでしょうか？もし後者なら、なぜプロセスが守られなかったのでしょうか？もし過去事象が記録されているとしたら、なぜ使われなかったのでしょうか？探すのが難しかったのか、繰り返しを防止することに十分な情報が含まれていなかったのでしょうか？記録された情報を使うような手順はあったのでしょうか？等々。」これらの質問に答えることは、将来の学びを向上させ、また損失を繰り返すことを防止する推奨事項を作成するために、有用な情報を提供します。単に「企業は事象から学ぶことを失敗した」と結論づけることは、将来の状況を改善するために必須となる情報を提供することなく、責めを負わせるだけです。

「失敗」の使用を排除することは、事故から学ぶことを大きく促進します。「失敗があ

[9] Sidney Dekker, *A Field Guide to Understanding Human Error*, London: Ashgate, 2006.

った」と結論づけて理解のための調査を省略するようなことをしなければ、私達は事故調査、学び、そしてあわよくば安全性を計り知れないほど改善させることができます。

損失からの学びを高めるためには、より一般的には、事故報告書で責めを負わせることを排除する必要があります。これは難しいかもしれません。人は悲劇に対して誰かの責任を探すという性があります。しかし、悪人を特定したい個人の満足か、将来にこのような事故を防止する機会をつかむかのどちらかを選択をする必要があります。エンジニアは、非難は法制度に任せるべきです。そして企業やその他の者は、責任を自分自身から他者に移すために公式の事故調査を使用すべきではありません。非難のない方法で事象に対する全ての寄与因子と理由を含めて単に何が起こったのかを記述した報告書は、責任の割当や回避するための労力を、元々それに取り組むべきである法的プロセスへと転嫁します。

不適切な事故因果関係モデルの使用

もう一つの要因は、事故調査から何をどれだけ学ぶかに大きな影響を与えます。前のセクションで述べた問題の多くは、事故分析で用いた「原因」の定義に由来するため、この定義をもう少し考慮する価値があります。「原因」の定義は、調査で使用されている事故因果関係モデルに依存します。このセクションでは、次の質問に回答することとします：

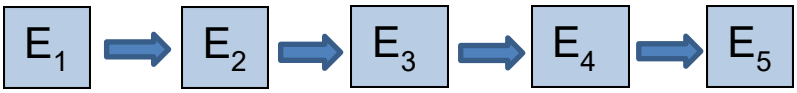
- *事故因果関係モデルとはなにか？*
- *今日、ほとんどの場合どのような因果関係モデルが使われているか？*
- *従来の因果関係モデルの限界は何か？*
- *代替の方法はあるか？*

事故因果関係モデルとはなにか？

因果関係モデルは、何かが起こった理由を単純に説明します。事故の場合、モデルを使用して事故が発生した理由を説明しています。私たちは皆、どのようにして、そしてなぜ事故が起こるのかと考えるモデルを、頭の中に持っています。意識して考えているわけではないかもしれませんが、思考に影響を与えています。私たちが事故から学び、防止しようとするとき、その過程でそのモデルを使います。もしモデルが、考慮される原因メカニズムを制限するのであれば、それは学習を減らすことになります。

今日、ほとんどの場合どのような因果関係モデルが使われているか？

因果関係の最も一般的なモデルは、事故は事象の連鎖の結果であることを前提としています。この場合、事象は通常、システムコンポーネントの故障（failure）を含み、各故障または事象はそれに先行するものの直接的な原因です。



このモデルには、事象の記述に使用されるさまざまな名前と類似性が与えられていますが（図6および図7）、基本となるモデルは同じであり、それは、故障の事象の連鎖です。



図 6：ハインリッヒのDominoモデル、1932

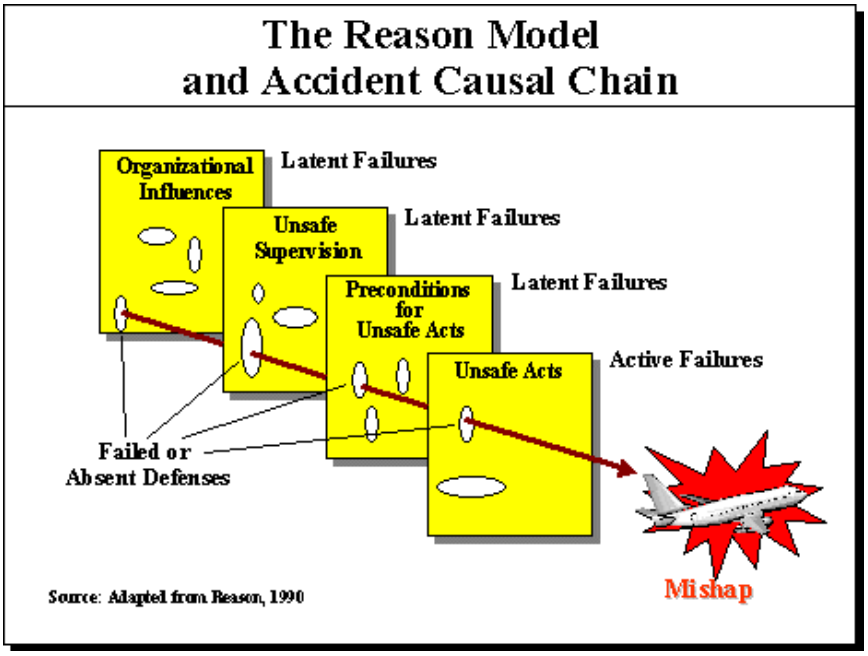


図 7：リーズンのスイスチーズモデル

何万人もの人々が死亡し、重傷を負った、ボパール（インド）化学プラントからのイソシアン酸メチル（MIC）の漏出を一例として考えてみます。事象の連鎖は次のように記述されます。

E1: MICから水を隔離するために、作業員がスリップブラインドを挿入せずにパイプを洗う。

E2: パイプ洗浄水がMICタンクに漏れ（水がある状態では、MICは爆発性がある）、タンク内の圧力が上昇する。

E3: 計器が故障しているため、制御室オペレータは圧力を緩和するための二次リリーフタンクへのバルブを開かない。彼はリリーフタンクが満杯であると考えている。

E4: 爆発が起きる。

E5: 高圧下で自動リリーフ弁が（設計されたとおりに）開く。

E6: いずれの保護装置（フレアタワー、ベントスクラバー、ウォーターカーテン）もMICの放出を妨げず、MICは大気中にばら撒かれる。

E7: MICが、プラント周辺の人口密集地に風によって運ばれる。

この一連の事象から、通常は１つの事象が根本原因として選ばれます。この事故では、ユニオン・カーバイド社（プラントの所有者）とプラントを運営しているインドの子会社の両方が、スリップブラインドを挿入せずにパイプを洗い流した下級労働者を指摘し、彼は実際に刑務所に入れられました。ただし、この選択は独断的であることに注意が必要です。オペレータがリリーフタンクへのバルブを開放しない、保護装置が作動しないなど、その他の事象を選ぶことができた可能性があります。

ここでの一連の事象はもっと遡ることもできたかもしれませんが、連鎖は通常、責任を負わせることができる都合のよい人や事象が見つかった場合、この場合はパイプ洗浄作業者で停止します。選ばれた根本原因事象には、通常、実際に損失が発生した時刻に近いオペレータのアクションまたは非アクションが含まれます。労働者を刑務所に入れることは、関係する他の（自分たちから非難をそらすことに満足していた）ほとんどすべての人の目的を満足させたかもしれませんが、はるかに複雑であった事故の真の原因を特定し排除する助けにはなりません。基本的には、事故から学び、事故を防ぐためには、何が起こったのかだけでなく、なぜ起こったのかを知る必要があります。これらの事象が、常に単純な因果関係の連鎖の中で起こるという想定は正しくありません。

例えば、なぜパイプ洗浄者はスリップブラインドを入れなかったのでしょうか？実際、パイプの洗浄作業に割り当てられていた作業員は、バルブが漏れたことを知ってはいましたが、パイプがきちんと隔離されているかどうかは確認していなかったそうです。スリップブラインドの挿入は保守部門の仕事でしたが、保守シートにはこのディスク（スリップブラインド）を挿入する指示がありませんでした。本来なら２番目のシフトがパイプの洗浄作業を監督することになっていましたが、コスト削減のため、このシフトは廃止されていました。もちろん、事象連鎖モデルを使用すれば、前の事象、たとえば２番目のシフト監督者の解雇などを根本原因として書き入れるだけで済みます。しかし、連鎖はやはりまだ、なぜこの事故が起こったのかを説明していないので、これでは問題は解決しません。多くの事故がそうであるように、注意深く調査した結果、この事故は単なる事象連鎖よりもはるかに複雑であることがわかりました。この複雑な一連の事象を理解する上での、そして将来このような事象を回避する上での主な限界は、事象連鎖を使用する中で暗黙的に過度に単純化していることに起因します。ボパール発電所の設計と運転条件を考えると、実際には事故が起こるのを待っている状況でした。:

> 「しかし、[水]が入ったとしても、もし[MICを非爆発温度に保つために必要である]冷却装置が切断されておらず、[節約のために]フロンが排出されていなければ、計器が適切に作動して監視されていれば、MICの臭いに最初に気が付いたときに、休憩の後まで持ち越さずに様々な措置を取っていれば、スクラバー（洗浄機）が使用されていれば、放水口が十分に高くなるように設計されていれば、あるいはフレアタワーが作動していて大規模な暴走に対処できるように設計されていれば、大爆発は起こらなかったでしょう。[10]」

そして、これは始まりに過ぎません。特に、２年前の安全監査では、損失に関係したすべてのものを含む、プラントにおける多くの問題を指摘していましたが、特定された欠陥は決して修正されませんでした。ここでは詳細は重要ではありません。基本的な問題は、複雑な損失の因果関係を単純な事象連鎖では捉えることはできないということです。

従来の因果関係モデルの限界は何か？

[10] Charles Perrow, The Habit of Courting Disaster, *The Nation*, October, 1986, p. 349

最も重要な限界の一つは事故原因の線形性（linearity）に関する前提です。連鎖内の次の事象に対する１つの事象の影響以外に、事象が独立しているという前提があることにも注意が必要です。実際に、連鎖のすべての事象に影響を及ぼすような体系的な原因は、ほとんど常に存在しています。

ボパール事故をもう一度考えてみましょう。この事故の原因は、漏れのあるバルブに対して防護具を挿入せずにパイプを洗い流した作業員にあると特定されました。同プラントの劣悪な環境の多くは、財務上の圧力のために放置されていました。MICに対する需要が急激に減少したため、生産量が減少し、同社にはコスト削減の圧力がかかりました。これに伴い、保守・運転要員を半減しました。保守手順が大幅に削減され、シフト交替システムが停止しました。つまり、シフトの最後に交替要員が現れなければ、次のシフトは無人になるということです。パイプにスリップブラインドを挿入する責任を持つ者が、シフトに来なかったので、交替されず、誰も保護装置を挿入しないということになりました。

ボパールのプラントが赤字になったため、熟練労働者の多くはより安定した仕事に向かいました。彼らの穴は補充されなかったか、あるいは（事故で非難されたパイプ洗浄者のような）未熟練労働者によって補充されました。職員の教育水準は、研修とともに低下しました。経営と労働の問題が財務的損失に続き、プラントの士気低下につながりました。

これらはこの大惨事に関与した要因のほんの一部であり、それにはプラントにおけるその他の技術的および人的ミス、設計上のミス、管理上の過失、米国およびインド政府による規制上の不備、そしてそもそもこのような危険な化学物質がインドで作られた理由に関連する一般的な農業および技術移転政策が含まれていました。これらの観点や原因のいずれか一つだけでは、事故を理解し、将来の事故を防止するには不十分です。全ての要因を考慮すると、パイプ洗浄作業者が本事故の「根本」または「想定」原因である可能性はますます低くなります。これまで述べてきたすべての問題（他にもたくさんあるが）を考えると、このプラントでの将来の事故を防ぐために、（事故後に起こったように）パイプ洗浄を担当した人を刑務所に入れることが効果的だと思いますか？

事象モデルの連鎖においては、連鎖における事象間の直接的因果関係、すなわちA→Bとなること（AがBの必要十分な原因であること）は、暗黙的な前提です。この論理ステートメントの対偶命題は、Bが起きていないのであれば、Aは起きていないということを意味しています。これは洗練された形式的な論理にはなりますが、私たちが住んでいる混乱した現実の世界に適用すると、事故原因の包括的な特定を妨げます。例えば、事象連鎖の対偶命題および正式な定義を用いても、喫煙者全員が肺癌になるわけではなく、肺癌になる人全員が喫煙するわけではないため、「喫煙は肺がんの原因になる」という表現は不可能となります。実際、タバコの圧力団体は何十年にもわたって対偶的な（contrapositive）議論を用いて、たばこと喫煙に制限が加えられるのを防いできました。私たちは関連があることを知ってはいますが、それは明らかに、単純で直接的なものではありません。

上述した体系的な原因の多くは、損失に先行する近接した事象に間接的に関連しているにすぎません。このことは、対偶法を用いることにより、それらを原因と見なすことができなかったことを意味します。実際に、これらの要因の多くは連鎖内のすべての事象に影響を及ぼしており、単純な連鎖のような直接的な関係でない限り事象は無関係であるという前提を打ち消しています。なぜ事故が発生したのか、また、それを将来どのように防止するかを理解する上で、事象の連鎖を特定することは、ほとんど役に立たず、せいぜい、原因分析の出発点にすぎません。その場合でも、考慮される要因が制限され、結果にバイアスがかかる可能性があります。

複雑なシステムにおける事故を効果的に防止するためには、社会システム並びに技術及びその基礎科学を含む事故モデルを使用する必要があります。システムを構築・運用する上での目的・目標・判断基準を理解しなければ、事故を完全に把握し、最も効果的に防止することはできません。

代替の方法はあるか？

いくつかの単純な事故においては、事象連鎖モデルが適切かもしれませんが、今日の複雑な社会技術システムからの学習を最大化し、事故を防ぐには、なぜ事象が起こったのかをより完全に理解するのに役立つ何かが必要です。

CASTの基礎となる因果関係の新しいモデルは、その機会を提供します。STAMP（System Theoretic Accident Model and Processes（システム理論に基づく事故モデルとプロセス）は、従来の分解と信頼性理論ではなく、システム理論に基づいています。従来の理論では、安全性は本質的にシステムコンポーネントの信頼性（reliability）と同等です。[11]CASTを使用するために、STAMPの技術的な詳細を説明する必要はありませんが、この新しい因果関係モデルのいくつかの重要な特徴を理解することは有用といえます。

CASTはシステム思考（systems thinking）とシステム理論（systems theory）に基づいています。工学（engineering）で使われているシステム理論は、第二次世界大戦後に、当時構築され始めたシステムの複雑さの増大に対処するために考案されました。また、生物システムの複雑さを首尾よく理解するために、生物学のためのシステム理論が独自に考案されました。これらのシステムでは、個々のコンポーネントの振る舞いが明らかではない方法で結合されているので、相互作用するコンポーネント（サブシステム）を分離し個別に分析すると、システム全体の結果を歪ませます。これらの新しいアイデアの最初の工学的利用は、1950年代と1960年代のミサイルと早期警報システムでした。C.O.ミラーは、1950年代から安全性に対してシステム理論の概念の導入を始めました。同氏はまた、「システム安全（System Safety）」 という名称を初めて使用したと主張しました。

「システム思考」は、数学的に形式的なシステム理論の非公式な同義語として使用されることがあります。システム思考は、システムコンポーネント（物理デバイス、自動化、人間、管理、規制監視など）が時間の経過とともにどのように相互に関連し、動作するかに焦点を当てた分析への総合的なアプローチです。このシステムアプローチを事故分析へ使用することにより、いくつかの原因要因に焦点を当てることから離れ、代わりに、強力な予防措置を特定するために使用できる因果関係のより大きな見解を提供します。

伝統的に、複雑なシステムは、関心のあるいくつかの特性について評価されたサブコンポーネントに分解されてきました。システムは、物理的特性または機能的特性に、あるいは時がたつにつれて事象連鎖に分かれるかもしれません。そして、システム全体の結果を得るために各コンポーネントの結果を組み合わせます。このプロセスの有用性は、いくつかの前提に基づいています。すなわち、システムコンポーネントは独立して動作し、分割（分解）は、考慮されている現象を歪めないことを前提としています。このことは、コンポーネント間の相互作用（interaction）を対として検査できることを意味しており、したがって、コンポーネントを個別に測定し、組み合わせることで現象のシステム値を生成できることになります。このことはまた、コンポーネント（または連鎖内の事象）がフィードバックループ及び非線形相互作用（non-linear interactions）の影響を受けないことも意味します。

システム理論は、第二次世界大戦後、我々のシステムが非常に複雑になり、分解がもはや機能しなくなったという事実に応えて生まれました（それでも人々は分解の利用をやめませんでしたが）。分解アプローチの基礎となる前提は、今日のソフトウェア集約型で複雑なシステムには当てはまりません。その代わりに、次のシステム理論を用います：

- システムは、部分の総和としてではなく、全体として扱います。「全体は部分の総和以上のものである。」という言葉をよく耳にしたことがあるでしょう。
- 主要な関心事は、*創発（emergent）特性*（図8）であり、これは、個々のコンポーネントの総和には含まれていないが、コンポーネントが相互作用するときに 「創発する」特性です。創発特性は、そのすべての技術的及び社会的側面を考慮することによってのみ、適切に取り扱うことができます。安全性は、セキュリティやその他の重要な工学的システム特性と同様に、創発特性です。

[11] Nancy Leveson, Engineering a Safer World, MIT Press, 2012.

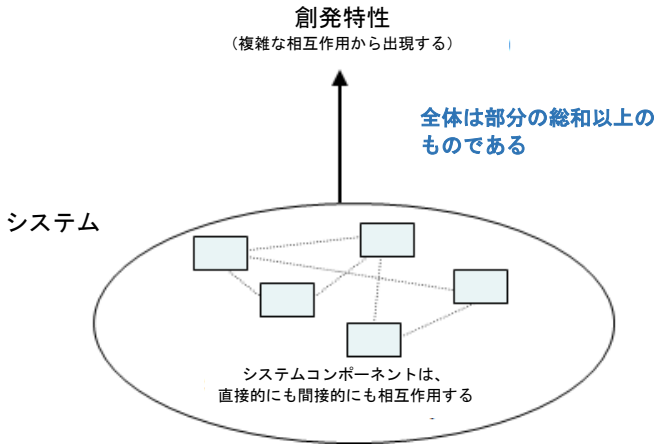


図 8：システム理論における創発特性

- 創発特性は、システムの各部分間の関係、すなわち、それらがどのように相互作用し合い、適合するかによって生じます。

創発特性が、個々のコンポーネントの振る舞いあるいはコンポーネント間の複雑な相互作用から生じる場合には、安全性のような創発特性を制御するには、個々のコンポーネントの振る舞い及びコンポーネント間の相互作用の両方をコントロールする必要があることは理にかなっています。この目的を達成するために、システムに対するコントローラ（controller）を追加できます。コントローラは、システムに対するコントロールアクション（control action）を提供し、コントロールアクションの影響を判断するためのフィードバックを得ます。工学においては、これは標準的なフィードバックコントロールループ（付録Eを参照）です。

コントローラは、*システムの振る舞いに制約を強制*します。安全制約の例としては、航空機や自動車は最小限の間隔をあけなければならないこと、深海井戸の圧力は安全レベル以下にしなければならないこと、着陸しない限り航空機は十分な揚力を維持しなければならないこと、有害物質を発電所から放出してはならないこと、偶発的な爆発や兵器の発射があってはならないことなどが挙げられます。

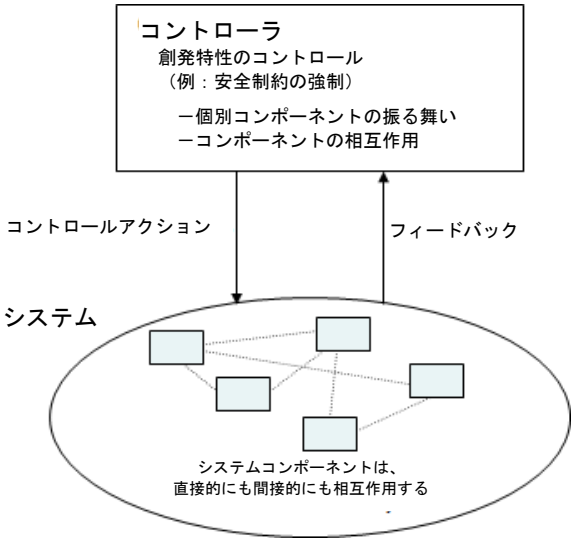


図 9：コントローラは、振る舞いに制約を強制する

コントロールは幅広く解釈されており、したがって、安全工学で現在行われているすべてのことに加え、さらに多くのことが含まれます。例えば、コンポーネントの故障及び非安全な相互作用は、冗長性、インターロック、障壁、またはフェイルセーフ設計を使用するなどの設計によってコントロールすることができます。安全もまた、開発及び訓練プロセス、製造プロセス及び手順、保守プロセス並びに一般的なシステムオペレーティングプロセスのようなプロセスを通じてコントロールすることができます。最後に、安全は、政府の規制、文化、保険、法律及び裁判所、または個人の利益を含む社会的規制を用いてコントロールすることができます。人間の振る舞いは、社会的または組織的なインセンティブ構造、あるいはその他の管理プロセスの設計を通じて部分的にコントロールすることができます。

安全コントロールストラクチャーは安全制約を強制します。システムに特定の振る舞いを課する責任は、システムのコントロールストラクチャー全体に分配されます。図10は、一般的な例です。システム全体の運用におけるシステム安全制約の不十分な強制によって、事故は生じます。言い換えれば、安全コントロールストラクチャーの脆弱性は、システム安全制約の違反、ひいては損失につながります。

複雑な社会工学システムを扱うには、問題の社会的側面と技術的側面の両方をモデル化して分析する必要があり、両方を組み合わせて分析することができます。図10は、米国の典型的な規制された産業の階層的な安全コントロールストラクチャーの例です。国際的なコントローラを含めることができます。図の右下の運用プロセス（ほとんどの事故分析の焦点）は、安全コントロールストラクチャーの一部に過ぎません。

図10に示す二つの基本的な階層的コントロールストラクチャーは、システム開発（左側）とシステム運用（右側）のためのもので、両者の間には相互作用があります。ストラクチャーの各レベルには、下位のレベルのコンポーネント間の相互作用とコンポーネントの振る舞いを制御する責任を持つコントローラが含まれています。より高いレベルのコントローラは、全体的な安全方針、規格及び手順（下向き矢印）を提供し、事故及び事故報告書を含む様々な種類の報告を通じてそれらの影響に関するフィードバック（上向き矢印）を得ることができます。例えば、企業の経営者は、安全方針、規格、資源を提供し、企業の運営に関する報告書の形でフィードバックを得ます。フィードバックは、安全コントロールの有効性を、学び、そして改善する能力を提供します。

メーカーは当初の安全分析の基礎となった運用環境に関する想定、例えば、保守の品質と手順、並びに安全な運用手順に関する情報を顧客に伝達しなければなりません。同様に、運用環境は、製造者、および場合によっては政府当局などの他の者に、運用中のシステムの性能に関するフィードバックを提供します。階層的安全コントロールストラクチャーの各コンポーネントは、そのコンポーネントに適した安全制約を強制する責任を有しており、これらの責任が一体となってシステム全体の安全制約を実施するべきです。

「コントロール」 という用語の使用は、厳密な命令や制御構造を意味しないことに注意が必要です。振る舞いは、工学的なシステムや直接的な管理介入によってコントロールされるだけでなく、方針、手順、共有価値システム、その他の組織文化の側面によっても間接的にコントロールされます。すべての振る舞いは、その振る舞いが起こる社会的および組織的なコンテキスト（context）に影響され、少なくとも部分的に「コントロール」されます。このコンテキストを「エンジニアリング（工学）」することは、安全文化、すなわち、組織または社会の参加者による安全についての一般的な考え方を反映する組織または社会の文化の部分集合を、創造し、変えるための効果的な方法であり得ます。[12]実用的意義については、ハンドブックの中でこれ以降、説明します。

[12] Edgar Shein, *Organizational Culture and Leadership*, San Francisco: Jossey Bass, 2004

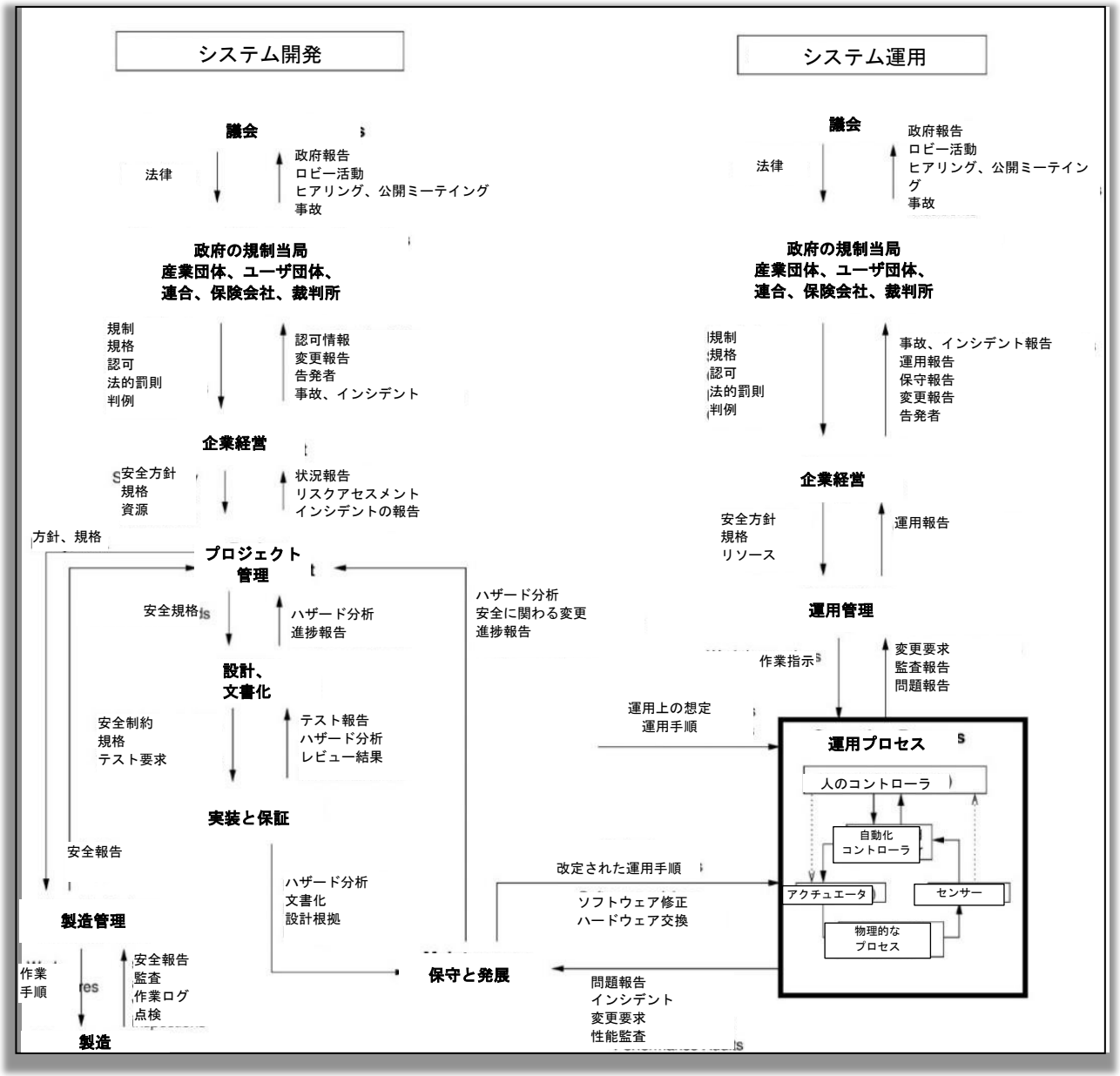


図 10：一般的な安全コントロールストラクチャー

重大な事故から学んだように、経営上及び組織上の要因、およびしばしば政府による統制（または、統制の不足）は、事故の原因及び防止における技術的要因と同様に重要です。紙面の都合上、図10は、安全コントロールストラクチャーのハイレベルなコンポーネントを強調しており、それらの詳細な設計は強調していません。そのそれぞれが非常に複雑であり、なぜ事故が起こったのかを理解するために包括的に調べる必要があります。

図11は、コントロールストラクチャーのレベル間の相互作用の基本形式を示しており、コントローラは、コントロール対象のプロセス（controlled process）にコントロールアクションを与えます。工学では、これをフィードバックコントロールループと呼びます。以下に示すように、効果的な管理 （責任、権限および説明責任の割り当て） のための標準的な要件は、コントロールストラクチャーの設計と仕様の一部です。

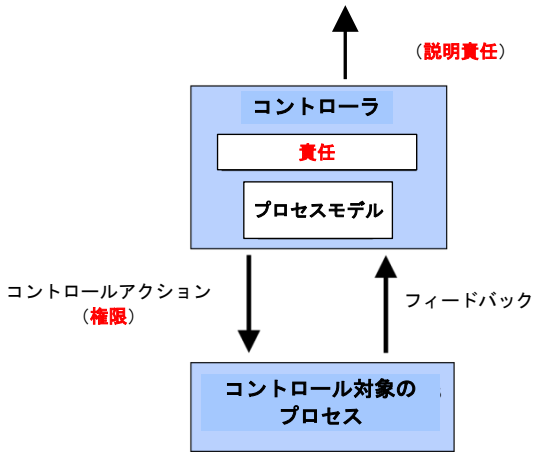


図 11：安全コントロールストラクチャーの基本コンポーネント

コントローラは、例えば、リフトを制御するために航空機の制御面にコマンドを発行すること、または、化学プラントでは、タンク内の圧力の安全レベルを維持するためにバルブを開閉することなど、システム安全制約を実施することに関して、コントローラに割り当てられた責任を有します。コントローラ（人間であっても自動であってもよい）は、コントロールしている（権限を有している）プロセスに対してコントロールアクションを発行することで、これらの責任を果たします。コントローラは、コントロールされているプロセスからのフィードバックによって特定される、コントロール対象のプロセスの現在の状態を前提として、ハザードを防止する責任を果たすためにどのような種類のコントロールアクションが必要かを決定します。

上位コントローラの一例として、FAAは米国内の飛行の安全を監督する責任を負っています。この機関は、責務を遂行するために、耐空性に関する助言、通達、FAA規則、ハンドブック及びマニュアル、航空従事者への通知（NOTAMs）、方針及び指導等様々な種類のコントロールアクションを有しています。フィードバックは、航空輸送システムの安全性の現在の状態を判断するために、報告システム、事故・インシデント分析、監査、検査などの形式で行われます。最終的にFAAは、運輸省、連邦議会、および一般市民に対する責任があります。

フィードバック情報は、*プロセスモデル（process model）*と呼ばれる、コントロール対象のプロセスに関するコントローラのモデルに組み込まれます。プロセスモデルは、コントローラが人間の場合は、*メンタルモデル*と呼ばれることもあります。事故は、コントローラのプロセスモデルがプロセスの実際の状態と矛盾し、結果としてコントローラが非安全なコントロールを提供する場合にしばしば生じます。例えば、航空管制官は、2機の航空機が衝突経路上にないと考え、一方または両方の経路を変更しない場合があります。他の例としては、パイロットが特定の操縦を安全に行うための十分な訓練と専門知識を持っていないのに、持っていると信じている航空会社の経営者や、氷結していないのに氷結したと思っているパイロットがあげられます。

単純なフィードバックコントロールループでは、コントローラは、航空機の操縦かんをプルバックする、プラントのバルブを開くなどのコントロールアクションを実行します。「アクチュエータ」（簡略化のため図示していません）はコントロール対象のプロセスにおいてそのコントロールアクションを実行します。フィードバックは通常、コントローラがコントロールアクションの効果を判断し、次に何をすべきかを決定できるように、システム上に設計されます。

ここで、フィードバックの重要性が明らかになります。フィードバックは、コントローラが必要なコントロールアクションを決定するために使用する現在のプロセスモデルまたはメンタルモデルを通知します。工学では、効果的なコントロールを行うために、すべてのコ

ントローラにコントロール対象のプロセスのモデルを含める必要があります。このプロセスモデルまたはメンタルモデルには、コントロール対象のプロセスがどのように動作するか、およびコントロール対象のプロセスの現在の状態に関する想定（assumption）が含まれます。これは、システムの効果的な運用に必要なコントロールアクションを、決定するために使用されます。例えば、パイロットのメンタルモデルは、姿勢及び操縦面の状態のような、物理的な航空機に関する情報が含まれるでしょう。航空機が制御の自動化（今日のほとんどすべての航空機に当てはまる）を有する場合、パイロットは、自動化（automation）がどのように動作するか、および操作モードなどの自動化の現在の状態に関する情報を有していなければなりません。自動化は、物理コントロールストラクチャーの現在の状態など、プロセス状態のモデルも有しています。

複雑なシステムにおける事故は、コントローラによって使用されるプロセスモデルと実際のプロセスの状態との間の不整合に起因することが多く、その結果、コントローラが非安全なコントロールアクションを提供することになります。例として、自動操縦ソフトウェアが、実際には降下しているにもかかわらず上昇していると判断し、誤った制御規則を適用する；軍のパイロットが、味方の航空機を敵であると考え、その航空機に向けてミサイルを発射する；ソフトウェアが、宇宙船が着陸したと考え、早めに降下エンジンを停止させる；早期警報システムが、国が敵意を持つ人物の標的になったと判断し、味方の標的に向けて迎撃ミサイルを発射する、などがあげられます。誤ったプロセスモデルが、意図的ではない原因によるものか、意図的な原因によるものかは問題ではないということに注意が必要です。つまり、セキュリティを同様に扱うことができるということです。イランの原子炉プログラムのStuxnetワームがその一例です。このワームは、コントローラのプロセスモデルに、遠心分離機の回転が実際よりも遅いと思わせました。コントローラは遠心分離器に「増速」コマンドを送ることで摩耗を早め、イランの核兵器開発を遅らせました。

効果的な安全コントロールストラクチャーを設計する際の課題として、コントローラが持つコントロール対象のプロセスのモデルを、コントロール対象のプロセスの実際の状態と一致させるために、必要なフィードバックと入力を提供することがあげられます。なぜ事故や損失が発生したのかを理解する上で重要な要素は、システムの振る舞いに対する安全制約を強制するうえで、コントロールがどのように、そしてなぜ効果的でなかったのかを究明することです。これは、しばしば、コントローラで使用されているプロセスモデルが、何かしら不正確であったか、または不適切であったためです。

要約すると、システム理論を用いると、事故は、システムコンポーネントの故障から生じるのではなく、安全コントロールストラクチャーがシステムの振る舞いに対する制約を維持できないことから生じています。例えば、衝突を回避するには、航空機を空中に保つ揚力が不十分である、あるいは、不変の地形からの距離が十分に保たれていない、などです。物理的な故障が発生してコントロールが不十分になることもありますが、考慮すべき点はまだ数多くあります。

システム理論を安全へ適用するには、現在使用されているものを拡張する新しい事故因果関係モデルが必要です。STAMP （System-Theoretic Accident Model and Processes）は 、システムコンポーネント間のより複雑なプロセスや非安全な相互作用を含めるために、直接的に関連する故障の事象やコンポーネントの故障の連鎖を超えて、因果関係の従来のモデルを拡張します。[13] STAMPでは、事故は、物理システム、人間、社会システムの間の複雑な相互作用によって引き起こされます。安全性は故障防止の問題というよりも動的なコントロールの問題として扱われます。STAMPモデルから除外されている原因はありませんが（事象連鎖モデルは（STAMPモデルの）サブセットです）、さらに多くの原因が含まれており、重点は、故障の防止から、システムの振る舞いに対する制約の強制へと変わります。

[13] Nancy G. Leveson, Engineering a Safer World, MIT Press (2012), Cambridge MA.を参照してください。

STAMPを利用するいくつかの利点を以下に示します：

- ボトムアップではなく、抽象度の高いレベルからトップダウンで機能するため、非常に複雑なシステムに適用されます。
- ソフトウェア、人、組織、安全文化などを区別せずに、事故や損失の原因として扱います。

STAMPはCASTの基礎となる事故因果関係モデルです。

要約すると、事故因果関係モデルおよび損失が発生した理由を分析するために用いられる情報は、特定された原因と事故調査の結論に大きな影響を与えます。それではCASTの紹介に入りますが、まずはその目的から始めましょう。

改善された事故分析手法の目的

これまでに示されてきたことをまとめると、「根本原因」と呼ばれるものを特定したり、責任に焦点を当てることは、事故調査において考慮することを不必要に制限することになります。あまりにも多くの要因が見逃され、解決されません。また、損失の後、誰もが他人を非難しようとするので、調査の範囲と有効性を制限することになります。

それよりも、原因分析の目的は、将来の失敗を防ぐために損失から学ぶことであり、非難すべき人やものを見つけることではありません。これらの人々の多くは、たいていは低レベルのオペレータで、損失が避けられないシステムに取り込まれただけであり、その人が不運にも引き金となってしまった、もしくは「起こるのを待っている」事故の事象に巻き込まれてしまったということです。

事故及び事象からの学習を最大化する事故分析手法は、以下の目的を持つべきです。

1. いくつかのいわゆる「根本」または「想定（probable）」原因に焦点を当てず、すべての原因(学習を最適化する)を含める。
2. 後知恵バイアスを減らす。
3. 人間の振る舞いに対して、システムの考え方を用いる。
4. 「誰」よりも、「なぜ」と「どのように」を考慮して、損失が発生した理由を非難のない説明で提供する。
5. 特定の種類の損失を防止するために策定されたコントロールが、当面の事例において効果的でなかった理由、そして、将来同様の損失を防止するために、安全コントロールストラクチャーを強化する方法に重点を置いた、包括的な事故因果関係モデルを使用する。

CASTは、これらの目的を念頭に置いて作成されており、複雑な事故を調査してきた数十年間の経験を基に開発および改良されてきました。このハンドブックの残りの部分では、CAST分析の方法について説明します。

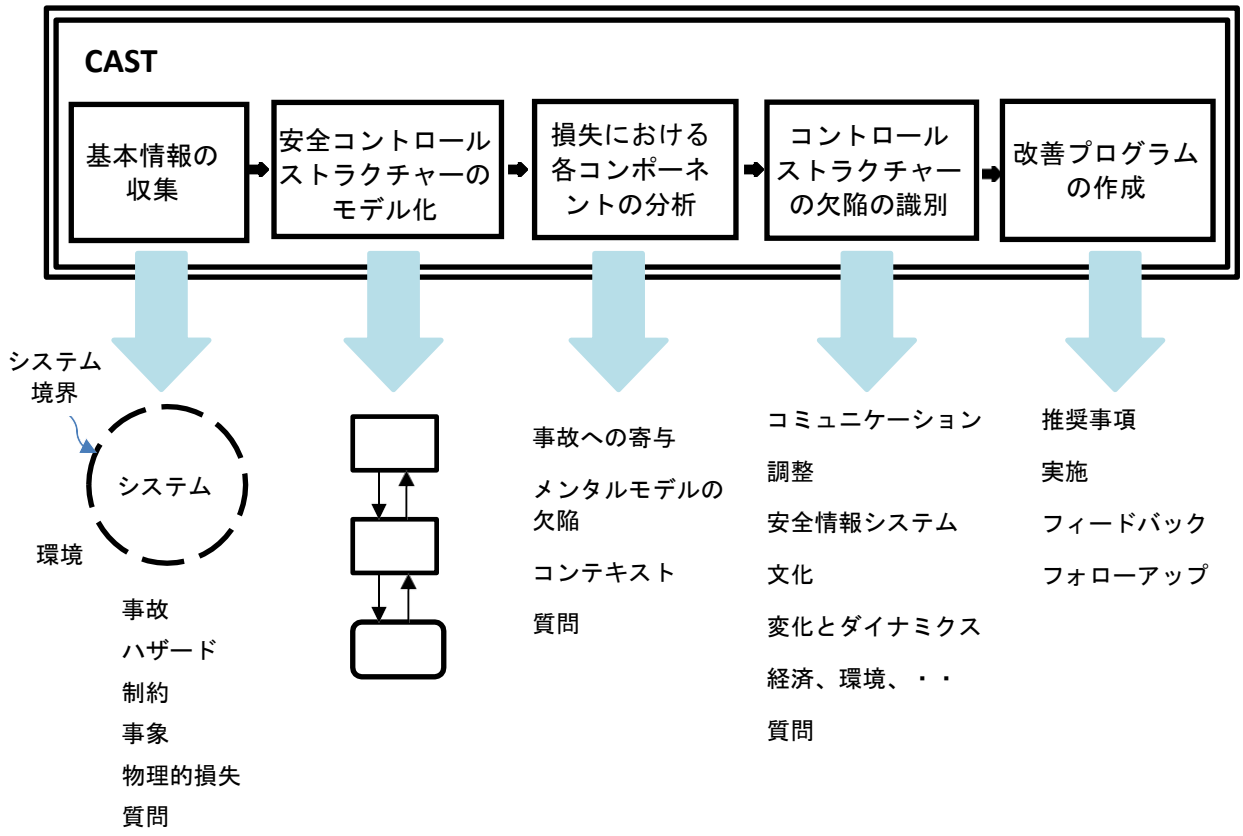
第４章：CAST分析の実施

CASTの基本コンポーネント

CAST（Causal Analysis Based on Systems Theory：システム理論に基づく因果分析）は、システムの視点から事故原因を分析するための構造化された手法です。[14] CASTは評価技術ではありません。しかし、事故調査を進める際にCAST分析を行うことは、損失が発生した理由を包括的に説明し、将来の関連事故を防止するための推奨事項を策定するために、調査中に回答する必要のある質問と収集する必要のある情報を特定するのに役立ちます。

STAMPでは、事故の原因は、損失を防ぐことができなかった安全コントロールストラクチャーであると定義しているので、事故調査の目的は、安全コントロールストラクチャーが、破られた安全制約を強制できなかった理由を特定することと、将来関連する損失を防ぐためにコントロールストラクチャーに必要な変更を判断することです。ほとんどの場合、調査者は、安全コントロールストラクチャーの低いレベルだけでなく、すべてのレベルにおいて不適切なコントロールが提供されていたことを見つけるでしょう。

CASTは５つのパートで構成されます。



[14] 商用航空安全チーム（Commercial Aviation Safety Team）に同じ頭字語が使われているのは残念なことです。どちらの用途も長い間存在していたため、単純な解決策はないようです。このハンドブックでは、CASTは常にシステム理論に基づく因果分析（Causal Analysis based on System Theory）を意味するために使用されます。

CAST分析の基本的なコンポーネント

1. 分析を実行するための基本的な情報の収集：

a. 関連するシステムと分析の境界を定義する。

b. 損失と損失につながった危険な状態を説明する。

c. ハザードから、ハザードを防止するために必要なシステムレベルの安全制約（システムの安全要求および制約）を識別する。

d. 結論付けたり非難することなく、何が起こったのか（事象）を説明する。事象が発生した理由を説明するために回答する必要がある質問を生成する。

e. 物理的な機器とコントロールに関する物理的な喪失、関連するハザードを防止するための物理的な設計要求、この種の事故を防止するために設計に含まれる物理的なコントロール（緊急および安全のための装置）、故障とハザードを引き起こす非安全な相互作用、事故を防ぐはずだった物理的なコントロールの欠落または不適切さ、および、事象に影響を与えるあらゆるコンテキスト要因、について分析する。

残りの分析の目的は、損失を許した安全コントロールストラクチャーの限界と将来それをどのように強化するかを特定することです。

2. この種のハザードに対する既存の安全コントロールストラクチャーをモデル化する。

3. コントロールストラクチャーのコンポーネントを調べ、それらが損失の防止に効果的ではなかった理由を判断する：コントロールストラクチャーの下部から開始し、各コンポーネントが事故で果たした役割とその振る舞いの説明を示す（何をしたのか、なぜそのようにしたのか、また、なぜその振る舞いがその時にすべき正しいことだと思ったのか）。

4. 損失に寄与したコントロールストラクチャー全体の欠陥（一般的な体系的要因）を特定する。体系的要因は個々のシステムコントロールストラクチャーのコンポーネントにまたがる。

5. 将来同様の損失が発生するのを防ぐために、コントロールストラクチャーの変更に関する推奨事項を作成する。可能なら、全体的なリスク管理プログラムの一環として、このハザードに対する継続的改善プログラムを設計する。

これらは厳密なステップや直線的なプロセスではありません。最初の２つのパートは後の活動のための基本的な情報を提供し、少なくとも他のパートを試みる前に開始する必要があるかもしれませんが、それぞれのパートの作業は、適切かつ実用的と考えられる調査を通して進めることができます。調査中にさらに多くのことが学ばれるにつれて、分析が再検討され、結果が変わる、あるいは、不足が補われます。

より多くのことが学ばれるのと同様に、各ステップには、後で答えるために質問を生成することが含まれます。その質問は、損失が発生した理由を詳しく説明するために何を学ぶ必要があるかを、評価者が判断するのに役立ちます。調査の最後の目的は、すべての質問に答えられるようにすること、またはそれらに回答できないと決定することです。質問に対する回答は、事象の「理由」を提供します。

分析結果を記録するために必要なフォーマットは、このハンドブックでは提供されません。 異なる状況では、異なるフォーマットが適切な場合があります。いくつかの例が章の最後に提供されていますが、目的のためにより良いフォーマットが見つかるでしょう。さらに、航空などの一部の業界では、最終調査報告書に必要なフォーマットと内容があります。これは、CAST分析自体のフォーマットに影響を与える可能性があります。

このハンドブックでは、CASTプロセスを説明するために実行中の分析例を使用します。それは本当の事故：オランダのシェル ムールダイク工場で2014年6月3日に発生した化学

反応器の爆発と火災です。内容物は広い環境に放出された一方、反応器の区画は250メートルにわたって爆破され、その他の破片は800メートル離れた場所で後に発見されました。爆発は20キロ離れたところでも聞こえました。爆発した反応器の反対側で働く２人の人は、爆発の圧力波と、周囲に飛びかう高温で燃焼している触媒ペレットに襲われました。大規模な激しい火災が起こり、かなりの量の煙が発生しました。



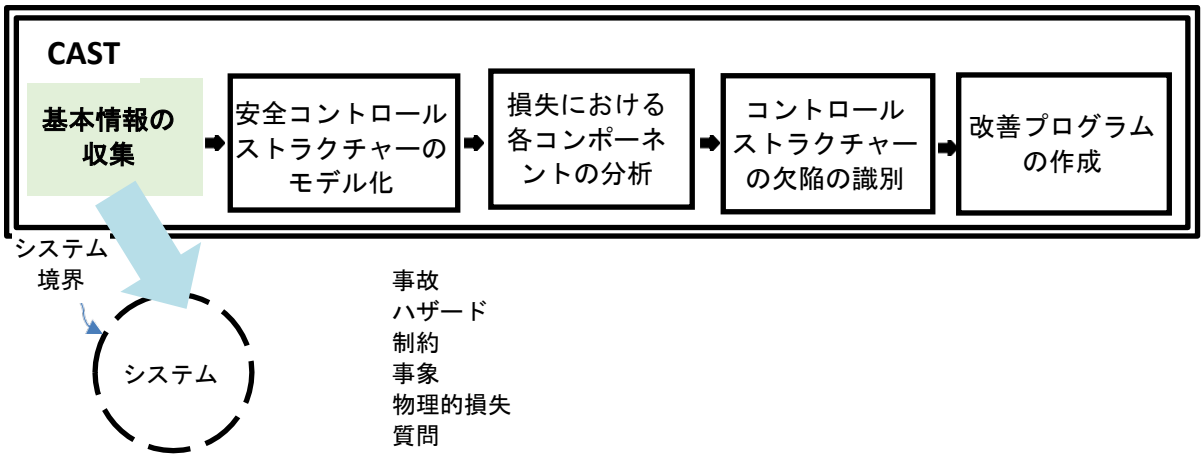
図 12：シェル ムールダイク爆発

ここで使用されている実行例を含む、さまざまな事故に関する実際のCAST分析のオンライン例へのリンクは、付録Ａに記載されています。

この事故の完全なCAST分析はこのハンドブックに含めるには大きすぎますが、付録Ａに提供されているリンクを通してオンラインでアクセスすることができます。CASTの例を理解するために必要なもの以上の、化学プロセスに関する技術情報については、完全なCAST分析結果の要約と共に付録Ｂに記載されています。

この章の残りの部分では、この事故を例に、各CASTプロセスのステップがどのように実行されるかを説明します。説明と例を読みながら、ご自身がよく知っている事故について、CASTのステップを経験することをお奨めします。

基本情報の収集



1. 分析を実行するための基本的な情報の収集：

a. 関連するシステムと分析の境界を定義する。

b. 損失と損失につながった危険な状態を説明する。

c. ハザードから、ハザードを防止するために必要な、システムレベルの安全制約（システムの安全要求および制約）を識別する。

d. 結論付けたり非難することなく、何が起こったのか（事象）を説明する。事象が発生した理由を説明するために回答する必要がある質問を生成する。

e. 物理的な機器と制御に関する物理的な喪失、関連するハザードを防止するための物理的な設計要求、この種の事故を防止するために設計に含まれる物理的な制御（緊急および安全のための装置）、故障とハザードを引き起こす非安全な相互作用、事故を防ぐはずだった物理的な制御の欠落または不適切さ、および、事象に影響を与えるあらゆるコンテキスト要因、について分析する。

残りの分析の目的は、損失を許した安全コントロールストラクチャーの限界と将来それをどのように強化するかを特定することです。

最初のステップは、何が起こったのかについての基本的な情報を収集し、分析の目的を特定することです。発生したシステムハザードと安全制約への違反が最初に特定されます。

一見単純で明白なように思われますが、ハザードと安全制約は、ハザードを防ぎ、安全制約を強化するために、安全コントロールストラクチャーに含まれるコントロールを識別するのに重要です。すべての制約とコントロールから始めるのは非効率的です。

まず、関心のあるシステムの境界を特定することから始めます。シェル ムールダイク事故において分析されたシステムは、化学プラント、その設備、プラント内の作業者、ならびに工場周辺の公衆です。損失は、保守停止後に始動中であったユニット4800の爆発を含みます。詳細は付録Ｂに記載されています。

次に、損失につながったハザード、およびシステムの設計と運用において満足すべき制約を特定します。

システムハザード1：公衆または作業者の有害化学物質への曝露

安全制約：

1. 作業者と公衆が潜在的に有害な化学物質にさらされてはいけません。
2. 発生した場合には、曝露を低減するための対策が講じられなければなりません。
3. プラントの内部または外部で曝露された個人を治療するために、利用可能で、効果的な手段があり、そして使用されなければなりません。

システムハザード2：爆発（制御不能なエネルギー放出）および/または火災

安全制約：

1. 化学物質は常に確かなコントロール下になければならない、すなわち暴走反応を防止しなければなりません。
2. プラント内の作業者を保護し、外部コミュニティへの損失を最小限に抑えるために、警告やその他の対策が利用可能でなければなりません。
3. プラント内外の爆発や火災に対処するために、利用可能で、効果的な手段があり、使用されなければなりません。

この事故の場合、２つのハザードが発生しました。制約には、調査の懸念と考慮すべき安全コントロールストラクチャーが含まれますが、これらはプラント自体の境界を超えて、実際にはシェル社の責任を超えて拡張されます。例えば、公衆（地域社会）衛生に対する責任は、化学プラントの所有者単独の責任ではありませんが、法律上、参加することを義務付けられている場合があります。

ハザードから安全制約を導出することは、ハザードが回避されない場合に対処するための制約を含めることを除いて、かなり明白です。 化学プラントのためのシステムハザード１（*公衆または作業者の有害化学物質への曝露*）の最初の安全制約は、単純に、ハザードを目的文、例えば、作業者と公衆は潜在的に有害な化学物質にさらされてはならない 、といった文に変換することです。

２番目と３番目は見逃されやすい制約です。安全制約が強制されない可能性は常にあります。その場合、ハザードを回避することはできませんが、ハザードが発生した場合に、ハザードを軽減し、潜在的な害を軽減することは可能です。それが２番目と３番目の安全制約の目的であり、システムおよびシステム環境の設計者およびコントローラに対して、以下の項目について適切な対応を要求します。

(1) ハザードが発生した場合に、ハザードの影響をできるだけ軽減すること

(2) ハザードの影響を完全に軽減できない場合は、潜在的な損失を最小限に抑えること

ハザード自体を特定することは少し面倒です。第１章では、ハザードとは、設計中のシステムのコントロール下、またはシステムの境界内にあるべきものとして定義されています。その議論はここでは繰り返しません。エンジニアリングにおいては、設計者とオペレータは自分がコントロールしているものだけを防ぐことができます。さらに、設計や運用は、予想されるケースや平均的なケースではなく、最悪の環境を考慮して実行されなければいけません。

一般的な間違いは、システム全体に関するハザードではなく、システムコンポーネントに関するハザードについて記述することです。システムコンポーネントの故障や非安全な振る舞いはシステムのハザードではなく、ハザードの原因です。原因はCASTプロセスの後半で特定されます。システムレベルから始めて、後でシステムハザードの原因を生成することで、因果分析において、パズルのピース全体を省略してしまう可能性がはるかに低くなります。また、原因が欠落している際に識別しやすくなります。

ここでは、適切なシステムハザードの例とそうではない例を挙げます。

システムハザード：航空機は失速し、揚力を得るのに十分な対気速度を持っていない。
非システムハザード：エンジンは飛行に十分な推進力を提供していない。
非システムハザード：パイロットは失速を防ぐ、または対処するための迎角を保持していない。

システムハザード：自動車は、先行車からの最小車間距離に違反している。
非システムハザード：運転手は、最小車間距離に違反して自動車を運転している。
非システムハザード：自動運転は、先行車からの最小車間距離への違反を避けるための、車の減速を適切に行わない。
非システムハザード：ブレーキの故障。

システムハザード：化学プラントでの爆発と火災。
非システムハザード：圧力開放弁の故障。

非システムハザード：反応器の過加圧。
非システムハザード：反応器の圧力に対するコントロールを持続しないオペレータ。
非システムハザード：製造されている化学物質に対する不適切な反応器設計。

ハザードの仕様にこれらの制限が課されるのはなぜでしょうか？誤ったシステムレベルのハザードの最後の例である「製造されている化学物質に対する不適切な反応器設計」を考察します。問題は、その化学物質がそもそも生産されるべきだったかどうか、あるいは当時存在していたより大きな工場の条件下で生産されるべきだったか、という疑問を無視していることです。その代わり、反応器の設計に焦点を当てており、損失の一因となった可能性がある工場の他の構成要素の運用には焦点を当てていません。影響を与えたかもしれない経営上の決定を無視しています。その代わり、システムの一部の物理的設計レベル、つまり反応器の設計自体に調査を集中させてしまいます。

覚えておいて欲しいのは、私たちの目的は単に事象の説明を見つけることではなく、学習を最大化し、将来の損失をできるだけ多く防ぐために、最も包括的な説明と損失へのすべての寄与を識別することです。あるコンポーネントの動作に注目すると、他のシステムコンポーネントの寄与や、自動車、運転手、自動車とドライバーの間のインターフェースの設計など、複数のコンポーネント間の相互作用が見逃されることになります。たとえあったとしても、一つのシステムコンポーネントだけが損失に関与していることはまれであり、焦点を絞りすぎると、重要な情報が失われます。

必要であれば、この時点で事象を明確にすることができます。 損失調査において、事象の連鎖の有用性は限られているため、それを生成することはCAST分析の完了には必須ではありません。実際には、それにより、注意が向けられるべき場所から注意をそらしてしまう可能性があります。事象だけに焦点を当てても、事象が発生した理由を判断するために必要な情報は提供されません。その情報を提供することが、CAST分析の目的です。

CAST分析の開始に必須ではありませんが、損失の前に発生した近接事象を識別することは、事故調査や因果分析で回答を要する質問を生成するプロセスの開始に役立つ場合があります。表1は、シェル ムールダイクでの爆発に至るまでとそれに続く主要な近接事象、および事故分析が答えるべきいくつかの質問を示しています。繰り返しになりますが、目的は、将来このような事故を防止する方法を特定することであり、非難する誰か、あるいは何かを見つけることではありません。

事象をリスト化する目的は、１つまたはいくつかを選択して、損失の原因として識別するためではないことを忘れないでください。その目的は、全体的な因果分析で使用される調査のための質問を生成することです。事象を記述する際に、オペレータが失敗した、あるいは“やるべきだった”などの非難を含む言葉を使用しないでください。これらは暗に結論と非難を意味します。ハードウェアやオペレータが行ったことと行わなかったことを、単に記述してください。

表 1：シェル ムールダイク損失に至るまでの近接事象

ID	事象	挙げられた質問の例
1.	プラントは、触媒ペレットを交換するための短時間の定期保守停止（ピットストップと呼ばれる）のためにシャットダウンされており、爆発時に再起動が行われていました。	*事故は通常、何らかの種類の変化（計画的または計画外）の後に発生します。通常、この変化には、シャットダウンや起動、定期保守（回避策または一時的な「修正」を含む）が含まれることがあります。 工場と会社にMOC（変更管理）ポリシーがありましたか？もしそうなら、それに従うことになっていましたか？それに従われなかったならば、それはなぜですか？それに従ったとして、なぜそれが効果的でなかったのでしょうか？*
2.	再起動手順の１つに、エチルベンゼンを含む反応器の暖機があります。 暖機（再加熱）プロセス中に、コントロールされていないエネルギーが放出され、そして加熱液体（エチルベンゼン）と使用された触媒ペレットとの間で予期せぬ化学反応が起こりました。	*なぜ反応が予測できなかったのですか？それらは予見可能でしたか？反応の予測のために使用できたかもしれない前兆がありましたか？オペレータは爆発の前にこれらの反応を検出しましたか？そうでないならば、その理由は何ですか？もし検出したのなら、なぜ彼らは反応をコントロールすることについて何もしなかったのでしょうか？*
3	反応はガス形成を引き起こし、反応器内の圧力を増加させました。	*この圧力の増加の可能性を設計上考慮しましたか？ そうでない場合は、なぜですか？このリスクは設計段階で評価されましたか？*
4	液体が排気ガスシステム（フレア）に入るのを防ぐように設計された自動保護システムが作動しました。しかし、液体がフレアに入るのを防ぐと、システム内のガスが排出されなくなり、反応器内の圧力が上昇します。	*オペレータはこれに気付きましたか？それは検出可能でしたか？なぜ彼らは反応しなかったのですか？これは予測可能な設計上の欠陥のようです。２つの要件（液体がフレアに入るのを防ぐこととガスをフレアに放出する必要があること）の間の安全でない相互作用は、設計またはハザード分析の取り組みで特定されましたか？もしそうなら、なぜそれは設計や運用手順で扱われなかったのですか？それが識別されなかったならば、その理由は何ですか？*
5	*反応器を継続的に暖機すると、エチルベンゼンと触媒ペレットとの間でより多くの化学反応が起こり、より多くのガスが形成され、反応器内の圧力が上昇しました。*	*圧力の増加が検出されて処理されなかったのはなぜですか？警告があったとしても、なぜそれらが圧力の増加に対処する効果的な行動をもたらさなかったのでしょうか。自動過圧制御装置（例えばリリーフバルブ）があった場合、なぜそれら*

		は効果的ではなかったのでしょうか。自動装置がなかったのであれば、その理由は何でしょうか。それらを提供することは実現不可能でしたか？
6	*圧力は非常に速く上昇したため、圧力除去装置によってコントロールすることができず、そして反応器は高圧のために爆発し、そして分離容器は崩壊して爆発が起きました。*	*より効果的な圧力解放を提供することは不可能でしたか？それが可能だった場合、なぜそれが提供されなかったのでしょうか。この種の圧力上昇は予想されましたか？それが予想されていたとしたら、それはなぜ設計や運用手順で扱われなかったのでしょうか。それが予想されなかったならば、その理由は何ですか？*
7	*反応器の内容物およびその関連分離容器はより広い環境に放出されました。破片が後に800メートル離れて発見され、反応器の区画は250メートルにわたって爆破されました。爆発は20キロメートル離れたところでも聞こえました。*	*内容物を管理区域（バリア）、少なくとも触媒ペレット内に封じ込める方法はありましたか。*
8	*爆発時にユニット4800の反対側で作業していた２人が爆発の圧力波と飛んでいた燃焼している触媒ペレットに襲われました。*	*危険な操作をしているときに、反応器周辺が隔離されなかったのはなぜですか？触媒ペレットが飛散するのを防ぐことができなかったのはなぜですか？*
9	*大規模で激しい局所的な火災が発生し、かなりの量の煙が発生しました。*	
10	*地域消防、医療、危機管理、そして危機コミュニケーションが開始されました。*	

「失敗した（failed）」という単語は、事象説明のどこにも現れていません（物理コンポーネントの失敗が発生しない限り、CAST分析のどこにも現れません）。また、「オペレータは持っているべきだ…」といった後知恵バイアスの文もありません。判断や結論を出すには時期尚早です（これは後であっても避けるべきです）。さらに、分析のこの早い段階で特定された質問は非常に一般的です。より多くのことが学ばれるにつれて、これらの質問は洗練され、その答えはさらに多くの質問を生み出すでしょう。最後に、目的はすべての質問に答えること、または答えられないと判断することです。答えをまとめると、なぜこの事故が発生したのか、またなぜ制御装置や保護装置が事象の影響を軽減しなかったのかについての詳細な理解が得られます。

ここで提供されている事象連鎖の例は「完全（complete）」からは程遠いものです（もっと多くの事象が常に追加される可能性があるため、どのような意味においても）。実際、それらの完全性はCAST分析の結果にほとんど影響を与えません。答えが必要な質問がここにない場合には、後で生成されます。明らかでない場合は、事象連鎖が開始点を提供するだけです。繰り返しになりますが、CAST分析を行うときには、事象連鎖から始めることは、厳密には必要ではありません。

推奨される演習：よく知っている、または起きたことの詳細な説明にアクセスできる事故を取り上げてください。リストを完全にする必要はありません。これは出発点にすぎません。事故原因を理解するために回答される必要のある事象に関する質問を作成します。事故が非常に単純でない限り、その質問はおそらく完成しません。作成した質問は、思考における出発点を形成します。CASTプロセスを経るにつれて、より多くの質問が作成され、うまくいけば回答されます。

コントロール対象のプロセスにおいて発生したことの理解

「なぜ」何かが発生したのかを識別するためには、まず「何が」発生したのかを知る必要があります。身体的傷害または損失は必然的に物理的プロセスを含み、他の種類の損失（例えば、金銭的）は非物理的プロセスを含むでしょう。どちらの場合でも、最初のステップはコントロール対象のプロセスで何が起こったのかを理解することです。CASTは、ビジネスプロセスや犯罪および法的プロセスなど、他の種類のプロセスを含む損失にも適用できます（また適用されています）が、この章の例では物理的プロセスに焦点を当てています。次の章では、CASTを社会システムに適用する例を示します。

爆発や火災は化学プラントではよく知られているハザードです。通常、多数の保護システム、アラーム、センサ、圧力開放弁などがあります。まず、プラントの物理的コントロールを調べて、それらが爆発をコントロールしなかった理由を突き止めます。この時点で、CAST分析においては単なる物理的な失敗以上のものが考慮されることを除いて、ほとんどの事故分析で行われた分析とCAST分析では、それほど違いはありません。シェル ムールダイクの場合、物理レベルでは、CAST分析は次の物理的なコントロールの記述を生成することから開始します。

ハザード軽減のための要件：
ハザードに対する物理的保護の提供（周辺内の従業員や近隣住民の保護）

1. 暴走反応からの保護
2. 不注意による有毒化学物質の放出や爆発からの保護
3. 安全上重要な機器の状態および状態についてのフィードバックの提供
4. ハザードな状態の存在の指標（警報）の提供
5. 放出された化学物質の無害化、または危険性の低い形態への変換
6. 誤って放出された有毒化学物質を阻止する
7. 放出後の人体または環境への暴露に対する物理的保護

コントロール：
化学プラントの物理的安全装置（コントロール）は通常、上記のハザード軽減要求を満たすための一連の障壁として設計されています。シェル ムールダイク工場には標準タイプの安全装置が設置されていました。ただし、すべてが期待どおりに機能したわけではありません。
この事故に関連する緊急安全装置は次のとおりです。：

1. フレアタワーにガスを放出するための自動保護システム
2. 過過圧の場合の圧力リリーフ装置
3. アラーム
4. 反応器内の温度センサ

次に、何が起こったのかを判断します。どのような物理的な障害や相互作用がハザード

を引き起こしたのでしょうか？

失敗：圧力が臨界レベルに達した後の反応器および分離容器の最終的な崩壊を除いて、物理的コントロールのいずれも故障しませんでした。

非安全な相互作用：事故はしばしばシステムコンポーネント間の相互作用から発生します。この場合、以下の非安全な（そしてほとんど予想外の）相互作用が発生しました：

1. エチルベンゼンを触媒ペレット上に散布させる（それらを湿らせる）プロセスは乾燥ゾーンをもたらしました。これらの乾燥ゾーンには主に２つの理由がありました。：
   - 窒素流量が少なすぎました。触媒を適切に湿潤させるためには、適切な量のエチルベンゼンと窒素を適切な割合で散布板を通過させなければなりません。窒素流量が少な過ぎたため、散布板は適切に作動しませんでした。 この問題のために、他の意図しない相互作用と共に、圧力は最終的に反応器への窒素の流れを超える点まで上昇し、窒素の流れは停止し、負圧差が生じました。
   - エチルベンゼンの流れは不安定で時々低すぎました。十分に高い窒素流量に加えて、ペレットを適切に湿らせるためにはエチルベンゼンの一定かつ十分な流速が必要です。ユニット4800の２つの反応器は異なる直径を有し、これは反応器１が毎時約88トンのエチルベンゼン流を必要とし、一方反応器２が毎時約22トンを必要とすることを意味します。この容積の一定の流れが反応器１において達成されました。正しい容積の一定の流れもまた最初に反応器２に関して達成されました。しかしながら、一旦エチルベンゼンが加熱され始めると、流れは不安定になりました。爆発前の最後の1時間では、この流れは２回でほぼゼロでした。その結果、エチルベンゼンは触媒ペレット上に均一に広がらず、触媒ペレットは十分に湿潤されず、反応器２内に乾燥ゾーンが発生したのです。
2. 反応器の暖機中に放出されたエネルギーは、加熱された液体（エチルベンゼン）と乾燥ゾーンの触媒ペレットとの間に予期せぬ化学反応をもたらしました。 加熱が起こるにつれて、エチルベンゼンは触媒元素の１つ（クロム酸バリウム）と反応し始め、熱を発生しました。 エチルベンゼンはこの熱を十分に濡れた領域で消散させました。しかしながら、乾燥ゾーンでは、この熱はエチルベンゼンの欠如のために消散しませんでした。 その結果、乾燥ゾーンでは触媒ペレットがかなり加熱され、そして非常に高温の領域または「ホットスポット」が局所的に発生しました。 反応器内の温度センサの数が限られているため、ホットスポットは自動的に検出されませんでした。
3. 温度が上がるため、ホットスポット内の反応は加速し続け、それによってさらに多くの熱が発生します。局所化された温度は今や非常に高く、それはエチルベンゼンと他の触媒元素（酸化銅）との間の化学反応をもたらしました。この反応によりガスが放出されました。これらの後続の反応は互いに強めあって、もはや止めることができませんでした：暴走が起きました。急速に温度が上昇すると、局所的にエチルベンゼンが蒸発しました。
4. ガス形成は反応器内の圧力を高めました。 同時に、第２の分離容器内の最大液体レベルを超え、液体が排気ガスシステム（フレア）に入るのを防ぐために、自動保護システム（過剰な圧力を解放するために使用される）を自動的に停止させました。その結果、システム内のガスを排出することができなくなりました。液体がフレアに入るのを防ぐためのこの自動保護装置は設計どおりに作動しましたが、ガスの放出を防ぐという意図しない結果をもたらしました。

5. ガスの蓄積により圧力が上昇しました。 やがて、圧力は、設置されている自動圧力開放装置がそれを適切に解放することができない点に達しました。分離容器上の圧力解放装置は、そのような急激な圧力上昇のためには設計されておらず、そして最終的に反応器の崩壊圧力に達しました。 反応器２は崩壊して爆発し、その20秒後に最初の分離容器が爆発しました。
6. 反応器と分離容器の内容物は、ユニット4800の境界を越えて広がりました。圧力波と熱く燃えている触媒ペレットにより、その区域の作業員が襲われ、怪我をしました。
7. ３つの遠隔制御封じ込めバルブがあります。 爆発はこれらのバルブを無効にしました。別の方法として、他の制限弁の使用がありましたが、これらの弁は遠隔操作ができませんでした（手動で操作する必要があります）。発生した火災の強さと爆発の危険性があるため、これらを直ちに操作することは不可能でした。最初の試みは02:30頃に行われました。

上記では、CAST分析とは別に近接事象のリスト化を始める必要がない理由を示しています。重要な事象（失敗と非安全な相互作用）は、それらの事象から生じる質問と共に識別されます。

何が起こったのかを扱った後は、それがなぜ起こったのかを調べる必要があります。その理由のほとんどは後の分析で見つかるでしょうが、ここには物理的な設計上の欠陥とコンテキスト上の要因が含まれます。

事故を防止した可能性のあるプラントの物理的制御の欠如や不適切さ：

1. ホットスポット検出のための反応器内の温度センサの数が不適切でした。
2. 暴走を防止するための圧力開放弁がプラントに備わっていませんでした。設置されていたものは、発生した急激な圧力増加に対応するよう設計されていませんでした。

コンテキスト上の要因：

1. 触媒となる顆粒を交換する短時間の計画保守のために、プラントは運転を停止しました。
2. 次のような設計に関連する脆弱性が原因で、予期しない反応が発生しました。
   - 設計上の欠陥による不十分な湿潤（ホットスポット）の可能性。
   - エチルベンゼンの使用、および、この物質が触媒ペレット存在下では不活性という設計上の想定。

本事故における物理的コンポーネントの役割に関する要約：どの物理的コントロールも失敗しませんでした。反応器および分離容器の最終的な物理的崩壊は、圧力が臨界レベルに達した後に発生しました。これは、予期せず、取り扱われていない化学的かつ物理的な相互作用に起因していました。
これらの非安全な相互作用の多くは、反応器または安全に関する制御における設計上の欠陥の結果でした。

この記述で注意すべきことがいくつかあります。記述は物理的なシステムに限定されています。オペレータやプロセス制御システムなどは言及されていませんし、言及されるべきではありません。彼らが果たした役割については後で考慮されます。

また、CASTの基礎となる事故モデル（STAMP）では、事故がコントロールの欠如から生じると述べていることに注意してください。これには失敗に対するコントロールも含まれます。分析のこの部分では、なぜ物理的コントロールが失敗したのかについての理解が得られます。コントロールは、システムコンポーネントおよびシステム全体の振る舞いに対

する制約を強制するために使用され、不適切なコントロールの識別は、高レベルのシステムハザードおよびハザードを防止するために必要な安全制約の洗練を手助けします。

元のハザードと制約は非常に一般的なものであり、ほとんどすべての化学プラントのプロセスに適用されます。実際、これらは業界全体として識別され、あらゆる事故に適用可能です。物理的プロセスにおいて発生した特定の失敗や非安全な相互作用を特定することで、一般的なシステムハザードと安全制約を、この特定の損失向けに洗練できるため、原因分析の方向性を高めることができます。

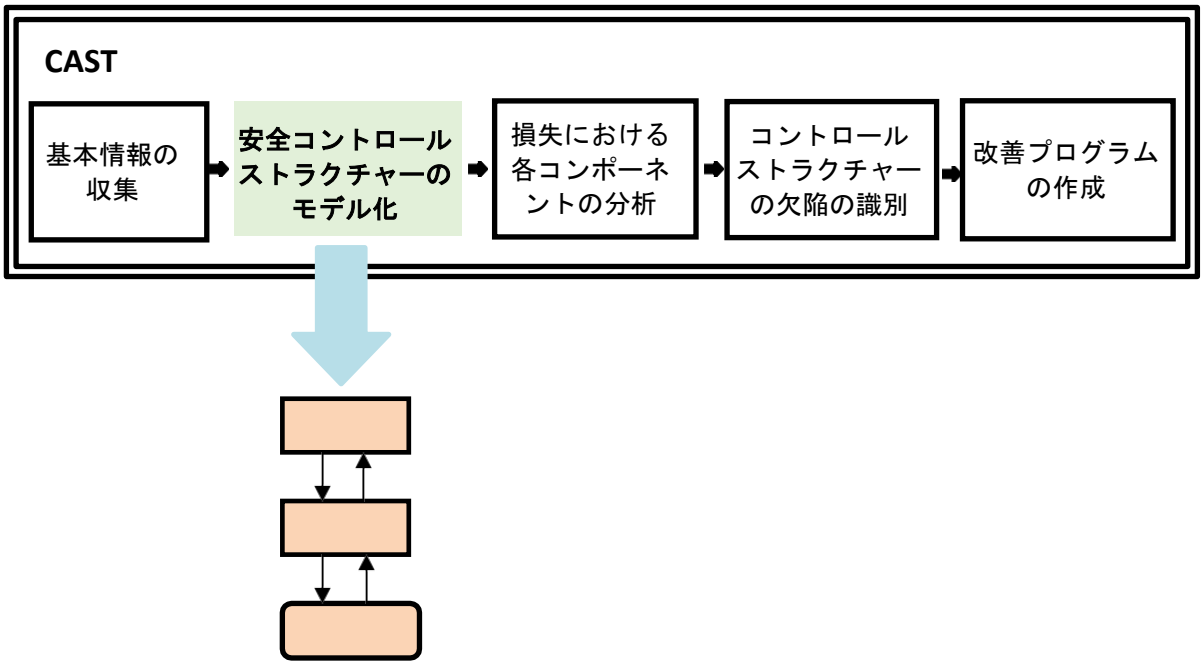
一例として、シェル ムールダイクのケースでは、化学物質を積極的なコントロール下に置くための一般的な制約を洗練することにより、違反された特定の制約を識別し、それにより、この事故のための具体的な目的を識別することができます。

1. 化学物質は常に積極的なコントロール下に置かれる必要があります。つまり、暴走反応を防止する必要があります（37ページのシステムハザード２の一般的な安全制約１を参照のこと）。
    a. 触媒ペレット上へのエチルベンゼンの散布は、反応器の再始動中に乾燥スポットを生じさせてはならない。
    b. それでも発生した場合、乾燥スポットに関連する意図しない反応によって発生する熱や圧力に対応するように保護および警告システムが作成される必要がある。

物理システム設計から関連するハザード状態を排除すること、ハザードを防止または最小限に抑えるための物理設計のコントロールを提供すること、あるいは運用上のコントロールを提供することによって、理論的に制約が課されます。通常、エンジニアリング設計が完璧になることはほとんどないため、それらすべてが使用されます。したがって、分析の目的は、設計上の欠陥が導入された理由、つまり物理設計を介して制約を強制する試みが無効であった理由、および運用のコントロールもまた成功しなかった理由を特定することです。

この分析の目的を達成するために、まず、安全コントロールストラクチャーを調べることから開始し、事故防止における安全コントロールストラクチャーの限界を特定します。通常、システム開発とシステム運用の両方を含める必要があります。多くの場合、事故分析はシステム開発ではなく運用にのみ焦点を当てているため、運用上の限界だけが考慮されます。システム開発方法における欠陥については、識別または完全な理解が常になされるわけではありません。

安全コントロールストラクチャーのモデル化[15]



[15] 安全コントロールストラクチャーのより一般的な名称は安全管理システム（SMS）ですが、安全管理システムのいくつかの規格は安全コントロールストラクチャーに関して不完全です。安全コントロールストラクチャーには、必ずしもSMSに含まれているとは限らない機能やコンポーネントが含まれています。

2. この種のハザードに対する既存の安全コントロールストラクチャーをモデル化する。

CASTの根底にある因果関係のモデルは、安全を失敗の問題ではなくコントロールの問題として扱います。原因は常に、コントロールストラクチャーとハザード防止のために構築されたコントロールが、ハザードを防ぐことに対して、効果的ではなかったことにあります。目的は、なぜ、そして、どのように改善されるのかを判断することです。

CASTは、コントロールとコントローラと、事故におけるそれらの役割に焦点を当てるため、分析の開始において、コントロールストラクチャーをモデル化することが必要です。システムの安全コントロールストラクチャーと前のステップで識別されたハザードがまだ存在しないとすると、モデル化を達成するための唯一のまたは最善の方法というものはありません。しかし、役立つヒントや発見的方法はあります。最も有用な方法のうちの２つは、（1）非常に高レベルの抽象的なコントロールストラクチャーから始めて、後でそれを洗練すること、および（2）ハザードに対して一般的に存在するコントロールの識別から始めることです。これら２つの活動は別々に行われてもよく、あるいは、関係し合っていても構いません。

通常、同様の事故が以前に発生しており、それらを防ぐためのコントロールが作成されています。その場合の分析の主な目的は、上記のような効果がなぜ得られなかったのか、また、どのように改善するのかを決定することです。コントロールは、一般的な安全対策ということもあり、また、特有の状況のために設計された特別なコントロールということもあるでしょう。すべてのコントロールを最初から特定する必要はありません。分析が進むにつれて発生する質問は、より多くの制約とコントロールを特定するでしょう。唯一の間違いは、あまりにも狭く始めてしまい、それにより、重要なコントロールやコントローラ、あるいはシステムのハザードを見逃してしまうことです。完成した設計のリスクを評価するために、コンポーネントの故障の確率を単に特定することにとどまらないハザード分析が行われていたとすれば、コントロールを識別する際の重要な手がかりは、通常は、工場の元々のハザード分析から得ることができます。

もし、STPAがシステムの設計に使用されていれば、識別された事故につながるシナリオとシステム開発中に作成されたコントロールの明示的なリストがあるでしょう。システムのSTPA分析が既に存在する場合は、発生した問題に関する多くの情報が提供されます。理論的には、STPA分析には発生したシナリオが含まれているはずです。そうでない場合は、開発時の分析とシステムの運用との間が切り離されていたのでしょう。一つの可能性は、オリジナルのSTPAがすべての潜在的シナリオを完全には特定していないことです。もう一つは、発生したシナリオは特定されたものの、効果的なコントロールが実装されなかったということです。そしてもちろん、システム稼働後にシステムとその環境が時間とともに変化し、設計されたコントロールの有効性が否定され、もともと分析されていなかった新しい因果関係のシナリオが導入された可能性があります。

システムのコントロールストラクチャーがまだ存在しない場合、この種のイベントの一般的なコントロールを含む、非常に抽象的な上位レベルのコントロールストラクチャーから始めると便利です。図13は、シェル ムールダイクの予備的で非常に上位レベルの安全コントロールストラクチャーを示しています。化学物質の生産と公衆衛生という、コントロールされている２つの物理的なプロセスがあります。

シェル ムールダイク プラントは、化学プロセス自体の安全をコントロールする直接的な責任を負っており、州・地方の緊急管理は、公衆衛生を保護する責任を負っています。グローバルなシェル企業は、世界中の子会社とシェルのプラントを統括しています。分析の初期段階では、コントロールの種類と責任関係については、ほとんど分かっていません。これらは調査を通じて詳しく記述される必要があります。政府の監督に関しては、

地方およびオランダの監督機関と包括的なEU規制があります。関係するハザードに関して、コンポーネントごとに負っている（これまでに理解されている）責任を文書化することは、通常役に立ちます。繰り返しますが、調査中にさらに情報が蓄積されるとモデルは変わります。

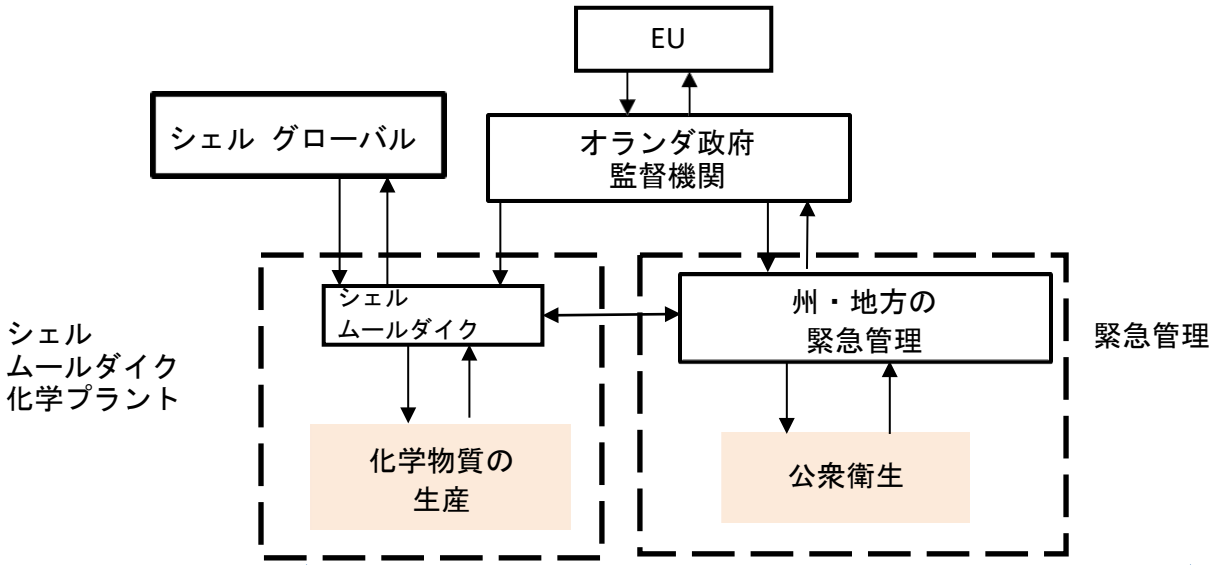


図 13：シェル ムールダイクの非常に上位レベルでの安全コントロールストラクチャーモデル

モデルを作成する過程において、一般的なものと特定システムの両方で、どのような種類のコントロールが存在するかを最初に特定することが、ハザードを防ぐために役立つ場合があります。コントロールのリストを作成したら（おそらく後で追加されるでしょうが）、コントロールの責任が、物理的設計、人的コントロール、自動化、または組織や社会構造のどこにあるのかを検討します。例えば、物理的制御（インターロックやリリーフバルブなど）、電子制御（航空機の地上近接警報システムなど）、プロセスパラメータを監視および調節する電子プロセス制御システム、人間のオペレータ、機器保守者、管理監督、規制管理などがあるでしょう。

コントロールが特定された後は、（何が何をコントロールするのかを示すための）階層のモデル化が、残された唯一の課題となります。これにより何らかの困難が生じ、最終的にいくらかの変更があったとしても驚かないでください。上位レベルの安全コントロールストラクチャーから始めると、コントロールを発見しながらストラクチャー内にコントロールを配置できるはずです。進めていくにつれて、より多くの詳細を追加することができます。

システムの調査と理解が進むにつれて、コントロールストラクチャーもおそらく変わるでしょう。最初に、表示されている最も高いレベルで変更を加えることが、役立つ場合があります。上位レベルのコントロールストラクチャーの変更は、低い抽象化レベルにおいて複数の変更を引き起こす可能性があります。最初に上位レベルで変更を加えることは、コントロールストラクチャーの大規模な修正が必要とされる場所を特定するのに役立ちます。例えば、分析プロセスの後半で保守が関係していることが分かったとしましょう。それまでに得られた非常に詳細なコントロールストラクチャーに保守を追加し、他のシステムコンポーネントとのやり取りをすべて含めるよりも、上位レベルのストラクチャーに戻り、機器のコントローラとして保守を追加し、他のコントローラとの関係を理解する方が簡単な場合があります。システム内の保守の全体的な役割と場所がモデル化されると、保守管理との関係を含むように、より詳細なコントロールストラクチャーを変更でき

ます。

通常、事故を防止するためのコントロールは、制約やコントロールを最も適切に実行できるグループまたはシステムコンポーネントに向けて、コントロールストラクチャーの随所に分散されます。より高レベルのコンポーネントは、それ以下のコンポーネントによるコントロールの運用を監督する責任を含む、より全般的な責任を持ちます。例えば、人間のオペレータは、コントロール対象のプロセスにおける物理的パラメータを調整する責任があります。運用管理は、事業者が自らの責任を確実に遂行するために必要な訓練を提供し、適切な経歴を持つ作業者を雇用する責任を負う場合があります。運用管理はまた、運用中のパフォーマンスを監視して、オペレータが適切に機能していることを確実にすることにもおそらく責任があります。より高レベルの管理者は、訓練が行われていること（通常、その訓練の詳細を明示する責任は負いません）、および運用管理が許容可能に実行されていることを確実にします。最高レベルの企業管理と外部の規制監督は、抽象化と詳細化のさらに高いレベルになります。合わせて、安全コントロールストラクチャー全体で、ハザードを排除またはコントロールし、システム動作に対する安全制約を強制する必要があります。

繰り返しになりますが、因果分析で最初にすべてを識別する必要はありません。分析を進めながら、質問を生成して答えることで、より多くのコントロールおよび制約さえも特定するでしょう。特定の種類の損失について複数のCAST分析が存在する場合、コントロールはおそらく以前の分析で特定されているはずです。そのため、このステップは簡単になり、関係する特定の損失に対する固有のコントロールを見つけるだけで済みます。コントロールが効果的だった理由については、次のステップの中で分析します。このステップでは、コントロールをリスト化するだけです。

ここでは、シェル ムールダイクのコントロールストラクチャーの詳細化プロセスについて、図13の非常に上位のコントロールストラクチャーから始めて、説明していきます。この時点では、完全で最終的なコントロールストラクチャーを生成する必要はありません。調査が進むにつれて、変更が行われ、ストラクチャーが追加される可能性があります。目的は、詳細なCAST分析を開始するためのコントローラとその責任を特定することだけです。

爆発や火災は化学プラントではよく知られているハザードであり、それらを防ぐためのコントロールが常に含まれています。コントロールには通常、保護システム、アラーム、センサ、圧力開放弁などが含まれます。物理的保護システム以外に、通常、オペレータ、プロセス制御システム、および安全管理があります。それらの上には、これらのシステムコンポーネントおよび一般的なプラント運用のためのさまざまなレベルの管理があります。安全の観点から開発と運用の両方を監督する安全グループが通常存在します。このグループは、さまざまな種類のハザード分析とリスクアセスメントの活動に責任があるかもしれません。事象が触媒の再加熱中の暴走反応を指しているため、図14では、触媒サプライヤを含めています（ただし、触媒の役割がまだ明らかでない場合は後で追加することが可能）。事故を説明する必要がない場合は、後で削除することもできますし、この時点で省略した場合は、後で追加することもできます。コントロールストラクチャーは、分析を導き、欠落した原因分析を容易に識別することができますが、最終報告書におけるその主な用途は、事故がなぜ起きたのか、そして何を変える必要があるのかについての首尾一貫した説明の提供を支援することです。

設計活動の責任はどこかにあります。シェル ムールダイクの場合、グローバルレベルのシェル プロジェクトアンドテクノロジーによる監視またはレビューの下、現地の設計グループがプラント設計を行います（図14には示されていませんが、現地の設計グループはプラント管理のコントロール下にあり、その一部と思われます）。

企業レベルまたはグローバルレベルでは、常に何らかの種類の安全管理があります。最後に、経営管理（少なくとも取締役会レベル）は、ほとんどの場合、企業管理レベルの

安全において、何らかの企業責任と監督を有しています。この時点で、コントロールストラクチャーは次のようになります。

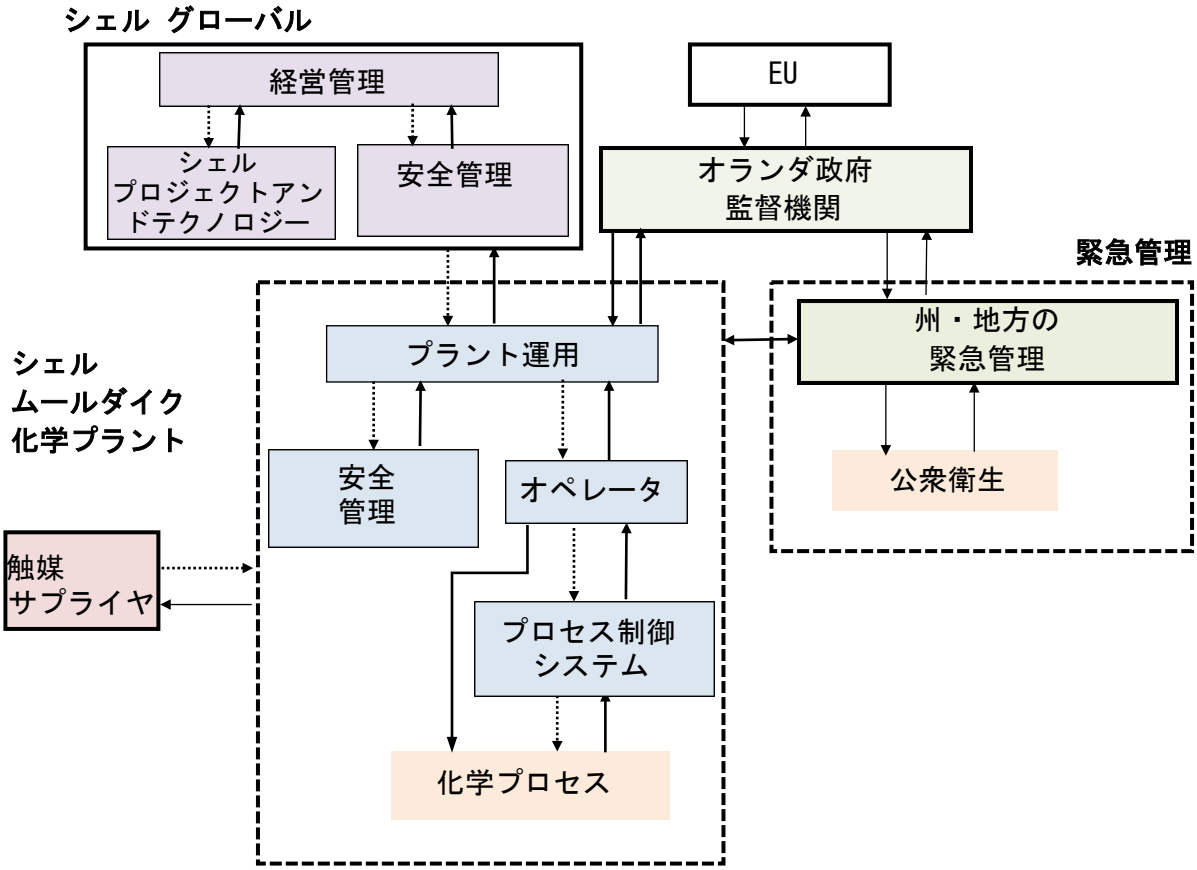


図 14：シェル ムールダイクの安全コントロールストラクチャーの詳細

コントロールストラクチャーのモデル化から始まるSTPAに精通している読者にとって、CASTで使用されるモデルは、STPAを実行するために必要とされるほど詳細である必要はありません。CASTを使用する場合、分析が進むにつれて詳細のほとんどが記入されます。しかし、基本的なコンポーネントは、分析を導くのを助けるために最初に識別されるべきです。

基本的なコンポーネントが特定されたら、各コンポーネントの責任の特定を開始することができます。例えば、これまでにシェル ムールダイクの安全コントロールストラクチャーに含まれていたコンポーネントに対する責任は次のとおりです（図14）。

プロセス制御システムの安全に関する責任：

- 通常の生産および非定常時の運用（運転停止、始動、保守、緊急事態など）の際に、オペレータがプラントを制御することを支援します。
- 関連する値の表示、アラートの提供、プラントの機器に対するコントロールアクションを発行します。
- プロセスが安全域内に留まり、アラーム状態にならないように、温度、圧力、レベル、および流量を制御します。

オペレータの責任：

一般：

- ハザードを引き起こさない方法でプラントを運用します。
  - プラントの状況とアラームを監視します。
  - 運用の安全な範囲に収まるようにプロセスを制御します。
  - 発生した非安全な状況に対応します。

今回の事故に特有の事項：

- 起動中に必要に応じて、ガスと液体の流量を調節します。
- （触媒ペレットの損傷を防ぐために）装置が急速に加熱されすぎないことを確認します。

プラント安全管理関連の責任

- プラントのハザードを識別し、ハザードの除去、軽減、管理を確実にします。
- セーフティクリティカルな活動についての作業指示書を提供するか、あるいは他の誰かから提供された作業指示書を、安全への影響の観点からレビューします。
- 適切に訓練され熟練した経験豊富な人が、リスクの高いプロセスに割り当てられるようにします。
- 変更管理（MOC）手順に従い、変更に対するリスク評価を行い、その結果に基づいてリスク管理を実施します。
- 被爆者または負傷者への緊急治療を提供し、必要な医療設備および要員が常に稼働できる状態であることを確実にします。[*負傷者は現場で適切に治療されたため、この観点についてこれ以上は言及しません。*]
- セーフティクリティカルな活動の監査を実施する、あるいはそのような監査を実施する際のプラント運用管理を支援します。[*事故報告書からは監査の責任者は明らかではないが、監査は行われたように思われます。*]

運用管理関連の安全に関する責任

- 運用の安全方針を確立します。
- 安全管理がその責任を果たし、現実的なリスクおよびハザード評価を提供していることを確実にします。

- プラント運用に関する意思決定には、安全管理から提供されたハザードおよびリスク分析の結果を使用します。
- 全体的なシェル グローバル安全管理システムと整合性のあるシェル ムールダイク安全管理システムを作成し、それが効果的かつ遵守されていることを確実にします。

より個別の運用管理、安全関連の責任として、以下があります。

- 通常時および非定常時の作業活動について、オペレータに適切なトレーニングを提供します。
- MOC（変更管理）の手順に従ってリスク評価を実施する、あるいは安全管理が変更のリスク評価を実施することを確実にします。プラントおよび運用手順において、プロセスを監視し、リスク管理を設計・実施できるように、リスク評価を使用します。
- 作業指示書を準備します（あるいは少なくともレビューします）。それらが安全であり、それに従って作業が行われることを確実にします。
- 定期補修工事のようなリスクの高い運用の際は、（リスクに）に近い要員数を最小限に抑えます。
- インシデントの記録と教訓を維持するとともに、確実に伝達し、そこから学ぶ必要のある人によって使われることを確実にします。
- 活動に必要な経験と訓練に見合った要員配置を行います。
- オペレータがクリティカルな活動を実施するのを支援できるプロセス制御システムを提供します。
- 監査を実施します。監査（および他のフィードバック情報源）で使用される先行指標を確立するか、安全エンジニアリングが適切な先行指標を特定していることを確実にします。

<u>シェル企業プロジェクトアンドテクノロジー（エンジニアリング）の安全に関する責任</u>

- 安全設計の作成：ハザード分析を実行（または他のグループによって作成されたハザード分析の結果を利用）し、設計内のハザードを排除または軽減します。
- 設計自体において、設計者が排除または十分に軽減することができなかったハザードにつながるシナリオを回避できるように、プラントを運用しているオペレータに対して、設計、ハザード、および運用情報を提供します。
- 設計による運用から学び、そのフィードバックに基づいて設計を改善します。

<u>シェル企業の安全管理関連の責任</u>

- 子会社にライセンス付与した設計に関するハザード分析の実施を含む、プラント設計の安全性。
- シェルの様々なプラントや施設における運用上の安全性を監督します。
- 安全に関する変更手順の管理：変更手順を作成し、確実に守られるようにし、インシデントからのフィードバックを用いて改善します。
- インシデントや教訓などについて、世界各地のプラント間でコミュニケーションが取れるようにします。
- シェル全体の安全情報システムを作成および更新し、その情報がシェル企業内およびグローバルレベルの両方で適切に伝達されることを確実にするとともに、それが完全かつ有用であることを確実にします。

経営層の企業管理の責任：

- 対策がとられていることを確実にします。
  - 主要な事故の発生を防ぎます。
  - 事故が発生した場合は、人や環境への影響を低減します。
- 作業に関係する全ての面において、従業員の健康と安全を確保します。（労働条件に関する法令やその他規制に基づいて）
- プラントがある国の政府規制に従います。
- 効果的な安全管理システムを構築し、強力な安全文化方針を確立します。 SMSと安全方針が遵守され、それらが有効であることを確実にします。

触媒製造業者の安全に関する責任

- 設計中および/または運用中の反応器における触媒の使用を評価するために、必要な情報を顧客に提供します。
- 使用上の安全性に影響を与える可能性のある変更が、触媒に加えられた場合は、顧客に警告します。

オランダの規制当局

ここでは、オランダのすべての安全と環境に関する監督当局をまとめて示します。この規制監督の根底には、２つの主要な方針があります。

1. Brzo：企業は事故を防ぐためにあらゆる対策を講じなければなりません。また事故が発生した場合は、人間および環境への影響を低減する必要があります。企業は、重大事故防止方針（PBZO）に方針の前提を定め、安全報告書（VR）を作成し、安全管理システムを組織することによって、この義務を履行する必要があります。
2. Wabo：規制当局は、環境観点の許可、つまり環境の安全性に関連する規制を企業が遵守しているかどうかを検査しなければなりません。

安全に関する一般的な責任：

- 環境と公衆を保護するため、オランダの法律に対する監督と執行に責任を負います。 プロセスの安全性を重視したBrzo検査および環境の安全性を重視したWabo検査を実施します。
- オランダ国内でのEUの安全衛生法の執行に責任を負います。

より具体的な責任：

- 監督する責任がある企業の欠点を識別します。
- 監督と執行を通して、セーフティクリティカルなプロセスを改善するよう企業に働きかけます。欠点を識別し、インシデントや事故の根本的な原因を調査して検出するように促すべく企業に継続的に質問します。特定された欠点が是正されることを確実にします。
- プラント、手順、およびプロセスに加えられた変更を評価します（ただし、企業のリスク分析を実行することは想定されていません）。
- 保守や化学反応器の起動など、セーフティクリティカルなプロセスに最大限の注意を払います。

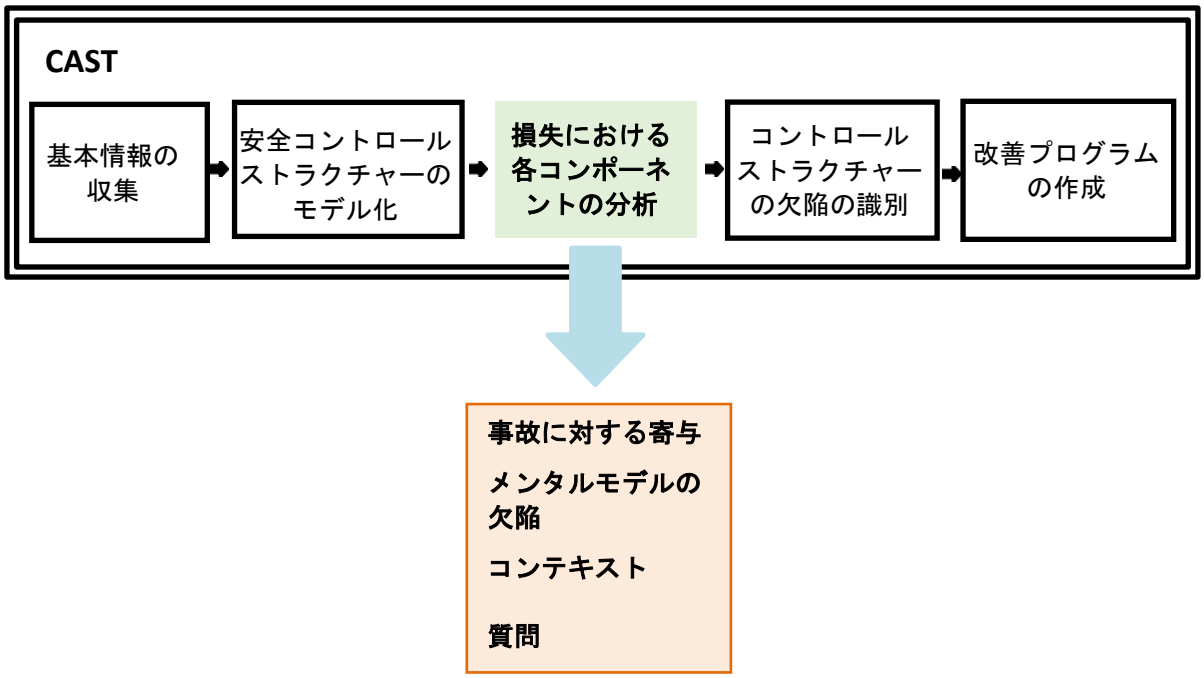
緊急サービスの責任

- 消化活動[本事故においては、共同消防隊が効果的に実施した]、危機管理、特に以下を含む危機コミュニケーション:
  - 市民へのインシデント関する周知
  - 放出された物質を調整した基準で測定
  - 電話相談窓口の運用
  - 放出された物質の測定結果とそれに基づく勧告の市民への周知

繰り返しになりますが、コントロールストラクチャーモデルは固定されておらず、事故およびコントロールストラクチャーの各要素の責任についての知識が増えるにつれて、進化して変化する可能性が最も高くなります。CAST分析は本質的に、責任が効果的に実行されたかどうか、そして実行されない場合、なぜこのタイプの事故を防ぐために実行されないのか、そして将来この種の事故を防止するためにどのように変更できるかを特定することを含みます。もう１つの考えられる結論としては、責任が適切に特定されていない、または適切に割り当てられていないこと、そして基本的な安全コントロールストラクチャーを再設計する必要があるということです。ほとんどの事故調査では、両方のタイプの損失の原因が見つかる可能性があります。

アナリストはどのように責任を特定するのでしょうか？これらのほとんどは、企業のマニュアルまたは政府の文書のいずれかに記載されています。さらに、調査中に自分の責任と他人の責任についてコントローラに質問すると、少なくともコントローラが自分でどう考えているかについて、引き出すことになります。ここでの混乱と矛盾は、なぜ事故が発生したのかに関する手がかりになる可能性があります。アメリカ海軍のSUBSAFEプログラムは、50年以上の歴史の中で見事に成功してきましたが、その重要な特徴の１つは、プログラムの全員が自分の責任と他人の役割を正確に知っているということです。責任に関するこの知識を継続的に強化し監査することで、事故が減少します。

各コンポーネントに対する分析：なぜコントロールが有効でなかったのか？



3.コントロールストラクチャーのコンポーネントが損失防止に有効でなかった理由を分析します：

最下層のコントロールストラクチャーから、各コントローラが事故の際に果たした役割とその振る舞いに関する説明（各制御コンポーネントが、なぜそうしたのか、なぜそうすることが、そのときには正しいと判断したのか）を明らかにします。

基本的なコントロールストラクチャーとコントロールを識別できたら、次のステップとして、コントロールストラクチャー、すなわち現在のコントロールがなぜ事故を防ぐことができなかったのかを明らかにします。このプロセスには２つの部分があります。このセクションで説明されている最初のものは、個々のコントローラ（自動化されている場合もあれば、人間である場合もあります）、および事故においてそれらが果たした役割に着目したものです。次のセクションで説明する２つ目は、コントロールストラクチャー全体の動作とコンポーネント間の相互作用に着目したものです。忘れてはいけないのは、コントロールストラクチャーの欠陥を識別することが目的であるということです。つまり個人や個々のコンポーネントに責任を負わせるのではなく、なぜそれらがそのような振る舞いをしたのが当然であったのかを理解することです。

また前ステップで開始したように、CASTプロセスでは、最終的になぜ事故が発生したのかについての完全な説明を提供できるよう、回答が必要な質問を分析中に生成していきます。コントロールストラクチャーの最下層のコンポーネントから始めて、上位層に向かって分析をすることが最も有用です。

各コントローラに対するCAST分析にはいくつかの種類があります。

- 事故に関するコンポーネントの責任
- ハザード状態への寄与（行動、行動の欠如、意思決定）：[16]

なぜか？

- 行動へ寄与しているメンタルモデル/プロセスモデルにおける欠陥
- 行動、意思決定、プロセスモデルの欠陥を説明できるコンテキスト要因：

上記の最初の２つの分析は、コンポーネントが損失で果たした役割があれば、それを分かりやすく文書化するものです。安全コントロールストラクチャーをモデル化する際に、コンポーネントの安全に関する責任が特定されていますが、損失に関するものだけを考慮する必要があります。役割あるいは寄与（ハザード状態に関する振る舞い）が、果たされなかった責任ということになります。例えば、シェル ムールダイクにおける化学反応器の保守終了後の再加熱時のオペレータの責任の１つは、加熱が運用の安全な範囲内に留まるようにプロセスをコントロールすることです。このプラントにおける事故では、彼らは、触媒ペレットの過熱を防ぐことができるようにガスと液体の流量を調整しませんでした。忘れてはいけないのは、彼らが流量を調整するのに「失敗」した、あるいは流量を調整「すべきであった」というように、批判的あるいは後知恵的な言葉を使うべきではないということです。非難を伴わない形で何が起こったのかを分かりやすく記述してください。ただ、その人またはグループが何をしたのか、あるいはしなかったのかを示すように、損失に寄与した振る舞いをありのままに記述します。

「なぜ」の分析には、コンポーネントがそのように動作した理由、つまり、その時点でそれらのコンポーネントにとって正しいように見えたコンテキスト要因やその他の要因の説明を含めます。例えば、コンテキスト要因には、コントローラがその時点で保持していた誤った情報、不適切なトレーニング、行動へ影響を及ぼすプレッシャーやインセンティブ、その役割やコントロールされたコンポーネントがどのように動作するかについての誤解などが含まれます。「なぜ」の分析には、コンポーネントの振る舞いに関して以前に出た質問への回答も含まれます。コンポーネントに対する「なぜ」の質問に答えると、通

[16] STPAでは、「非安全なコントロールアクション」という用語を、あまり苦情を受けることなく使っていますが、そこでの使用は仮説に基づいたアクションに関するものであり、実際に起こったことではありません。CASTでその用語を使用すると、多少の責任追及と批判の色あいがでるため、使用を控えてください。一般的に非難の意を含む用語を避けるために、「ハザードに寄与するコントロールアクション」、「一因となるコントロールアクション」、あるいは単に「ハザード状態へのコントローラの役割または寄与」などのさまざまな用語を使用しています。

常、より多くの質問が出てきますが、この質問に対しては、より上位のコントロールストラクチャーの分析において答える必要があるかもしれません。最終的にはCAST分析で生じたすべての質問に答えることが目的となります。実際は、断定的に答えることができない質問が残ってしまうかもしれませんが、当然、これらは最終結論において文書化される必要があります。事故調査と原因分析の目的が「犯人」を見つけることではないことを関係者が理解している場合、ありのままの答えが得られる可能性が高くなります。将来の安全性を向上させるための説明プロセスの一環として関係者に協力を求めてください。当然ながら、このような信頼は長い時間をかけて築き上げる必要があります。

コントローラが「なぜ」そのように振る舞ったのかを理解することに着目してください。ほとんどのコントローラは正しいことをしようとしています。当然それらが悪意（自殺意図や殺人意図）を持っていたのであれば、それを識別する必要がありますが、そのような振る舞いは、事故ではめったにありません。通常、コントローラは良い働きをしようとしており、そうしなかったということにはいくつかの理由があります。自動コントローラの場合、理由を理解するためには、自動化のための設計、設計者、および必要な振る舞いに関して設計者が設定した想定に着目する必要があります。ソフトウェアに関連したほぼ全ての事故においては、ハザードを防ぐために必要な振る舞いに関する想定、すなわち安全な運用のために必要な要求が誤って理解されています。

発生した振る舞いの理由を理解することは、効果的な推奨事項を作成する際に最も役に立つガイドとなります。もし事故報告書が、コントローラが何を間違ったかだけしか識別しないのであれば、将来同じ振る舞いを防ぐために必要なこととして、「それをしない」ということ以上のことを事故報告書から学ぶことはできません。通常、コントローラには正当な理由があってそのように振る舞っているため、この種の指示は役に立ちません。ルールや手順というものは、あらゆる状況下で常に機械的に従わせるものではありません。もしシステムの設計者が、オペレータが文書による指示をそのまま考えずに従うことを意図している場合は、そのコントールに関する責任を自動化すべきです。チェックリストがガイドとして提供されることが多くありますが、通常、緊急時にはチェックリストの妥当性について人の判断が必要となります。もしチェックリストに従うべき時に、チェックリストに従わなかったのであれば、その理由を理解する必要があります。

今日のシステムの中には、何を行う必要があるか経験的知識に基づいて複雑な決定を行うために人間が含まれています。彼らが間違った決定をした場合、その理由（例えば、誤った情報を保持していた、プロセス制御システムの出力を誤解した、安全な決定をするための十分な支援がない、コントロールしていたコンポーネントの状態を把握するためのフィードバックがない、または誤解を招くフィードバック）は、コントローラが将来より良い判断を下すことを支援できる安全コントロールストラクチャーとコントロールを再設計するために必要な情報として役に立ちます。

CASTプロセスは、後知恵バイアスを可能な限り回避できるように設計されています。事故やインシデントの後では、振る舞いが明らかに誤っているように見えます。それは明白であり、言及する必要はありません。役に立つことは、「当時」コントローラにとって明らかな誤りではなかったのはなぜか、その理由を理解することです。なぜ明らかではなかったのか？よりよい判断を行うためにどのような情報が必要であったか？その情報を保持していたか？当時その情報が何を意味するのかを理解できていたか？情報を理解し処理することを難しくしてしまう他の競合しているプレッシャーはあったか？コンテキストをより完全に識別できればできるほど、結果として得られる推奨事項は、将来の損失を減らすうえでより効果的になります。コンテキストとは、例えば作業負荷、生産性へのプレッシャー、インセンティブ/ディスインセンティブなど身体的、心理的、情報的、管理的、状況的なものかもしれません。

この分析ステップの結果を記録するための表記法をどうするかは、情報が記録でき、理解がしやすければ重要なことではありません。この章の最後で、表記法についてこれま

でうまくいったいくつかの提案を示します。

本ハンドブックでは、シェル ムールダイクに対するCAST分析から少しだけ例を示します。全てのコンポーネントが果たす役割の要約は付録Ｂに記載されています。シェル ムールダイクの完全なCAST分析へのリンク、およびその他の多くの実際の事故へのリンクは付録Ａに記載されています。

自動プロセス制御システムは、プラントにおいては標準的なコントローラです。したがって、シェル ムールダイクでの爆発を理解するための出発点として、都合がよいです。安全に関連する責任は次のとおりです：

プロセス制御システムの安全に関する責任：

1. 通常の生産および非定常時の運用（運転停止、始動、保守、緊急事態など）の際に、オペレータがプラントを制御することを支援します。
2. 関連する値の表示、アラートの提供、プラントの機器に対するコントロールアクションを発行します。
3. プロセスが安全域内に留まり、アラーム状態にならないように、温度、圧力、レベル、および流量を制御します。

損失におけるその役割を識別するために、これらの責任が満たされたかどうかを判断することから始めることができます。この事例では、プロセス制御システムは次のようにして事故に寄与しています：

ハザード状態への寄与：

1. プロセス制御システムは、加熱速度や他の重要な変数を自動的にコントロールすることを含めて、起動プロセスを安全にコントロールするためにオペレータが必要とする支援を提供しませんでした。
2. プロセス制御システムは、圧力と温度が急激に上昇した際に、プロセスの停止処理に入りませんでした。
3. プロセス制御システムが、２回の高レベルのアラームの後に自動リセットを発行しなかったので、ガス排出システムが閉じたままとなりました。

2（プロセス制御システムは、圧力と温度が急激に上昇した際に、プロセスを停止しなかった）に対する詳細な「なぜ」の分析、つまりコンテキスト要因の例は、以下のとおりです。

なぜか？ （非安全なコントロールに影響したコンテキスト要因）	挙げられた質問
ユニット4800に対する非常停止ボタンがありませんでした。非常停止がないので、ボタンを１回押すだけで迅速にユニットの運用を安全に停止する方法はありませんでした。事故報告書にこの設計の「欠陥」の理由は記載されていませんでしたが、調査時に答えることができた可能性があります。セーフティクリティカルなシステムでは非常停止ボタンは標準的なものです。	*これは現状に満足しているのか、コストによるものか、あるいは、技術的な理由によるものなのでしょうか？*
機器ベースの安全装置は、特定の条件に対応してそれを防止するように設計されていますが、今回の発生した条件には対応していませんでした。この事故の後、水素との望ましくない化学反応に起因してユニット4800が過度に高温にならないように、安全装置を追加しました。	*安全装置でこれらの条件が省略されていたのはなぜですか？それらを特定することができるハザード分析は行われていましたか？*

「一つ以上の物質を封じ込めることを意図し、任意のコンポーネントが互いに永続的に接続されている一つまたは複数の機器」と説明されている、封じ込めシステムはあります。しかしながら、封じ込めシステムの弁は遠隔操作することはできず、手動で操作する必要があります。その夜の火災の激しさとさらなる爆発のリスクのために、これらの弁をすぐに動作させることは不可能で、実際には数時間後に火が消えるまで動作させることができませんでした。	*封じ込めシステムの設計は、この状況では役に立ちませんでした。これは事前に分かっていましたか？遠隔操作できるものを設計することは不可能でしたか？*

なぜコントローラがそのように振る舞ったのかを理解する上で重要な部分は、誤ったプロセスモデル/メンタルモデルから生じることがあります。CAST分析では、このモデルの欠陥を識別し、それらがなぜ発生したのかを判断します。

プロセス制御システムのプロセスモデルの欠陥：シェル ムールダイクのプロセス制御システムは、ほとんどの部分において、プロセスの状態に関する正しい情報を持っていました。しかしながら、化学反応器内に設けられた温度センサの数が適切ではなく、温度情報がいくつか欠落していました。

コンポーネント分析が完了して文書化されている場合（詳細はここには含みません）、推奨事項とともに事故におけるコンポーネントの役割について要約を作成することができます。原因分析において重要な未解決の質問は、すべて文書化されている必要があります。

プロセス制御システムが事故で果たした役割の要約：プロセス制御システムは、起動時にオペレータに必要な支援を提供したり、緊急時にプロセスを簡単に停止できるようには、設計されていませんでした。設計がこのようになった主な理由は、発生したシナリオは起こらないと設計者が誤った想定をしていたためです。過去に類似のプラントにおいて、この想定が破られたインシデントの後でさえ、その想定が疑問視される、あるいは再検討されるということはありませんでした（安全情報システムのCAST分析を参照）。
より一般的に言えば、プロセス制御システムは通常生産のフェーズのためだけに構成されていました。触媒が交換された後の、問題が生じた加熱フェーズのための特別な自動制御回路は存在しませんでした。実際、このフェーズは最も事故が発生しやすいと一般的に知られていますので、このフェーズ中にオペレータに対して自動的な支援を提供しないという判断はとても不思議ですが、事故報告書には説明はありません。

未回答の質問：運用再開フェーズにおいて、オペレータに支援を提供しないと判断したのはなぜですか？非常停止機能がシステムに組み込まれていないのはなぜですか？

推奨事項：オペレータの知識とスキルは、非定常時のフェーズにおいて最も試されるものであり、ほとんどの事故は、そのようなフェーズにおいて変更が行われた後に発生しています。プロセス制御システムは、セーフティクリティカルな非定常時の運用（今回の再起動シナリオだけでなく）において、オペレータを支援するように再設計する必要があります。
手動運用の場合は、プロセス制御システムは、意思決定や行動に必要なすべての支援をオペレータに対して提供するとともに、注意力を削ぐプレッシャーや時間に関するプレッシャーを減らすことを目指す必要があります（オペレータに関するセクションを参照）。

このセクションの残りの部分では、シェル ムールダイクの別のタイプのコントローラに

対するCAST分析の例を示します。プロセス制御システムに対する分析は自動化されたコントローラの例でしたが、別のタイプのコントローラは、人間や人間のグループとなります。紙面の都合上、ここでも詳細は省略します。

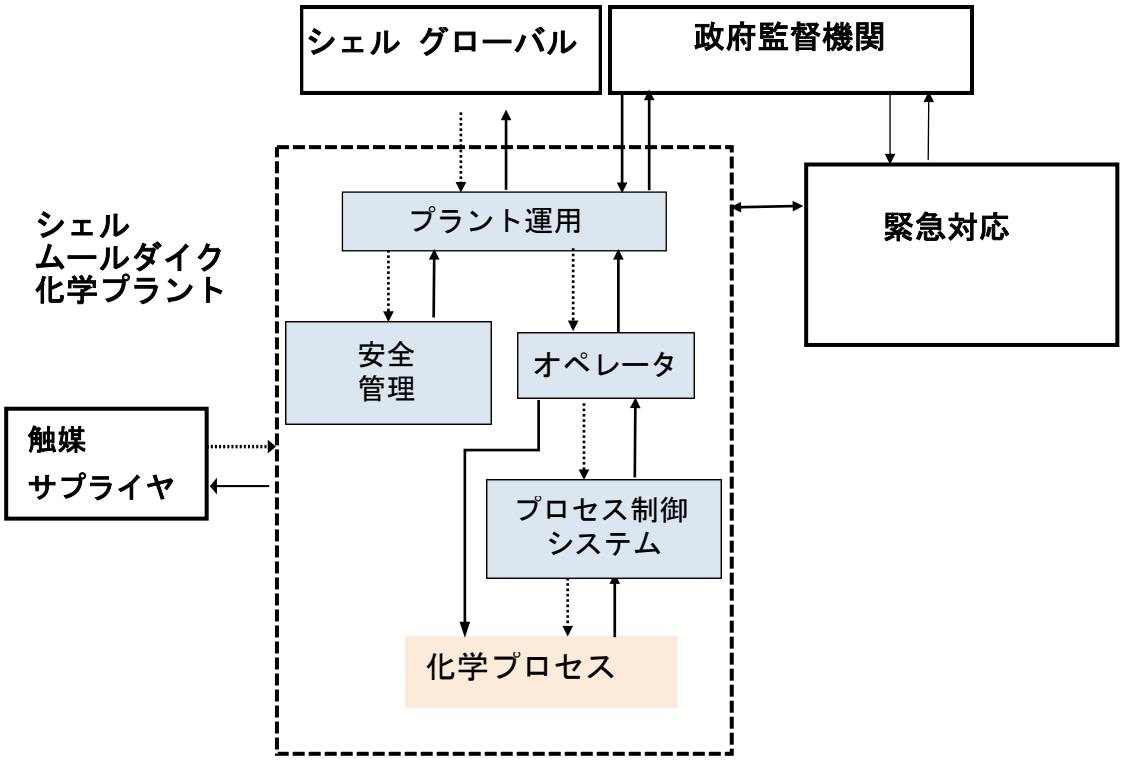


図 15：シェル ムールダイク化学プラントの安全コントロールストラクチャー

オペレータ

オペレータの行動は明らかに爆発の一因となっています。例えば、温度が急上昇しているときにエチルベンゼン対して手動で加熱を行っています。またホットスポットや負圧差に気づかずに対応しておらず、アラームに適切に対応していません。さらに、ガス増加時にガス排出システムを閉じたままにしており、事前に設定された限界を超えた時にも、プロセスを安定させ、速度を落とし、停止するということ行っていないなどもありました（これはシェルでのオペレータトレーニングにおける基本原則です）。

後知恵として、オペレータが誤った行動をとったこれら全てのことを考えると、オペレータは損失に対して大きな責任があります。実際にこのような行動を列挙すると、多くの（ほとんどの）事故原因分析や事故報告は行われないこととなり、オペレータが損失の主たる原因であるとみなされることになります。その日に定期補修工事の運用を行っていたオペレータの過失や無責任な行動であった可能性はありますが、彼らがベストを尽くそうとしていた可能性は高いです。なぜ彼らが誤った判断をしたのか、すなわち、なぜその判断が彼らには正しいと思われたのかを理解しなければ、将来の同様の誤った判断を防ぐことはほとんどできません。答えの多くは、より上位層のコントロールストラクチャーにありますが、オペレータの行動の中には、プロセスモデルと意思決定のコンテキストに着目することで理解できるものがあります。

オペレータに割り当てられている一般的な安全責任：

- ハザードを引き起こさない方法で計画を実行します。
  - プラントの状況とアラームの監視
  - 運用の安全な範囲に収まるようにプロセスを制御
  - 発生した非安全な状況への対応

今回のインシデントに特有の事項：

- 起動中に必要に応じて、ガスと液体の流量を調整します。
- （触媒ペレットの損傷を防ぐために）装置が急速に加熱されすぎないことを確認します。

これらの責任はどれも果たされませんでした。ハザード状態の原因となったオペレータの振る舞いの例は次のとおりです：

- クリティカルなプロセスの範囲を超えた際に、オペレータは爆発前にプロセスを安定化させたり停止したりしませんでした。
- まだ不安定かつ45分間だけしか加湿していないうちに、加熱が開始されました（21:00頃）。当時はおそらく適切な湿潤状態となっていませんでした。
- 温度が急上昇している際に、オペレータは手動でエチルベンゼンに追加で加熱しました。
- オペレータはホットスポットに気づかず対応しませんでした。また関連する負圧差に気付かず、それにも対応しませんでした。
- オペレータは窒素流量を適切に調整しませんでした。（必要以上に）窒素流量が少なかったことが事故の原因の１つでした。
- オペレータはアラームに対応しませんでした。

この振る舞いだけに着目すると、オペレータの振る舞いは実にひどいように思えます。ほとんどの事故報告書はここで終わってしまいます。しかしコンテキスト要因とプロセスモデルの欠陥を考慮すると、状況は大きく異なって見えます。紙面上の都合から、この中のいくつかの例だけを以下に示します。より詳細な分析については、CAST報告の完全な分析を参照してください。

なぜか？ （非安全なコントロールに影響したコンテキスト要因）	挙げられた質問
オペレータは、正しい判断を下すために必要な情報を提供されていませんでした。プロセス制御システムは、オペレータへの支援（フィードバック）をほとんど提供していません。事故報告書全体を通して、オペレータの行動の多くは、プロセスのダイナミクス（dynamics）に対する深い理解と強い注意を要すると指摘されています。	*なぜでしょうか？オペレータに手動かつプロセス制御システムの支援なしで起動をコントロールさせると判断した際に、確実にそれを行えることを保証するため、ヒューマンファクタ分析は行われましたか？*
中央ポンプに設計上の弱点があることが一つの理由で、ガスと液体の流量を調整するのは難しいことが分かっています。加えて、充填と循環をどのように行う必要があるかについて、職務分析は明確な指示を与えていませんでした。唯一の明確な指示は、中央ポンプを「乾燥」で運転すると壊すことになるため禁止するということだけでした。	

化学反応器における加熱中および湿潤中の安全性は、当時のオペレータと生産チームリーダーの知識とスキルに依存していました。シェル ムールダイクの書面による方針で決まっていたのは、化学反応器の起動と停止は、経験豊富なオペレータが、当該目的のための作業指示書を使用して行うことを要求していました。この保守のための停止を実施したのは経験豊富なスタッフで、彼らは通常の生産中にこの装置で作業するための訓練は受けていましたが、触媒交換は3、4年に1度しか行われないものであり、化学反応器の再起動は初めての経験でした。同時に、彼らは、起動時におけるプロセス制御システムからの支援を受けていませんでした。	
事故報告書によると、オペレータは起動手順書に正しく従っていました。したがって問題は手順書自体にあるはずで、事実、オペレータが使用した作業指示書は誤っており、不完全でした。作業指示書は、シェルがそのような指示書のために定めていたフォーマットに従っていないとともに、クリティカルな条件などの必要な情報やオペレータが踏むべきステップが省略されていました。例えば、窒素流量は事故後にはクリティカルであることが分かりましたが、クリティカルなものとして考慮されておらず、作業指示書には含まれていませんでした。	*誤った不完全な作業指示書がオペレータに提供されたのはなぜですか？*
起動手順書はオペレータによって作成されていました。技術者や安全担当者による専門家レビューは行われていないと考えられます。事故報告書には、なぜオペレータが、技術者や安全担当者による専門家レビューもなく、セーフティクリティカルな作業のために独自の作業指示書を書いているのかについての説明がありません。	*事故報告書では次の明白な質問に対し答えを示していません。作業指示書は、起動経験のあるオペレータによって作成されていましたか（経験のない人ではなかったですか）？他のオペレータであれば、作業指示書を作成するための経験と知識を持っていましたか？誰がこれらの作業指示書をレビューしていますか？今回の作業指示書は誰かがレビューしましたか？（この質問に対する答えはいいえ（No）となると思われます）。*
シェル グローバル プロジェクトアンドテクノロジーによって作成された設計書があり、この設計書には化学反応器の設計と運用に関する詳細な情報が含まれています。事故報告書によれば、この設計書はあまりにも詳細で「複雑に表現」されており、作業指示書の作成を担当するオペレータには理解できなかったため、設計書は起動のための作業指示書作成には使用されませんでした。	*ここには明白な質問が多くあります。*

なぜか？（プロセスモデルの欠陥）	挙げられた質問
事故報告書には、多くの後知恵バイアスをもってオペレータが「すべきであった」ことが示されていましたが、事故が発生した条件は、全て前回の保守停止時を踏まえ	*この場合、なぜ予想（プロセスの振る舞いにおけるメンタルモ*

た予想（プロセスモデル）と一致していました。オペレータは、再起動中の圧力変動は正常であると考えました（プロセスモデルの欠陥）。圧力は再起動が開始してから継続的に変動していました。このような変動は前回の再起動中にも発生しており、それは予想どおりでした。当然ながら後知恵で考えると、これらの予想は誤っていることが判明しました。この状況を踏まえると、プロセスが実際には通常の状態ではないという事実を知ることはなく、鳴ったアラーム数や頻度は異常ではありませんでした。	*デル）は正しくなかったのでしょうか。*
事故報告書では、特別な状況に介入するための判断を行うには、そのような特別な状況についての知識、経験、綿密な準備が必要であると示されています。オペレータは、リスクを判断するために、装置が限界を超える原因を完全に把握する必要がありますが、必要な知識や専門知識を持っていませんでした。 実際、企業の安全技術者でさえ、ここで発生した条件がハザード状態になる可能性があることを知りませんでした。設計者がそのようなシナリオが起こりえると考えなかったならば、なぜオペレータが起こりえると考えるでしょうか？事実、シェルの誰も、高速・高圧で起動が進むシナリオが起こりえるとは考えていませんでした。	*設計者や企業の安全技術者が、そのようなシナリオは起こりえないと考えたのはなぜですか？*

まとめると、調査の焦点を、誤ったことが判明したオペレータの行動そのものではなく、オペレータがそのように行動した理由に焦点を当てると、オペレータの行動にはそれほど明確な過失はありません。実際、オペレータは、彼らが従った誤った作業指示、トレーニングの欠如、作業を遂行するのに必要なスキルおよび知識といったコンテキストを考慮すると、適切に、少なくとも理解できるように行動していました。加えて、彼らはプロセス制御システムからは、ほとんど支援を提供されていませんでした。彼らがしなければならなかった仕事の多くが、細心の注意、正確さ、精神的な努力、プロセスダイナミクスの深い理解、そして絶えず変動するプロセスへの頻繁な調整を必要とするものでしたので、そのような支援は非常に貴重なものだったでしょう。

プラントの設計者がリスク（CAST分析の適切なセクションを参照）を認識または理解していなかったため、リスクがオペレータに十分に伝達されていない可能性があります。経営者は、オペレータが何かおかしなことを見つけた場合には、プロセスを停止させることに頼っているようでしたが、オペレータがこれを確実に行えるようにするための情報やトレーニングを提供しませんでした。そのような方針は、事故の後にオペレータを非難するための便利な言い訳でしかなく、オペレータが責任を果たすための助けにはなりません。

推奨事項の作成については後で説明しますが、この分析から明らかなことは、オペレータは割り当てられたことを実行するために適切なスキルと専門知識を持っている必要があるということです。その他の推奨事項としては、オペレータが確実に情報を提供されるように、ストレスの多い環境下でも、適切な判断を下すことができる作業状況を担保できるように、職務分析において人的要因を検討すること、運用の全フェーズに対してより自動化された支援を提供すること、起動時など危険であることが分かっている作業におけるトレーニングを提供すること、より良い生産プロセスになるよう作業指示書を改善することが有り得ます。

この分析では、いつものように、何が起こったのかを理解し、将来同様のことが起こらないようにするための推奨事項を作成するために、答える必要がある多くの質問を出せ

るようにします。読者の方にCASTプロセスと得られる結果について、より完全な全体像を理解していただけるよう、（詳細は省略しながら）ハンドブックのこのセクションの残りの部分でまとめます。

ここまでは、物理的プロセス、自動化されたプロセス制御システム、そしてプラントのオペレータに着目してきました。ここでは、安全コントロールストラクチャーを改善しながら、CAST分析により識別した他の各コントローラが損失で果たした役割について簡単に触れます。繰り返しになりますが、各コントローラの詳細なCAST分析はこのハンドブックには含まれておりません。

プラント安全管理

プラントの安全部門は通常、安全性を念頭に置いて運用上の意思決定が行われるよう、運用上の安全性を監督し、プラントの運用管理に情報を提供します。詳細な分析の例をここに示しますが、報告書は詳細すぎると理解が困難になります。詳細を含めるだけでなく、詳細分析の重要なポイントを要約した、事故におけるコンポーネント内の役割の要約も含めることが、有効な妥協案となります。

プラント安全管理関連の責任

- プラントのハザードを識別、および除去、軽減、管理を確実にします。
- セーフティクリティカルな活動についての作業指示書を提供するか、あるいは他の誰かから提供された作業指示書を、安全への影響の観点からレビューします。
- 適切に訓練され熟練した経験豊富な人が、リスクの高いプロセスに割り当てられるようにします。
- 変更管理（MOC）手順に従い、変更に対するリスク評価を行い、その結果に基づいてリスク管理を実施します。
- 被爆者または負傷者への緊急治療を提供し、必要な医療設備および要員が常に稼働できる状態であることを確保します。[*負傷者は現場で適切に治療されたため、この観点についてこれ以上は言及しません。*]
- セーフティクリティカルな活動の監査を実施する、あるいはそのような監査を実施する際のプラント運用管理を支援します。[*事故報告書からは監査の責任者は明らかではないが、監査は行われたように思われます。*]

プラント安全管理におけるプロセスモデルの欠陥

- このプロセスではエチルベンゼンを安全管理が必要な物質として扱っていました。
- 起動プロセスのリスクが高いことを考慮していませんでした。
- オペレータと生産チームリーダーが、知識と経験に基づいて手動で起動を管理し制御できると、考えていました。
- 他の類似のプラントにおいてインシデントが生じれば、彼らの想定に疑いが生じるリスクがあることを、彼らは確実に理解していました。あるいは、過去のインシデントに気づいていなかったのかもしれません。

コンテキスト要因/プロセスモデル要因の例（以降の要約にもさらに含まれています）：

- 時間の経過とともに、ユニット4800に関する最適な手順に対する理解が変化しました。いくつかの手順は安全上クリティカルであるとは考えられなくなりました。 そのため、それらの手順は改定された作業指示書には含まれていませんでした（または、以後含まれなくなりました）。
- 安全評価手順は政府の要求事項を遵守していました。
- ハザード評価は、より高いリスクと考えられているプロセスに焦点を当てており、主に安全性ではなく環境に対する物質の影響を評価していました。

シェル ムールダイクにおける安全管理が事故において果たした役割の要約：

- 使用された安全分析手法は、適切ではなかったか、適用されなかったか、または誤って適用されました。しかしながら、使用された手法は、シェルの要求に準拠しており、オランダの法規制要求を満たしていました。またそれらは石油化学産業では標準的なものでした。安全管理は、特定の関連情報を考慮せず、触媒と反応するエチルベンゼンが爆発を引き起こす可能性があるかどうかを調査しませんでした。一般的にも同様ですが、シェル ムールダイクでの安全管理は、様々な活動が行われているにも関わらず、ほとんど効果がなく、多くの活動は政府の規制に最低限準拠することに目が向けられていました。彼らの振る舞いを部分的に説明すると、誰もがエチルベンゼンと触媒の間の反応は不可能であり、起動プロセスは低リスクと考えていたということです。
- シェルの安全管理システムには変更に対処するための要求が含まれていますが、変更管理（MOC）手順は従われておらず、効果的に実施されていませんでした。プラント、触媒、プロセス、手順に加えられた変更に起因するリスクは特定されておらず、管理されていませんでした。MOCの手順に従わないことは、あらゆる産業で非常に多くの事故に関係しています。
- シェル ムールダイクでは新しい触媒を使うことが選択されましたが、新しい触媒は以前の触媒の性質と同じであると想定されていました。新しい触媒の変更された組成は製造業者によって提供された安全情報シートに記載されていましたが、安全エンジニアリングではこの変化に気付くことができませんでした。
- 手順の変更（加熱速度と窒素流量）は、リスク評価を行わずに実施されていました。これらの手順は、改定されたオペレータ作業指示書には含まれていませんでした。プラントや生産に関する他の変更は、全ての場合において、リスク分析に基づいた安全への影響についての体系的な検討が行われていませんでした。いくつかの故障シナリオのみが検討され、これがシェル グローバルの基準とオランダの法律の両方を満たしていました。事故に巻き込まれた装置の循環と加熱に焦点を当てた安全性検討は、全く行われていませんでした。安全性は1977年に行われた研究に基づいており、その研究では、（当時存在していた）触媒がエチルベンゼンの存在下で不活性であることを示していました。触媒の組成が時間とともに変化し、他のシェルの設備で同様のインシデントが起こりましたが、触媒がエチルベンゼンの存在下で不活性であるという想定は、再評価されませんでした。再評価するための要求は、シェル グローバルの基準またはオランダの法律にはありませんでした。
- プロセスの安全性の先行指標として、明らかにこの事故とは無関係な漏出数が使用されていました。近年、漏出数が大幅に減少したため、意思決定者は安全性が向上していると判断していました。この先行指標を使うことは、石油化学産業では一般的であり、オランダの規制当局によって承認されていました。
- 1999年に最初に起動して以後、シェル南海（Nanhai）とシェル ムールダイクとで同様のインシデントが発生していました。南海では特別な要因により爆発は発生しませんでした。これらの事象は、リスク、手順、あるいは暴走が不可能であるという想定の再評価には繋がりませんでした。南海でのインシデントを踏まえた推奨事項は、リスクを低減するために使用されていませんでした。*なぜでしょうか？事故報告書には、南海インシデントの推奨事項が、なぜ実施されなかったのかについての情報はありません。*
- 安全エンジニアリングでは、作業指示書の生成について適切な監督を行っていなかったため、非安全な作業指示書がオペレータに提供されていました。作業指示書は、シェルが提供した作業指示書のフォーマットに従っていませんでした。また作業指示書は、クリティカルな条件や必要な手順など、オペレータが必要とする情報の多くを省略していました。

推奨事項：

2014年6月3日に発生した爆発に固有の問題は、修正される必要はありますが、シェル ムールダイク安全管理の実運用には、オランダの公式な安全機関の事故報告書およびCAST分析の中で識別された多くの弱点がありました。これらを改善する必要があります。

- シェル ムールダイクの安全管理はより効果的に行われる必要があります。安全エンジニアリングは、単に申請をとおし、標準に最低限準拠するというもの以上である必要があります。
- 知識のある人がハザード分析の情報を使用して、全ての作業指示書を安全性の観点からレビューすべきです。 [本件ではハザード分析にも欠陥がありましたが、それは修正すべき別の問題となります。]
- MOCの手順は強制され、遵守されなければいけません。変化が発生した場合、過去の想定は再評価される必要があります。
- ハザード分析とリスク評価の方法を改善する必要があります。
- リスクに対し、より包括的で関連性のある先行指標を確立する必要があります。
- 教訓を取り込み利用するための手順を、確立または改善する必要があります。

運用管理

関連する安全に関する責任

- 運用の安全方針を確立します。
- 安全管理がその責任を果たし、現実的なリスクおよびハザード評価を提供していることを確実にします。
- プラント運用に関する意思決定には、安全管理から提供されたハザードおよびリスク分析の結果を使用します。
- 全体的なシェル グローバル安全管理システムと整合性のあるシェル ムールダイク安全管理システムを作成し、それが効果的かつ遵守されていることを確実にします。

より具体的な安全関連の責任には以下のものがあります：

- 通常時および非定常時の作業活動について、オペレータに適切なトレーニングを提供します。
- MOC（変更管理）の手順に従ってリスク評価を実施する、あるいは安全管理が変更のリスク評価を実施することを確実にします。プラントおよび運用手順において、プロセスを監視し、リスク管理を設計・実施できるように、リスク評価を使用します。
- 作業指示書を準備します（あるいは少なくともレビューします）。それらが安全であり、それに従って作業が行われることを確実にします。
- 定期補修工事のようなリスクの高い運用中は、（リスクに）に近い要員数を最小限に抑えます。
- インシデントの記録と教訓を維持するとともに、確実に伝達し、そこから学ぶ必要のある人によって使われることを確実にします。
- 活動に必要な経験と訓練に見合った要員配置を行います。
- オペレータがクリティカルな活動を実施するのを支援できるプロセス制御システムを提供します。
- 監査を実施します。監査（および他のフィードバック情報源）で使用される先行指標を確立するか、安全エンジニアリングが適切な先行指標を特定していることを確実にします。

運用管理担当者のプロセスモデルの欠陥

- エチルベンゼンを全てのプロセス条件下で安全な物質（不活性媒体）として扱いました。そのため加熱フェーズが危険であるとは考えませんでした。
- 定期補修工事に関与する要員は、適切な訓練と経験を持っていると考えていました。
- シェルの同じ設計の他の設備での同様のインシデントについて、彼らは知らなかったのでしょうか？それともユニット4800に関係するとは考えなかったのでしょうか？
- 一般的に、彼らはプラントに存在したリスクについて不正確な見解を持っていました。
- これらの欠陥につながる不適切なフィードバック：
  - プラント安全管理による報告書には、加熱フェーズに対するフィードバックは示されていませんでした。
  - プラント安全管理は、運用管理に対して、正しいリスク評価を提供していませんでした。

コンテキスト要因：（省略します。完全な分析を参照してください。以下の要約にも含まれています。）

事故における運用管理の役割の要約：

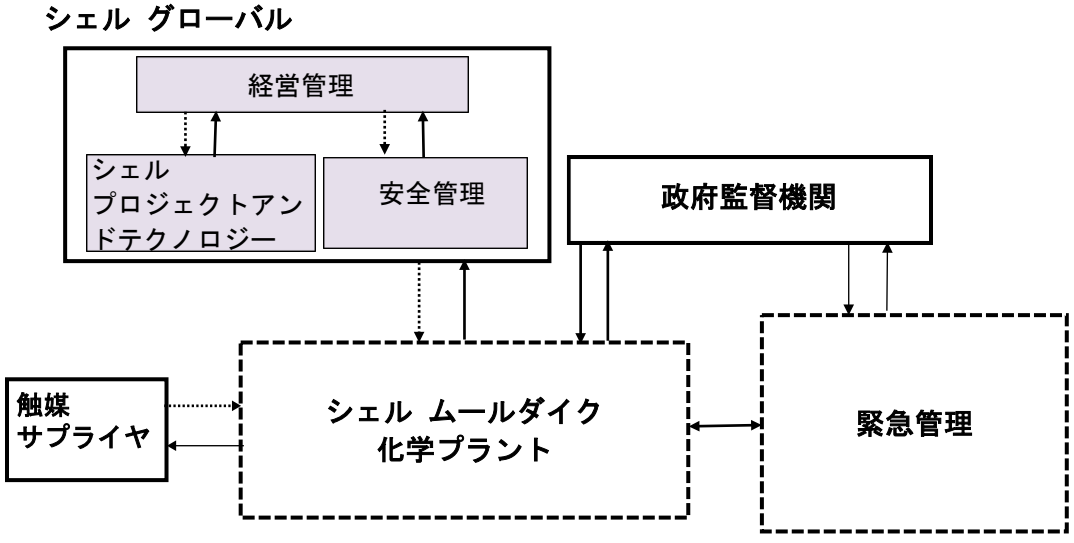
- 運用管理は、実行されたリスク分析やリスク分析に使用された手順の欠陥を識別していませんでした。リスク分析は、オランダの規制当局の最低限の要求に準拠しており、見た目はシェルの要求に準拠していました。
- 経時的な変化について、MOC手順に準拠しているかの評価を受けていませんでした。
- 作業指示書は、安全エンジニアリングの監督なしに、オペレータによって作成されました。その作業指示書は、シェルの作業指示書フォーマットに準拠しておらず、加熱速度のような作業に必要となる重要な基準を含んでいませんでした。事故において重要な要因である窒素流量は作業指示書では無視されていました。
- プロセス制御システムは、通常の生産フェーズに対して、プラントをコントロールするように構成することが意思決定されていましたが、生産以外のフェーズや保守フェーズは対象となっていませんでした。これらの活動はリスクが高いとは考えられておらず、手動運用で十分であろうと考えられていました。この意思決定の理由は、事故報告書にはありません。
- おそらく起動フェーズが危険であるとは考えていなかったため、異なる請負企業の２人の従業員に対して、起動時に隣接したユニットでの作業が許可されていました。
- 運用管理は、起動運用に対し、安全報告書で要求された資格を持つオペレータを割り当てませんでした。事故報告書には、その理由は示されていません。
- 運用管理は、同様のプラントにおける教訓や、シェル ムールダイクにおける1999年の教訓を、ユニット4800の設計と運用に確実に組み込むようにしませんでした。
- シェル ムールダイクの安全管理システムは、非安全な状況が見過ごされること、内部の手順が守られないことを阻止しませんでした。事故報告書には、誰が安全管理システムを作ったのか、安全管理システムを正しく機能させることを保証する責任が誰にあるのかについての情報はありません。
- シェル ムールダイクの内部監査では、これらの欠陥は一切示されていません。なぜ内部監査が有効に機能しなかったのかを判断するための十分な情報は、提供されていません。
- シェル ムールダイクには、安全管理が統合されたビジネス管理システムがあります。詳細は明らかにされていませんが、一般的にこれは良くない慣行であり、ディープウォーター・ホライズンのような石油化学企業の事故の主要な要因となっています。意思決定は、考慮されなければならない全ての要因に関する完全な情報に基づき、行われる必要があります。要因は、リスク情報を不透明な方法で統合することにより、失われることがあってはなりません。

推奨事項:

- 適切なMOC手順を確立し、それに従って運用されていることを確認してください。変化が生じた場合は、変化の影響を受ける可能性がある想定を再検証してください。これは、想定を記録しなければならないこと、想定がもはや正しくない可能性がある場合を識別するための先行指標を確立しなければならないこと、想定に影響を与えるかもしれない変化への対応と検証のためのプロセスを確立しなければならないことを意味します。
- シェル ムールダイクの安全管理システムは、なぜこの事故を防ぐことができなかったのかに着目して徹底的な見直しが行われる必要があります。この事故の主要な要因は、安全管理システムが管理するべき基本的な活動に結びついています。
- 作業指示書の作成・監督プロセスにおけるコントロール・監督の欠落、ハザード分析・リスク評価手順の不適切、定期補修工事の実行に必要なスキル・専門知識を持たないオペレータの割り当て、過去の教訓の不適切な活用、事故前に欠陥を識別できなかった監査手順といった事故原因を排除するために、手順を更新してください。
- 通常の生産以外の機能を実行するオペレータに対して、適切な支援を提供できるようにプロセス管理システムを改善してください。

シェル グローバル（企業）

ここには３つの基本的な機能が含まれています。エンジニアリング設計（シェル プロジェクトアンドテクノロジー）、企業の安全管理、そして取締役会を含む経営層の企業管理です。シェル グローバルの経営体制における安全責任の正確な分担は、事故報告書に含まれていないため、ここで想定したものとは異なる形でシェル グローバルの経営体制全体に分散しているかもしれません。肝心なことは、それらの責任が必ずどこかに存在する必要があるということです。



シェル プロジェクトアンドテクノロジー（エンジニアリング）

企業レベルでプラント設計が行われ、その技術のライセンスが施設に付与されていました。

安全に関する責任

- 安全設計の作成：ハザード分析を実行（または他のグループによって作成されたハザード分析の結果を利用）し、設計内のハザードを排除または軽減します。
- 設計自体において、設計者が排除または十分に軽減することができなかったハザードにつながるシナリオを回避できるように、プラントを運用しているオペレータに対して、設計、ハザード、および操作情報を提供します。
- 設計による運用から学び、そのフィードバックに基づいて設計を改善します。

シェル プロジェクトアンドテクノロジーの役割の要約:

ライセンス先に提供された設計データは、プラントで作業指示書を作成する人が使用することはできませんでした。この設計には、最初の設計段階のハザード分析で発見されなかったセーフティクリティカルな設計上の欠陥がありました。これらの欠陥は、シェルの他のプラントにおける関連したインシデントについての情報を受け取った後、修正されませんでした。欠陥の一つに、温度センサの数が不適切であることと、過度の圧力が発生しても圧力逃し弁が処理できないことが原因で発生した過剰圧力のインシデントがありました。シェル ムールダイクのユニット4800の定期補修工事のための非安全で不完全な作業指示書は、シェル プロジェクトアンドテクノロジーによって承認されていました。

未回答の質問：

シェルでの運用に関する詳細な情報は、事故報告書に含まれていないため、非安全なコントロールが行われた理由を正確に判断することは困難です。なぜ設計上の欠陥が混入したのか、設計プロセスをどのように通過したのかなど、CAST分析では、回答よりも、次のような多くの質問が生じます。*シェル プロジェクトアンドテクノロジーまたは他のグループは、どのような種類のハザード分析を行っていますか？1999年のシェル ムールダイクおよび2011年の南海でのインシデントの後、識別された設計上の欠陥が修正されなかったのはなぜですか？シェルの各プラントでの運用を踏まえた安全性に関する設計フィードバックとして、他にどのようなものがありますか？プラント設計の安全面（ハザード）に関して、シェル プロジェクトアンドテクノロジーからライセンス先に、どのような情報が提供されていますか？設計書にはどのような情報が含まれていますか？もし技術者がオペレータの代わりに作業指示書を作成した場合、設計データはライセンス先が安全な作業指示書を作成するのに十分なものですか？誰がその作業を実施するのか知りませんでしたか？なぜシェルの要求フォーマットにも従っていない非安全な作業指示書を承認したのでしょうか？起動と起動時のハザードについて、設計書にはどのような情報が記載されていますか？設計プロセスにおいては、どのような種類のハザード分析が実施されていますか？プロセスで変更が行われたときに、どのように安全を確保していますか？安全性に関する前提はどのように記録されており、これらの前提を再検討するトリガー（trigger）となるものは何ですか？設計者は運用についてどのようなフィードバックを得ていますか？*

推奨事項：

- 事故に寄与した設計特性を修正してください。これらの欠陥が設計プロセスをどのように通過したかを判断し、設計プロセスと設計レビュープロセスの両方を改善してください。作業指示書を作成する人が理解できるよう設計書を修正し、ライセンス付与した技術の導入を安全に行うために必要な全ての情報を含めてください。作業指示書が完全かつ安全であることを確実にするために、シェル プロジェクトアンドテクノロジーによる作業指示書のレビュープロセスを修正してください。シェル プロジェクトアンドテクノロジーで使用されているハザード分析プロセスをレビューし、改善してください。

企業の安全管理

事故報告書には、シェルの安全プログラムあるいはそのプログラムの事故への寄与の可能性について言及はありません。CAST分析では、シェル ムールダイクの地域レベルで何が起きたのかについての情報を踏まえ、欠陥のある安全活動をコントロールするためには、適切に設計された企業レベルのSMSの責任とは通常どのようなものになるのかを予測しました。企業レベルで安全に対する最終的な責任を持つ人がいたはずですが、その管理の役割に関係する活動が企業ストラクチャー内のどこにあったのか、また、これらの活動が発生したのかどうかさえ明確ではありません。

関連する責任

- 子会社にライセンス付与した設計に関するハザード分析の実施を含む、プラント設計の安全性を確保します。
- シェルの様々なプラントや施設における運用上の安全性を監督します。
- 安全に関する変更手順の管理：変更手順を作成し、確実に守られるようにし、インシデントからのフィードバックを用いて改善します。
- インシデントや教訓などについて、世界各地のプラント間でコミュニケーションが確実に取れるようにします。
- シェル全体の安全情報システムを作成および更新し、その情報がシェル企業内およびグローバルレベルの両方で適切に伝達されることを確実にするとともに、それが完全かつ有用であることを確実にします。

企業の安全管理の役割の要約：シェルの地域プラントにおける、リスク状態と安全管理システムの有効性についての誤った見解があったと見受けられます。欠陥のあるプロセスモデルは、不適切なフィードバック（監督や先行指標を含む）に関係している可能性が最も高いです。事故報告書によると、シェルは時代遅れとなったHEMPと蝶ネクタイモデルを使用しています。企業レベルにおいて、他にどのようなハザード分析およびリスク評価が用いられているかについての情報はほとんどありません。恐らくHAZOPも（プロセス産業のほとんどで行われているように）実施されているでしょうが、それは報告書には記載されていません。蝶ネクタイモデルは、1960年代後半の約60年前に考案されたものですが、単純な事象連鎖モデルを使用しており、化学プラントを含む今日の複雑なシステムにおけるハザードとリスクを捉えるには単純すぎます。繰り返しになりますが、CAST分析では、事故における企業レベルの安全管理の役割を理解し、今後、より効果的な安全管理を提供するために、回答が必要な質問が数多く提起されます。

推奨事項：シェルの安全監査を改善してください。全てのリスク評価とハザード分析のプロセスをレビューし、総体的に、安全分析と安全管理の両方について安全性に対するアプローチを改善してください。大手石油会社の中で、手法を最新化する必要があるのは、シェルだけではありません。石油化学産業には、回避できる事故やインシデントが多すぎます。

より具体的には、事故報告書において、「シェルはリスク分析方法を評価し、改変するべきです。これには過去の推測と前提の再評価に関する手順と方針を含める必要があります。新しいリスク分析を実施し、適切な対策を講じ、これらの分析を実行するチームが重要な能力を確実に十分持てるようにしてください。これまで除外されていた、リスクに基づく前提には特に注意してください。」と述べられています。

企業の安全管理システムを評価し改善します。プロセスの安全に関するインシデントから学ぶための手順を改善します。監査や主要な指標、インシデントから学ぶための手順など、より良いフィードバックメカニズムを作成します。

経営層の企業管理

責任：

- 以下に対して必要となる全ての手段を取ります。
  - 主要な事故の発生を防ぎます。
  - 事故が発生した場合は、人や環境への影響を低減します。
- 作業に関係する全ての面において、従業員の健康と安全を確保します。（労働条件に関する法令やその他規制に基づいて）
- プラントのある国の政府規制に従います。
- 効果的な安全管理システムを構築し、強力な安全文化方針を確立します。 SMSと安全方針が遵守され、それらが有効であることを確実にします。

プロセスモデルの欠陥

リーダーは、シェルの企業レベルや各施設における安全の状態と定義された手順の有効性について、明らかに誤解をしていました。

コンテキスト要因（省略。完全な分析を参照してください。）：

経営層の管理の役割の要約：

経営層は、効果的な安全管理システムが構築されていることを確実にする責任があります。シェルとシェル ムールダイクはともに、効果的な安全管理システムの典型的な方針に違反していました。シェルの企業レベルで安全を監督するグループは、明らかに効力がありませんでした。企業管理における安全関連責任に関しては、事故報告書には何も含まれていません。

また、事故報告書には、安全性に関する標準的な経営層の責任が、効果的に実行されなかった理由を説明できるコンテキスト情報は含まれていません。シェルには、安全文化に問題があるようです。（後述するシェルにおける安全文化と上位レベルの安全方針に対する分析を参照）。全世界の設備の安全性に対する企業管理監督の観点から見た化学産業の文化は、どのようになっているのでしょうか？

事故報告書によると、シェル ムールダイクでは安全管理システムが事業管理システムと統合されていました。企業レベルでも同じだったのでしょうか？ これは非常に不適切な慣行（practice）です（そして、ディープウォーター・ホライズン事故の要因でした）。安全リスク評価は、情報が高レベルの意思決定者から見えなくならないよう、ビジネスリスク評価とは分離されている必要があります。

推奨事項：SMSの設計をレビューし、安全性検討、変更手順管理、事故からの学習における欠点や規制（例えば、経験豊富なオペレータの配置、作業指示書フォーマットの遵守）への不遵守など、明らかな方針違反を防ぐことができなかった理由を突き止めてください。このような、手続き上の明白な違反を見つけるために、監査がなぜ有効に機能しなかったのかを判断してください。このような過失が起きたのは初めてだった可能性もありますが、まずありえません。単なる漏出数ではなく、リスク増加を示すよりよい先行指標を識別すること、安全管理システムが通常状態から逸脱し、リスクが増加していることを識別する他のフィードバック手段を作成することを含め、監査手順を強化してください。変更手順と企業の安全方針の管理が確実に守られるように、より良いフィードバック経路を確立してください。

触媒サプライヤ

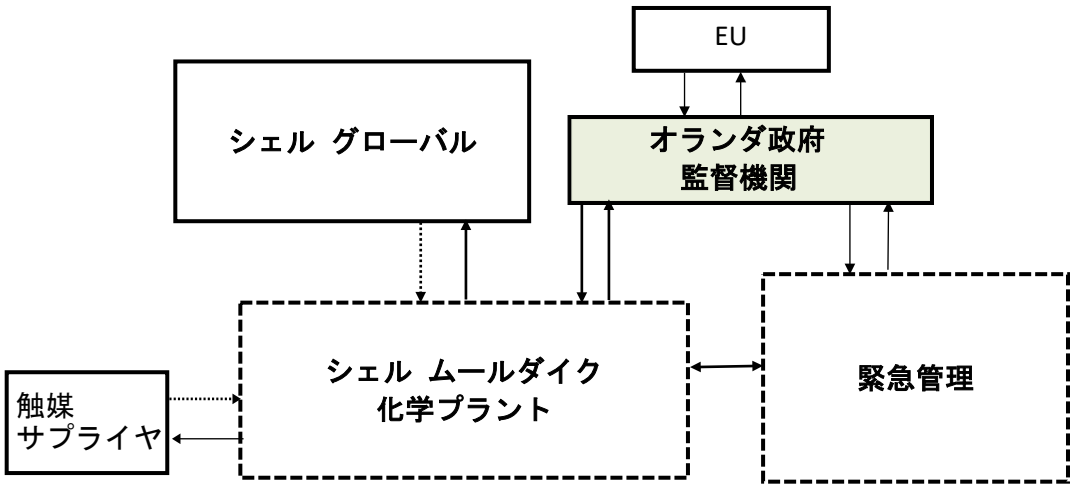
安全に関する責任

- 設計中および/または運用中の反応器における触媒の使用を評価するために、必要な情報を顧客に提供します。
- 使用上の安全性に影響を与える可能性のある変更が、触媒に加えられた場合は、顧客に警告します。

事故における触媒製造業者の役割の要約：触媒に加えられた変更は、シェルに注意喚起されませんでしたが、新しい安全情報シートに含まれていました。触媒製造業者は、変更が顧客に与える影響を判断することはできませんが、顧客が変化を気づくことができるように、変更が加えられたことと、変更は何であるかを明確に警告する必要があります。

推奨事項：潜在的にクリティカルな変更が適切に伝達されるように、シェルとサプライヤ間の契約関係を変更してください。変更が明確となるように、情報シート内で変更を加えてください。

オランダの規制当局



ここでは、オランダのすべての安全と環境に関する監督機関をまとめて示します。主に２つの方針があります：

1. Brzo: 企業は事故を防ぐためにあらゆる対策を講じなければなりません。また事故が発生した場合は、人間および環境への影響を低減する必要があります。企業は、重大事故防止方針（PBZO）に方針の前提を定め、安全報告書（VR）を作成し、安全管理システムを組織することによって、この義務を履行する必要があります。
2. Wabo: 規制当局は、環境観点の許可、つまり環境の安全性に関連する規制を、企業が遵守しているかどうかを検査しなければなりません。

安全に関する一般的な責任

- 環境と公衆を保護するため、オランダの法律に対する監督と執行に責任を負います。プロセスの安全性を重視したBrzo検査および環境の安全性を重視したWabo検査を実施します。
- オランダ国内でのEUの安全衛生法の執行に責任を負います。

より具体的な責任：

- 監督する責任がある企業の欠点を識別します。
- 監督と執行を通して、セーフティクリティカルなプロセスを改善するよう企業に働きかけます。欠点を識別し、インシデントや事故の根本的な原因を調査して検出することを企業に要求します。識別された欠点が是正されることを確実にします。
- プラント、手順、およびプロセスに加えられた変更を評価します（ただし、企業のリスク分析を実行することは想定されていません）。
- 保守や化学反応器の起動など、セーフティクリティカルなプロセスに最大限の注意を払います。

プロセスモデルの欠陥

事故報告書は、「規制当局は、シェル ムールダイクの安全管理システムについて肯定的な見方をしていました。シェル ムールダイクの欠点の数によって、この見方が改められることはありませんでした。」と述べています。

コンテキスト要因（省略。完全な分析と以下の要約を参照してください。）

サマリ：

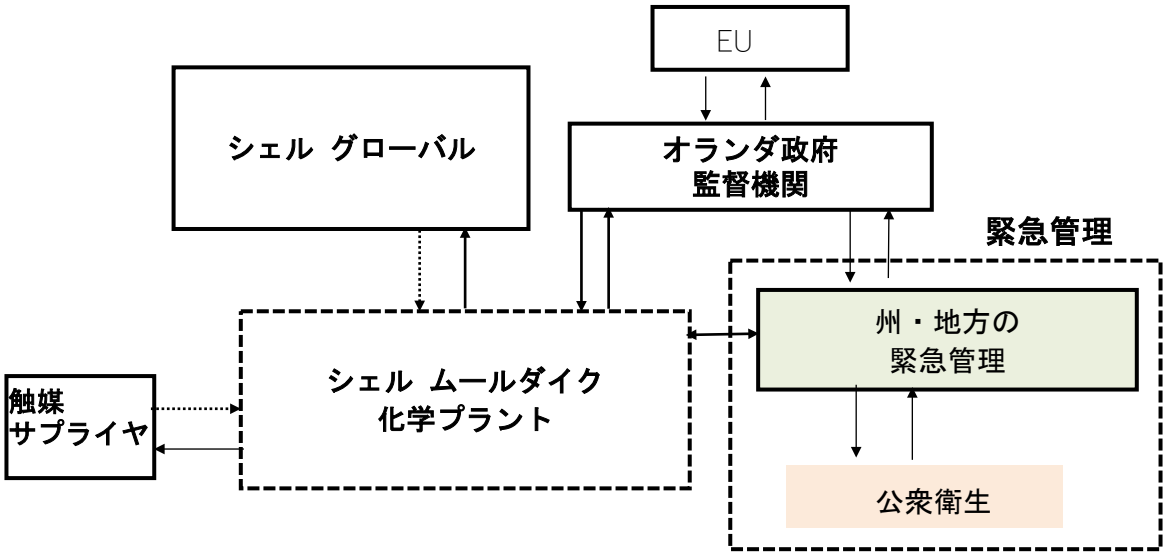
少なくともリソースが限られているなどの理由から、政府当局は「システム向けの監督」を行います。これは事実上、リスクの高い活動のオペレータに責任を負わせ、彼ら自身の欠点を識別するという、実績ベースの規制の一形態です。規制当局は、安全管理システムの設計と運用の両方を確認し、年１回の検査を実施して、設計されたとおりに運用されていることを確認します。規制当局は、企業が、文書化した正しい手順を持っていることを確認し、使用されていることを抜き取り検査するだけです。

彼らは、シェルが自社のSMSに従って行動していないことに気づいていないか、または反応を示しませんでした。いくつかの例を以下に示します：プラントへの変更や改修について、リスク分析は終始一貫して行われていませんが（シェルSMSの要求に違反）、この欠陥は規制当局によって指摘も修正要求もされませんでした。変更は、安全性について十分に評価されていませんでした。起動の実行に際し、専門知識を持っていることやトレーニングを受けることへの要求は強制されていませんでした。

事故報告書は、規制当局がシェル ムールダイクに、違反の可能性のある行動を許可したことを示唆しています。プラントのシナリオの欠陥は違反と考えられるべきでしたが、そのようはなりませんでした。そのシナリオは最新の状態ではないか、不完全なものでした。限られたリソースと時間の下で作業することは、どの監督モデルでも困難ですが、システムレベルの監督には、公衆の安全を確保する上で大きな限界があります。事故調査の結果、シェル ムールダイクにおいて定義され実施されていた安全管理運用には多くの欠陥がありました。*では、規制当局がその欠陥を発見できなかった監督モデルは、何が誤っているでしょうか？*

推奨事項：
定期補修工事を含めたリスクが最も高い活動に対しては、優れた監督が必要です。規制当局は、最も危険な活動に対して厳密な手順が使用されていること、および安全管理システムが効果的に機能し、規則に準拠していることを監視し、確実にする必要があります。限られたリソースが、効果的な行動を妨げることはありません。単に、実施される活動について、より知的な選択を必要とするだけです。安全管理システムの有効性に対する、よりよい評価手順と監視が必要です。規制当局は、シェル ムールダイクの爆発のような事故を防止する上で、効果的な活動を確実にするために、システムレベルの監督を再考する必要があります。

緊急サービス



責任

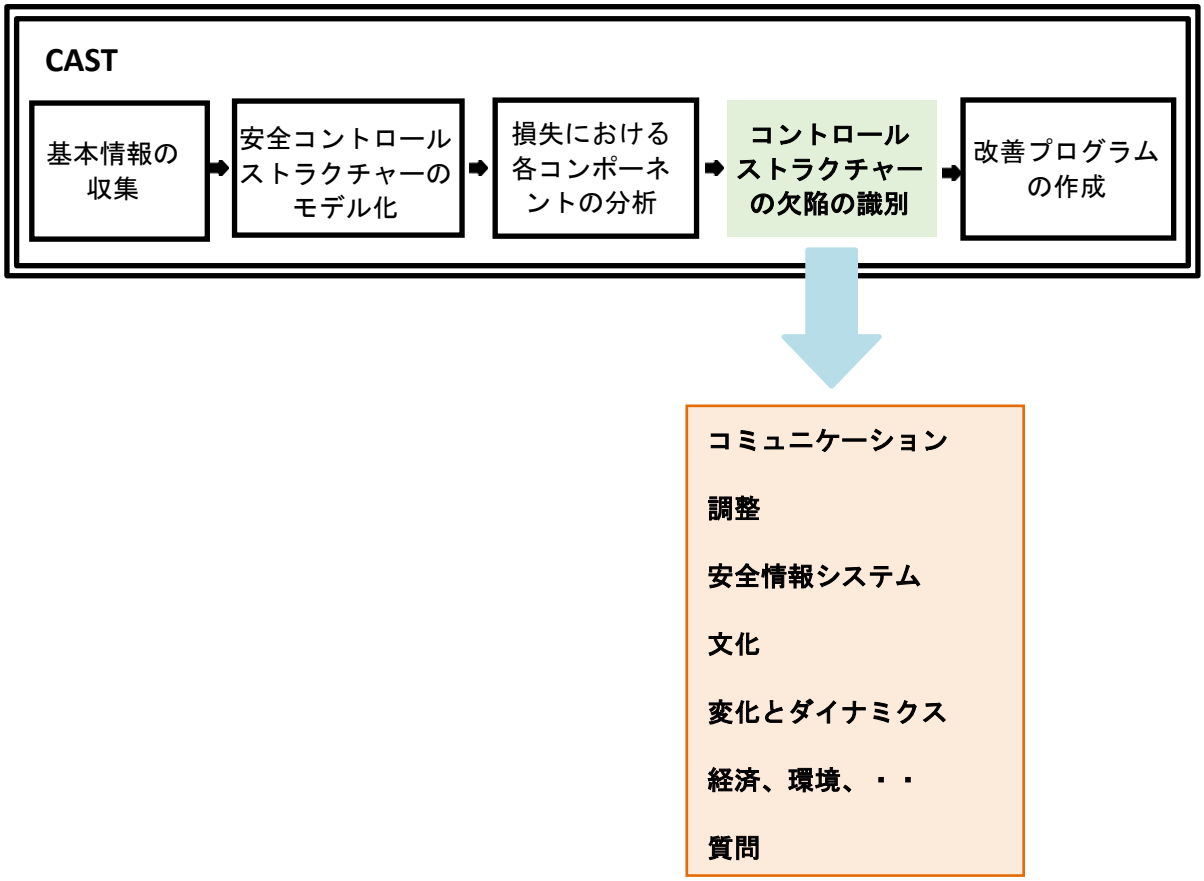
- 消化活動[本事故においては、共同消防隊が効果的に実施した]、危機管理、特に以下を含む危機コミュニケーション：
  - 市民へのインシデント関する周知
  - 放出された物質を調整した基準で測定
  - 電話相談窓口の運用
  - 放出された物質の測定結果とそれに基づく勧告の市民への周知

事故における緊急サービスの役割の要約：
緊急サービスは、責任を果たす上で非常に効果的に機能しましたが、事故対応において特にコミュニケーションにはいくつかの欠陥が発見されました。例えば、これらの状況で使用するために設計された国家危機管理システムの代わりに、多くの人がWhatsAppを使用しました。本事故の性質上、人命損失にはつながりませんでしたが、他の状況下では起こり得ます。

推奨事項：なぜ多くの人がWhatsAppを代わりに使用したのか、そして国家危機管理システムがそれらの機能をどのように取り入れることができるのかを含めて、この事例から学んだことは、国家危機管理システムを改善するために使用されるべきです。

この事例のように損失を引き起こさなかったシステムコンポーネントであったとしても、事故はストレスがある状況における実際のシステム運用を注意深く見る機会となり、貴重な学びを得る機会となります。この例で示されているように、ほとんどのコンポーネントは何らかの形で事故に寄与したか、または計画どおりに動作しなかった可能性があります。オペレータがしたこと、しなかったことだけを見ると、オペレータが損失の主要な要因であるように見えてしまいます。通常、この事故のように、オペレータの振る舞いの理由を調べれば、オペレータの行動が理解できるようになります。
本セクションでは、CASTでの個々のコンポーネント分析の例を示しました。しかしながらコントロールストラクチャー内の個々のコントローラを調べるだけでは不十分です。コントロールストラクチャー全体の運用も検討する必要があります。

全体としてのコントロールストラクチャーの分析



4.損失に寄与する概括的で体系的な要因を調査することによって、全体としてコントロールストラクチャーにおける欠陥を識別します。体系的な要因は、個々のシステムコントロールストラクチャーのコンポーネントをまたぎます。

ここまで説明してきたCASTの分析プロセスは、個々のシステムコンポーネント、および、他のコンポーネントに対するそれらのコントロールに焦点を当てています。それぞれのコントローラに割り当てられたコントロールと制約を、強制することができなかった理由を調べています。

それとは対照的に、CASTのこのパートでは、コントロールストラクチャーの全体と、設計されたコントロールの無効性につながった体系的な要因を調べます。おそらく、分析において最も構造化されていない部分ですが、ハンドブックのこのセクションでは、何を探すべきか、そして見つけたときに、それが果たした役割をどのように説明するかについてのガイダンスを提供します。

体系的な分析は、危険なシステム状態を防ぐために、安全コントロールストラクチャー内で一緒に機能する、すべてのコンポーネントの動作と相互作用に影響を与える要因に、焦点を当てています。個々のコンポーネントではなく、システム全体を確認することで、安全コントロールストラクチャーの、さまざまなコンポーネントの相互作用に影響を与える原因要因を特定できます。これらの体系的な要因は、もう一つの方向として、個々のコンポーネントが個々の安全責任を果たせない理由と、それらの動作が全体として、システムの安全制約を満たさなかった理由を理解するための方法を提供します。つまり、安全コントロールストラクチャーは通常、１つのコンポーネントの誤動作だけで事故につながることがないように作成されます。ただし、体系的な原因要因は、コンポーネントの多くまたはすべての動作に悪影響を及ぼし、これらの取り組みを無効にする可能性があります。

これは、スイスチーズやドミノモデルなどの事象ベースのモデルでは除外されている、事故分析へのシステムアプローチの真にユニークなところです。すべての防護壁が正しく機能することを妨害すると同時に、事故を防ぐために作成されたすべての防護とチーズスライスに「穴」を生じさせてしまう原因要因があります。わずかな原因要因に焦点を当てたり、１つまたはいくつかのコンポーネントの動作の観点で事故を説明することから離れることで、非常に強力な予防策を特定するために使用できる、因果関係のより大きなビューが提供されます。

以下は、考慮される可能性のある体系的な要因の一部です。このリストは包括的ではなく、単なる出発点です。

- コミュニケーションと調整
- 安全情報システム（safety information system）
- 安全文化
- 安全管理システムの設計
- 経時変化とダイナミクス：システム内と環境内
- システム環境における内外の経済的要因および関連要因は、これまでの分析ではカバーされていません。これらのうちのいくつかは、経時変化を考慮しながら生成することができます。

コミュニケーションと調整

損失につながる要因の多くは、安全コントロールストラクチャーのコンポーネント間の不適切な*コミュニケーション*と調整に関係しています。調整とコミュニケーションの欠如は、一貫性のないアクション、欠落したアクションなどにつながる可能性があります。

例としては、2002年にドイツ南部の町であるユーバーリンゲンで、２機の航空機が衝突したことが挙げられます。計画が不十分な保守作業により、航空管制塔のほとんどすべてのコミュニケーションリンクが一時的に切断されました。一部の停止は事前に分かっていましたが、その他は保守中のエラーが原因でした。コミュニケーションの喪失を計画しておけば、役に立ったでしょう。たとえば、当直の航空管制官は、起きうる衝突についての聴覚的、視覚的警告が、保守作業中に使用不可能になることを知りませんでした。保守

作業が計画され、変更手順の管理が使用されていれば、保守作業に対処するために緊急時の措置を講じることができたはずです。通信の停止により、このような衝突を防ぐために設計された組み込みの冗長性が、すべて排除されてしまいました。

意図していたコミュニケーションリンクと、事故の際に何が機能していたかを描くことにより、視覚的に説明することができます。図16は、システムに設計された通信チャネルを示しています。図17は、衝突時に機能していたものを示しています。このタイプの図は、何が起きたのか、そしてその理由について理解し、伝達するための強力なツールです。衝突が起きようとしているのを見た別の場所の管制官は、電話回線が切れていたので、警告を発するために連絡をつけることができませんでした。衝突時に２機を管制していた航空管制官は、不測の緊急着陸により過負荷になったときには、他の航空管制施設に連絡して過負荷を解消する方法はありませんでした。

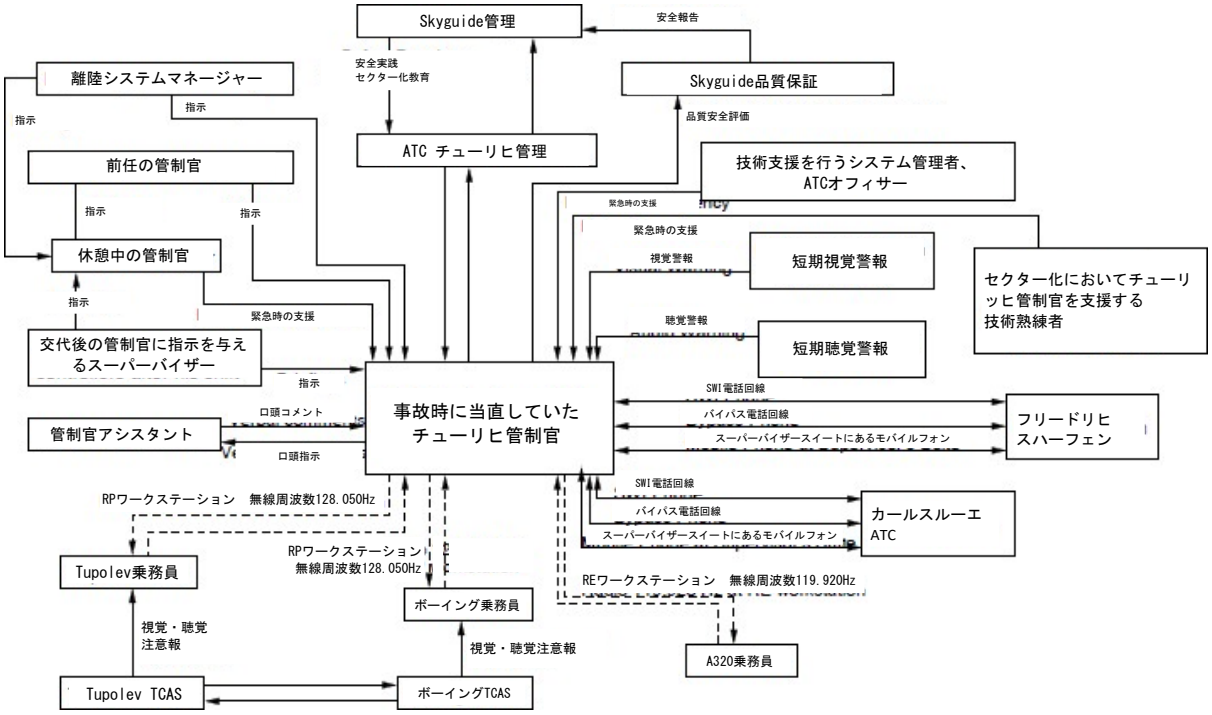


図 16：ユーバーリンゲン事故における理論的なコミュニケーションリンク

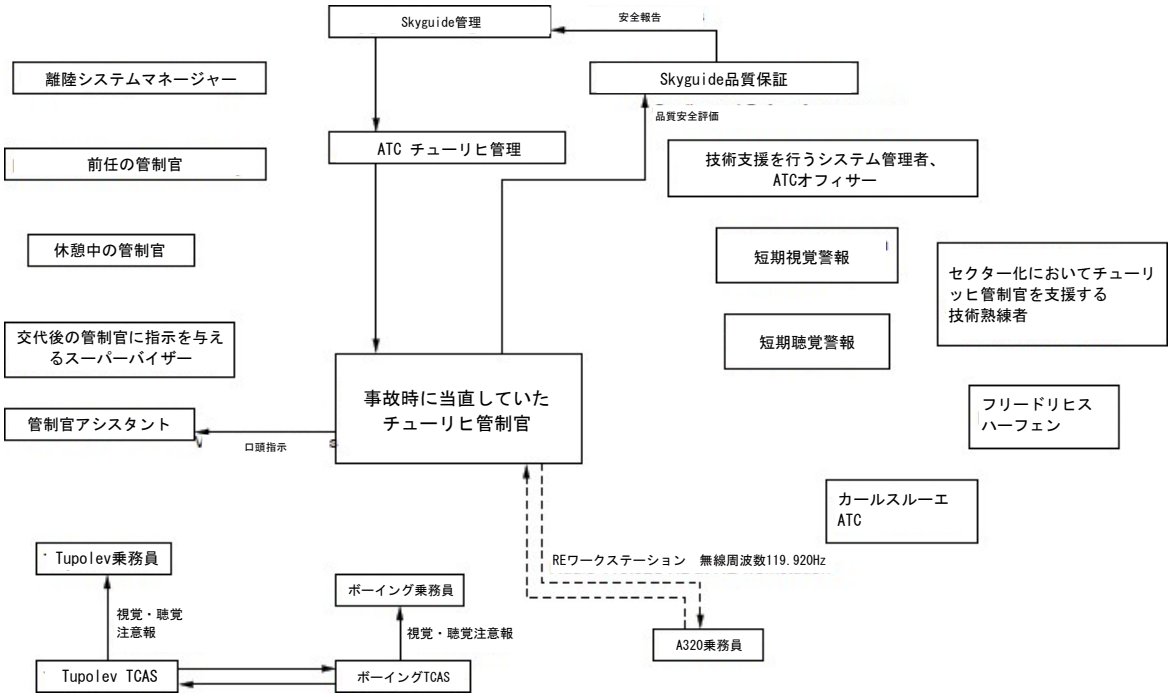


図 17：事故時の運用のコミュニケーションリンク

この場合のコミュニケーションと調整の問題は、事故時に限定されていました。しかし、この問題は、以前から長い間存在していた可能性があります。ときには、一方のコントローラは、もう一方のコントローラが責任を持っていると想定していますが、そのもう一方のコントローラは、最初のコントローラが責任を持っていると考えることがあります。一例として、カナダの水質汚染インシデントでは、環境省（MOE）と保健省（MOH）の両方が、同じ監視業務の一部を実行する責任がありました。地元のMOH施設は、MOEがこれを実行していると想定し、自らの活動を減少させましたが、MOEは予算が削減されており、その後の業務を実行しませんでした。事故後に共通している発見は、責任のある複数のグループが重複する責任を持つ場合には、それぞれのグループが、別のコントローラが必要な監視を実行していると、想定する可能性があるということです。あるいは、２つのコントローラの責任が重複していない場合もありますが、間接的に矛盾する指令を提供するかもしれません。

安全コントロールストラクチャーにおける不十分なフィードバックは、しばしば意思決定の不備に寄与することが見つかる、重要な種類のコミュニケーションの１つです。もちろん、他の種類のコミュニケーションも重要です。シェル ムールダイクの事故では、シェル グローバル プロジェクトアンドテクノロジーとシェル ムールダイクの間、およびシェル ムールダイク自体のグループ間で、無効なコミュニケーションが発生していました。さらに、製造業者による触媒に対する変更はシェルに通知されませんでした。事故当時、必要なコミュニケーションチャネルは存在していましたか？ それらは完全に機能していたでしょうか、あるいは必要な情報の伝達を妨げるものがあったのでしょうか？

Engineering a Safer World[17]の第５章で分析されたfriendly fire事故では、２つの異なるコントローラ間で追跡責任を振り分けることにより、味方の航空機を追跡する責任における潜在的なあいまいさは解消されていました。この責任の振り分けは、効率向上のための非公式な試みなどの要因によって時間の経過とともに崩壊しており、その結果、どちらのコントローラも、事故の起きた日に撃墜された航空機を追跡していませんでした。

[17] Nancy Leveson. Engineering a Safer World, MIT Press, 2012, Chapter 5.

安全コントロールストラクチャーのコンポーネントの、想定され設計された動作に対して、実際に起きることを確認するためのパフォーマンス監査が行われていませんでした。事故後、すべてのコミュニケーションリンクを調べて、設計において、重要な情報の伝達が可能であることを確認する必要があります。設計が適切であったとしても、伝達経路は適切に機能していましたか？ そうでない場合は、不十分なコミュニケーションの理由を特定する必要があります。コミュニケーションチャネルには、情報の伝達とは矛盾する目的を持つ人が関与する場合があります。場合によっては、コミュニケーションリンクが単に失敗した可能性があります。また、ユーバーリンゲン事故のように、保守のために意図的にダウンしている場合もあります。

たまに、コミュニケーションと調整のリンクが利用可能だとしても、コントローラがそれを知らないことがあります。friendly fireの例では、時間の経過とともにリンクが劣化し、動作しなくなっていました。

コミュニケーションを分析するには、最初に重要なコミュニケーションチャネルを理解してモデル化する必要があります。レキシントン空港での誤った滑走路離陸事故に対するポール・ネルソン機長によるCAST分析では、以下のコントロールストラクチャーが作成されました。コミュニケーションチャネルが存在しなかった（設計に含まれなかったフィードバック経路も含む）か、事故当時の様々な理由によって動作不能であったところを、点線で示しています。安全コントロールストラクチャーを描画し、設計で欠落しているフィードバック経路を見つけるだけで、コントロールストラクチャーの設計に問題があることを示す強力な手がかりになります。すべてのコントロールループには、適切な意思決定を行うためのフィードバック経路が必要です。

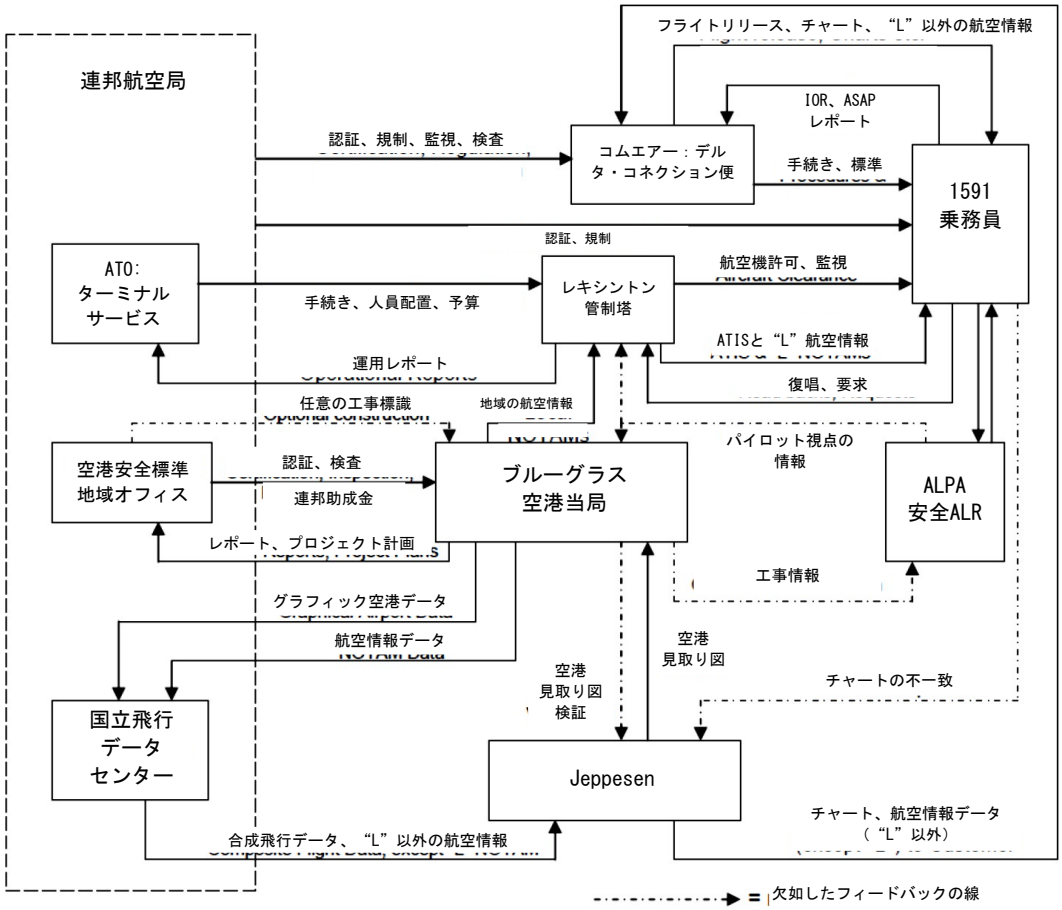


図 18：レキシントンでのコムエアーの誤った滑走路事故の安全コントロールストラクチャー。コントロールは上から下ではなく左から右に描画されます。点線は、損失の原因となっ

たフィードバックとコミュニケーションの欠如を表しています[Paul Nelson, A STAMP Analysis of the LEX Comair 5191 Accident, Master's Thesis, Lund University, June 2008.この論文へのリンクは付録Ａにあります。]

前述した他のよくある種類のコミュニケーション障害は、問題報告経路で発生する可能性があります。調査員は、多くの事故において、問題は損失を防ぐために時間内に特定されたが、多くの場合、必要な問題報告経路が使用不可能であったために、使用されなかったことを発見しています。

安全情報システム

ケランは、さまざまな企業の安全情報システムの研究で、安全情報システムの品質が、事故率の高い企業と低い企業を区別する上で２番目に重要な要素であることを発見しました[Kjellan1982][18]。安全情報システムの用途には、ハザードに関する情報の保存と伝達、事故の前兆となる傾向と逸脱の検出、安全管理と基準の有効性の評価、モデルとリスク評価の実際の行動との比較、ハザードの特定と管理による設計と基準の改善などが含まれます。安全調査には、組織の安全情報システム（SIS）の検査を含める必要があります。

シェル ムールダイクの事故報告書は、シェルまたはシェル ムールダイクのSISに関する情報を提供していませんが、インシデントや過去の保守停止から学習しない、相容れない証拠が生じたときに過去のハザードおよびリスク評価の欠陥を特定しないなど、適切に設計されたSISであれば防止できた可能性のある欠損の多くの例について説明しています。事故報告書は、ユニットの設計とユニットの最終的な運用管理の間で重要な情報が失われたことも示しています。報告書は、「したがって、設計段階で入手可能な情報と最終的に実施された運用管理との間に矛盾が生じた」と述べています。適切に設計された安全情報システムは、これらの種類の問題を防ぐことができるはずです。

安全情報システムを持っているだけでは、それが有用または使用されることを保証するものではありません。データは、収集方法によって歪む可能性があります。一般的な問題は、フィルタリング、抑制、および信頼性の欠如です。事故およびインシデントの報告で収集されるデータは、管理上の問題や組織の欠陥などの体系的な要因ではなく、近いところに位置する事象やアクターに焦点を当てる傾向があります。特にチェックリストを使用する場合には、限られたカテゴリの条件が識別されることがあります。偏りのない体系的な方法で複数のソースから比較可能なデータを取得することは困難です。

データ収集は、ハザードや原因要因に関する過去の経験がより限られている新しい種類のシステムの事象よりも、過去に発生したものに類似した事象に対して役立つ傾向があります。ソフトウェアエラーとコンピュータの問題は、知識の欠如やそのようなエラーを受け入れるための一貫した分類の欠如、または単なる原因要因として無視されるために、インシデント報告ではしばしば省略されるか、不適切に記述されます。CASTを使用することで、安全情報システムに体系的な要素を含めることを促進できます。

よくある欠陥として、事故の傾向や変化、およびその他の前兆を検出するため；事故の予防に使われるコントロールの有効性を評価するため；業界の人々のリスク評価を実際の行動と比較するため；事象から学び、安全管理の実践を改善するために必要となる情報を記録しないことが含まれます。

もちろん、単に情報を収集するだけでは十分ではありません。大量のデータを学習に役立つ形式に統合することが難しいため、問題が発生する可能性があります。今日のデジタルテクノロジーでは、大規模なデータ収集チャネルを設計するのは簡単ですが、結果と

[18] 最高ランクの要素は、経営トップレベルの安全性に関する懸念でした。Urban Kjellan, An evaluation of safety information systems at six medium-sized and large firms, *Journal of Occupational Accidents*, 3:273-288, 1982.

して生じるすべてのデータを分析するための時間と労力を見つけることは困難または非現実的です。その結果、安全情報システムには、コンピュータで簡単に処理できる要約統計データのみが含まれ、大きな損失が発生する前に事象から学習するために必要な傾向や経時変化に関する情報は含まれない場合があります。今日の航空会社は、大規模な自動情報収集のために、この種のデータ過負荷に特に苦しんでいます。

多くの安全情報システムのもう１つの欠点は、取り出しと伝播のメカニズムにあります。データと同じではない情報は、人々が学び、日常業務に適用し、システムライフサイクル全体で使用できる形式で提示されない場合があります。変更がタイムリーに行われない可能性があります：事故は、操作中の変化、またはエンジニアリングの更新時におけるハザード分析の不十分な変更が原因で発生してきました。情報は、ユーザーのニーズや認知スタイルに合わせるように調整されていないか、安全に関する決定が行われる環境に統合されていないため、使用が難しい場合があります。

安全情報システムは、提供された情報を使用して利益を得ることができる安全管理システム内にも存在する必要があります。安全情報システムに情報を保存するだけでは、企業がその恩恵を受けるために必要な構造とプロセスを持っているとは限りません。

事故調査を行う際には、安全情報システムや、事象へのどんな影響の可能性でも、検討する必要があります。損失を防ぐために必要な情報は、収集または保存されていたでしょうか？収集または分析プロセスで失われてしまったのでしょうか？利用可能であり、コントローラの日常の活動で簡単に取得できたのでしょうか？

安全管理システムの設計

安全管理システム（SMS）は、理論的にはCAST分析で使用される安全コントロールストラクチャーと同じです。一部の業界では、事故の防止に必要となる重要なコントロールを排除したSMSを定義しているため、ここでは「安全コントロールストラクチャー」という、より一般的な用語を使用します。

安全コントロールストラクチャーには、唯一の正しい設計というものはありません：従来とは異なる安全コントロールストラクチャーは、さまざまな方法で責任を分散する上で効果的です。業界と組織の文化は、実用的で効果的なものに影響を与えるでしょう。ただし、安全コントロールストラクチャーを有効にするために必要な一般的な設計原則がいくつかあり[19]、これらを使用して、事故後の組織の安全管理システムを評価できます。一般に、組織行動に必要な安全制約は、安全コントロールストラクチャーの設計に反映されるべきです：安全に対する責任、権限、および説明責任のコントローラへの割り当ては、ハザードや事故を防ぐのに十分でしょうか？割り当てる必要のある管理、開発、および運用の一般的な責任のリストは、付録Ｄに含まれています。

事故調査では、安全コントロールストラクチャーの公式な設計と、損失時の実際の動作を評価する必要があります。パフォーマンスやその他の種類の監査は、それが効果的に機能していることを確認するために使用されましたか？過去の軽微なインシデントは、何かが間違っているという手がかりである可能性があり、大きな損失の前に問題を特定するために使用されるべきでした。ニアミスおよびインシデント報告システムは、安全コントロールストラクチャーの操作の欠陥を特定するために使用されましたか？あるいは単に、オペレータに責任を割り当てるためだけに使用されたのでしょうか？

調査中に、どこを確かめるべきかについてのガイダンスを提供する手がかりが、利用可能になるでしょう。たとえば、シェル ムールダイクの公式な事故報告書は、シェルの安全管理システムについては記録、あるいは評価していませんが、次のことに言及しています：非安全な状況が見落とされた、内部手順が適切に守られなかった、過去のインシデン

[19] Leveson, Engineering a Safer World, 2012 および Leveson and Thomas, STPA HANDBOOK, 2018 の第7章（安全マネージメントシステム）

トから教訓を学ばなかった、基本的な化学反応についての誤った想定が誤っているという証拠が表面化した後でも、再評価されなかった、変更が管理およびコントロールされなかった、不適切なハザード分析およびリスク評価手順が使用された、過去のインシデントおよび事故からの推奨事項が実施されなかった、重要な活動の監視が欠落していた。これらの活動を実行および監督する責任は、割り当てられていたのですか？これらの種類の不適切な慣行を特定するために、どの種類の監査または検査が使用されましたか？なぜ事故前に特定され修正されなかったのですか？

企業の安全管理システム（SMS）の監視は、通常、政府または専門の規制の機関や組織の責任です。たとえば、シェル ムールダイクでは、オランダの規制当局は、会社に安全管理システムが導入されているかどうか、そのシステムに組み込まれているシステムと手順が適切かどうか、会社が実際にこれらのシステムと手順を適用しているかどうかを検査する責任があります。彼らは、シェルが自身のSMSに従って行動していないことに気づかなかったか、反応を示しませんでした。まさしくその例として、プラントの変更と改良は一貫してリスク分析の対象ではなく、このことはシェルのSMS要件に違反していましたが、この欠陥は規制当局によって指摘されず、かつ修正も要求されませんでした。変更は安全性について適切に評価されていませんでした。起動を実行するための専門知識とトレーニングの要件は強制されませんでした。

実際、規制当局はシェル ムールダイクのSMSに対する肯定的な評価に対して、全会一致でした。政府による検査と監督は、SMSの品質の審査により決定される部分もあるため、シェル ムールダイクの監視活動は限定されていました。オランダの規制当局は十分なリソースを持っていなかったため（よくある問題）、気が付いたリスクに基づいてリソースを割り当てました。彼らは「システム向けの監督」を実行するだけです。つまり、適切なシステムが整っている場合、当局はプラントでの実際の活動をそれ以上調べません。しかし、公式の事故報告書は、この種の限定的な監督の下でも、検査官は、プラントの変更と改良が一貫してリスク分析の対象ではなく、安全管理システムが実際にうまく機能していないことを観察することができたと述べています。

シェル ムールダイクの事故では、同じ触媒に関連する２つの過去のインシデントがありましたが、どちらもプラントの設計、実行されたリスク評価、または起動作業指示の作成について懸念や質問は生じていないようでした。インシデントに関する情報は、シェルによって効果的に保存されていなかった（したがって、安全情報システムの欠陥に起因する）かもしれませんが、単に会社の安全管理システムに運用上の欠陥があり、使用されなかった可能性の方が高いです。調査中に適切な質問をすることで、これらの問題の原因を特定できた可能性があります。

安全文化

受け入れ可能な安全情報システムと安全管理システムの構造は、どちらも安全文化の問題によって破壊される可能性があります。実際に、組織や業界の安全文化は、安全コントロールストラクチャーのすべてのコンポーネントの動作に影響を与えます。

「組織文化の父」と見なされているエドガー・シャインは、安全文化を「安全関連の決定を行うために使用される業界および/または組織の価値観と前提認識」と定義しました[20]。図19は、シャインによる組織文化（より具体的には、安全文化）の３つのレベルを示しています。

[20] Edgar Shein, *Organizational Culture and Leadership*, San Francisco: Jossey Bass, 2004

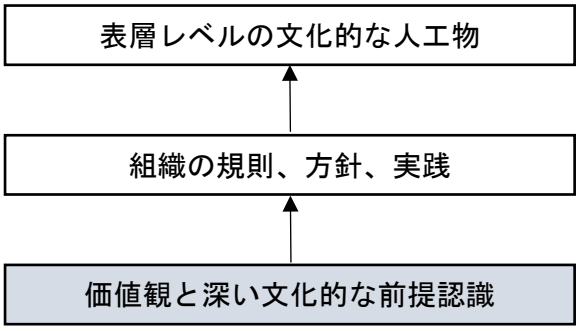


図 19：シャインの組織文化モデル

文化の本質は、組織または業界における意思決定と上位の文化的人工物の根底にある、最下層の価値観と深い文化的な前提認識です。中位層と上位層は文化ではありません。それらは単に組織文化を反映しているだけです。

安全文化は常にあります。重要な問題は、既存の安全文化が事故率にどのように影響するかです。事故を調査するときに、次のような安全文化の側面に目を向けるかもしれません：

- リスク受容の文化：この文化は、事故は避けられないものであり、すべての人に注意を促す以外に事故を防ぐためにできることは何もないという前提に基づいています。事故は生産性の代償と見なされます。多くの場合、この前提には、すべての人が自分自身と他の人の安全に責任を負うべきであり、事故は個人の責任ある行動の欠如に起因するという信念が伴います。誰もが責任を持って安全に行動すれば、事故は減る、あるいはなくなるという信念が普及しています。
- 否定の文化：否定の文化では、リスク評価は非現実的に貧弱で、信頼できるリスクと警告は適切な調査もなく却下されます：経営陣は良いニュースを聞きたいだけなので、まさにそれが伝えられます。焦点は、システムが非安全かもしれない状態を特定することではなく、システムが許容できるほど安全であることを示すことにあります。ハザード分析ではなく「安全ケース（safety cases）」の使用が一般的です。
- コンプライアンスの文化：ここでの焦点は、政府の規制を遵守することです。根底にある文化的信念は、規制を遵守することは許容できる結果につながるということです。規制当局は、最終製品またはサービスが安全であることの証明に重点を置く傾向があるため、開発中に設計に対して安全性を組み込むよりも、完成した設計または既存の設計の安全性の保証が強調されます。多くの場合、広範囲にわたる「安全ケース」の議論（arguments）が管理者または規制当局のために作成されますが、実際の製品または製品設計の取り組みには、ほとんどまたはまったく影響を与えません。さらに、安全対策の大部分が、組織の基本的価値である安全性の向上のための積極的に措置を講じることではなく、基準および規制当局の要求に準拠することを含む場合があります。従業員は、政府の検査官が不足していると判断したものをすぐに直したとしても、規制当局の指示を受けずに社内で積極的に問題を探したでしょうか？
- 文書業務の文化：この文化は、多くの書類と分析の文書を作成することが、安全な製品とサービスにつながるという信念に基づいています。大量な分析の文書が作成されますが、それらは設計と運用にほとんど影響を与えません。安全関連の文書業務の大部分は、製品の設計と運用、プロセスの実施、またはサービスの提供を行っている人々から独立しており、ほとんど相互作用のないグループによって作成される場合があります。文書はファイルに保存され、システムが安全であることをすべての人に保証します。

- 「威張る（Swagger）」文化：安全は弱虫のためのものです。本物の男性はリスクで成長します。もちろん、事故防止に関するここでの問題は明らかです。

どの組織の安全文化もトップマネジメントによって設定されています。経営陣による安全への誠実な決意は、安全を達成するための最も重要な要素として、しばしば言及されます。従業員が、仕事の安全性に合理的な懸念を示しており、スケジュールやコストなどの他の目的よりも安全性を優先している場合、彼らは支援されると感じる必要があります。多くの場合、安全性への懸念は単に口先だけのサービスとスローガンです。従業員は、空っぽな言葉からではなく、行動から手がかりをつかみます。

事故調査中の安全文化の分析は、会社の文書化された安全哲学と安全方針の評価から始める必要があります。これらが存在しない場合は、明らかに問題があります。医療機器に重大な安全上の問題が見つかった後、私はその会社に、参加して何が起こったのか調査するように頼まれました。私は以前に彼らに書面による安全方針が必要であると話していましたが、彼らは決して作成しませんでした。製品の安全性に問題があった後、その理由を尋ねたところ、設計・販売している機器がセーフティクリティカルであることは、従業員にとって明らかなので、方針は不要であると言われました。その一方で、他の製品プロパティに関する多くの書面による方針と規則はありました。さらに、彼らの弁護士が、製品が潜在的に危険であると認めることになるので、安全方針を作成しないように彼らに忠告したと言いました。製品の危険性は明らかであり、安全方針が無いからといって、製品に関して危険がないとだまして思い込ませることは、誰に対してもできなかったでしょう。それは単に会社を怠慢に見せただけでした。私が相談にのった有害事象の直後、会社は倒産し、存在が無くなりました。

安全哲学は、経営者が安全と他の組織の目的との間に望んでいる関係についての短い書面による声明です。安全哲学の声明の一部になりうる一般原則の例をいくつか示します:

1. すべての傷害や事故は予防可能です。
2. 安全性と生産性は密接に関係しています。安全管理の改善は、他の品質およびパフォーマンス要因の改善につながります。最大の業績には安全性が必要です。
3. 安全性は、製品またはサービスの設計に組み込まれている必要があります。後で追加すると、効果が低下し、コストが高くなります。事後保証は、安全性がまだ存在しない安全な設計を保証することはできません。事後に安全を確保しようとするよりも、安全を組み込む方が良いです。
4. 事故/インシデントの因果関係分析の目的は、責任を負う誰かや何かを見つけるのではなく、適切な変更を加えることができるように、損失（またはほぼ損失）が発生した理由を特定することです。
5. インシデントと事故は、安全に動作していないシステムを知るための重要な窓であり、包括的な原因分析と改善アクションのきっかけにする必要があります。
6. 安全情報は、恐れることなく表面化されなければなりません。安全分析は、非難することなく実施されます。
7. 安全への決意、オープン性、誠実さは、組織内で評価され、報酬を与えられます。
8. 効果的なコミュニケーションと情報の共有は、損失を防ぐために不可欠です。

これらの原則は一見単純に見えますが、実際には作成するにはかなりの考慮が必要であり、多くの場合、企業の意思決定を実際に導く原則ではありません。それらの背後にある詳細な説明は、STPA HANDBOOKの第７章にあります。

安全哲学は、より広範な安全方針と基準を構築および評価するための原則を確立し、従業員が安全関連の決定を下し、行動することを、経営陣がどのように望んでいるかについての簡潔な声明を提供します。

もちろん、単に哲学を書面で持っているからといって、経営陣や他の従業員から賛同を得ているわけではありません。マネージャーは実際に彼らの日常業務で哲学を実行していますか？哲学が採用され、原則が実践されていることを確認するためのプロセスはありますか？原則はどのように従業員に伝えられますか？安全哲学の書面による声明とより詳細な方針声明および基準は始まりですが、それだけでは十分ではありません。従業員は、書面による方針が実際の経営者の行動と異なる場合は、すばやく見分けます。従業員は、組織のトップの人々が安全に真摯に取り組んでおり、単にスローガンを立てて動いているだけではないと信じていますか？安全文化の欠如が事故の原因となっている場合には、いくつかの簡単な質問をすることで見分けることができます。

事故調査では、精巧な従業員調査を利用して既存の安全文化を理解することがありますが、私はそれが有用であるとは思いません。調査で彼らが言うべきだと思うことや信じるべきことを書き留めることは、彼らが実際にそのように考えたり行動したりすることを意味するものではありません。実際の行動を観察する方が、はるかに啓発的であることが分かります。安全文化は、経営陣と従業員の行動を直接研究することによって最もよく評価されます。人々がどのように行動するかは、調査で答えるよりも、内部の価値観のより良い指標です。

決意はどのように示されるでしょうか？それは、次のことによって示されます；優先順位を設定し、それに従うこと；主体的に関与すること（例えば、安全性の決定を行うトップマネジメントの議長グループが関与する、または少なくとも個人が関与する）;適切な組織構造を設定すること；選定された高位のリーダーを安全関連の責任に任命し、彼らが効果を発揮するための適切なリソースを提供すること；最高の従業員を安全関連の活動に割り当て、彼らの努力に対して報いること；その他の人の自発性に応えること。決意はまた、非難することを最小限に抑えることによっても伝えられます。リーダーは、インシデントや事故が発生したときに、責任を負わせる人（通常は組織の最下位レベルの人）を見つけるだけではなく、損失につながる体系的な要因を修正することが最優先事項であることを示し、先に進む必要があります。最後に、組織内のインセンティブ構造は、望ましい行動を奨励するように設計する必要があります。繰り返しになりますが、事故調査中にこれらの要因についていくつか質問することで、事象に対する安全文化の貢献についての洞察を得ることができます。経営陣は、昇進や昇給について決定を下す際の重要な基準として安全性を使用するのに十分なだけ、それを重視しているでしょうか？

経時変化とダイナミクス：システム内と環境内

事故は通常、ある種の変化の後に発生します。変化は、物理的プロセス、操作手順、個々の行動、安全活動またはプロセス、管理プロセス、監視慣行（内部および外部の両方）、またはシステムが存在し、システムが相互作用しなければならない環境の中にある可能性があります。

変化は計画的なことも計画外のこともあります。どちらのタイプの変化もコントロールする必要があり、そうでない場合は事故につながる可能性があります。

変化が計画されている場合は、施行され遵守された変更方針の、強力で適切に設計された管理を実施する必要があります。多くの事故では、変更管理（MOC）手順が存在していましたが、それらは効果的でも強制的でもありませんでした。 シェル ムールダイク爆発の例では、テストせずに新しい触媒に切り替え、以前の触媒特性がまだ保持されていると想定したり、ユニット4800の作業指示の一部を（ここでも評価なしで）重要と見なされなかったために削除したりしました。作業指示の定期的な更新において、その内容を不可欠

と思われる情報に限定し、安全性と運用の観点から、最も重要であると誤って考えられたものに焦点を当てようとした試みの中で、窒素流量に関する重要な要件は削除されました。時間の経過とともに、ユニット4800に関連する最も適切な手順への理解が変化したため、焦点を当てたもの以外の情報は作業指示から除外されました。

リスクに影響を与える変化は、計画外の場合もあります。安全性に影響を与える計画外の変化を検出し、その発生を防ぐ方法が必要です。検出は、先行指標と安全性に焦点を当てた監査を使用して行うことができます。また、当初の安全に関する設計機能と管理手順の基礎となる想定に対して、定期的に計画された再評価を行うこともできます。シェルムールダイクでは、先行指標（漏出数など）は不十分で範囲が狭すぎ、監査は効果的とは考えられず、1977年に確立されたエチルベンゼンの特性に関する想定が再検討されることはありませんでした。

シェル ムールダイクでユニット4800の作業指示書を使用して行われたように、変化は時間の経過とともにゆっくりと発生する可能性があります。作業指示書は各定期補修工事の前に修正されたため、重要な情報が除外されました。例としては、上記の窒素流量の要件や反応器に必要な加熱速度などがあります。変化は専門家によってレビューされたようには見えませんが、もしレビューされていた場合には、レビュープロセスに欠陥があったということです。

変化は、あるシステムコンポーネントでは、既知であり、計画されているかもしれませんが、システムの別のコンポーネントでは、計画外で、未知の変化として現れることがあります。触媒の組成における変化は、触媒の製造業者には知られていましたが、シェルムールダイクには知られていませんでした。ここでは明らかに、コミュニケーションが重要な要因です。

先行指標は、システムがより高リスクの状態に移行していることを見極めるために、一部の業界で一般的に使用されています。シェル ムールダイクやほとんどの化学プラントでは、使用される先行指標が業界全体で共通している可能性があります。この場合は漏出数です。彼らの選択は、主に収集の容易さと、より効果的なものを作成するための代替手段がないことに基づいているようです。

私は「想定に基づく先行指標」と呼ばれる先行指標を特定するための新しいアプローチを作成しました[21]。簡単に言うと、システムの開発中には、システムへの安全を設計するために使用される特定の想定が作られているという考え方です。時間の経過とともに、これらの想定が成り立たなくなると、組織はよりリスクの高い状態に移行する可能性があります。したがって、当初の安全に関する想定を運用中に検査して、それらがまだ真実であることを確認することによって、先行指標を識別できます。システムは常に変化し、時間とともに進化します。システムが動作する環境も同様です。変化は必要かつ不可避であるため、安全性が低下しないようにプロセスを作成する必要があります。先行指標へのこの新しいアプローチは、MITの博士号を取得したディオゴ・カスティーリョによって評価されています。[22]

変化は時間の経過とともにゆっくりと進行することがあり、その影響は明らかではない可能性があります。バーミンガム空港着陸時の貨物機の墜落に関するCAST分析では、安全コントロールストラクチャー全体の運用が不適切であった要因の１つは、空港での夜間の貨物運用の増加でした。貨物機の安全性は、旅客機と同じくらい重要と考えられているでしょうか。疲労で複雑になる可能性のある早朝の暗闇での運用よりも、日中の運用の方

[21] Nancy Leveson, (2015), A systems approach to risk management through leading safety indicators, *Reliability Engineering and System Safety*, 136: 17-34, April.

[22] Diogo Silva Castilho, *A Systems-Based Model and Processes for Integrated Safety Management Systems*, Ph.D. Dissertation, Aeronautics and Astronautics, MIT, expected September 2019.

が、懸念が示されているのでしょうか？航空会社の運用と輸送量の変化に照らして、空港の運用に関する過去における想定を再検討する必要があるかもしれないことが分かりました。

非公式な（公式のものでさえ）リスク評価は、損失がなければ、時間の経過とともに変化する可能性があります。実際のリスクはおそらく減少していませんが、私たちが認識するリスクは減少しています。これが、相反する目的の優先順位と決断に対して、変化をもたらします。実際に、スペースシャトルの損失は、特にコロンビア号の事故は、この方法で部分的に説明することができます。事故の防止に成功すると、逆説的にリスクを高める行動や意思決定が実際にはもたらされるという奇妙なダイナミクスが、残念ながら発生することがあります。安全への取り組みが成功すると循環ダイナミクスが発生します。事故は起こらないという感覚が高まり、安全への取り組みが減り、事故が発生すると、システムは危険な状態に戻り、再び自己満足が高まるまでのしばらくの間、コントロールが強化されます。

自己満足の要因は非常に一般的であるため、安全コントロールストラクチャーにはそれに対処する方法を含める必要があります。米国の原子力潜水艦の安全プログラムであるSUBSAFEは、この傾向との戦いに重点を置いており、この目的の達成において特に成功しています。高リスクな状態への移行を特定することが、事故調査の重要な部分です。非現実的なリスク認識が関与する事故原因の分析中にこの移行の理由を理解することは、その移行を防止するため、または発生時に検出するために、安全コントロールストラクチャーを設計する方法を特定するのに役立ちます。

この安全性の低下に対抗する方法の一つは、システムコントローラのプロセスモデルにおいて、正確なリスク評価を維持する方法を提供することです。コントローラがよりよい情報を持てば、プロセスモデルがより正確になり、それにより、意思決定も正確になります。事故分析には、安全をコントロールしている人々のメンタルモデルにおける、リスク認識の正確さについての注意深い調査が含まれるべきです。

内外の経済的要因および関連要因

事故の原因となる体系的な要因には、多くの場合、外部市場の競争や利益の減少など、内部と外部の両方の経済状況が関係しています。市況は、経営陣が安全マージンを減らし、確立された安全の習慣を無視することにつながる可能性があります。通常、これらの変化に関連するリスクの増大を示す前兆がありますが、この前兆が認識されないことが多すぎます。

もう１つの一般的な要因は、人と危険なプロセスとの間の物理的な距離が近くなっていることです。危険な施設は通常、もともと人口密集地から遠く離れた場所に配置されていますが、施設が作成された後、住民は移動します。人々は仕事場の近くに住みたいと思っており、長い通勤は好きではありません。臭く、汚染されたプラントの近くでは、おそらく土地と住宅は安いでしょう。ボパールの場合のように、第三世界の国々においては、重工業プラントの近くでは、電力や水などの公共設備や輸送を、より簡単に利用できるかもしれません。仕事と経済発展を提供するという誘惑により、政府当局者はリスクを軽視し、安全管理と緊急対応の要件を厳格に実施しなくなる可能性があります。

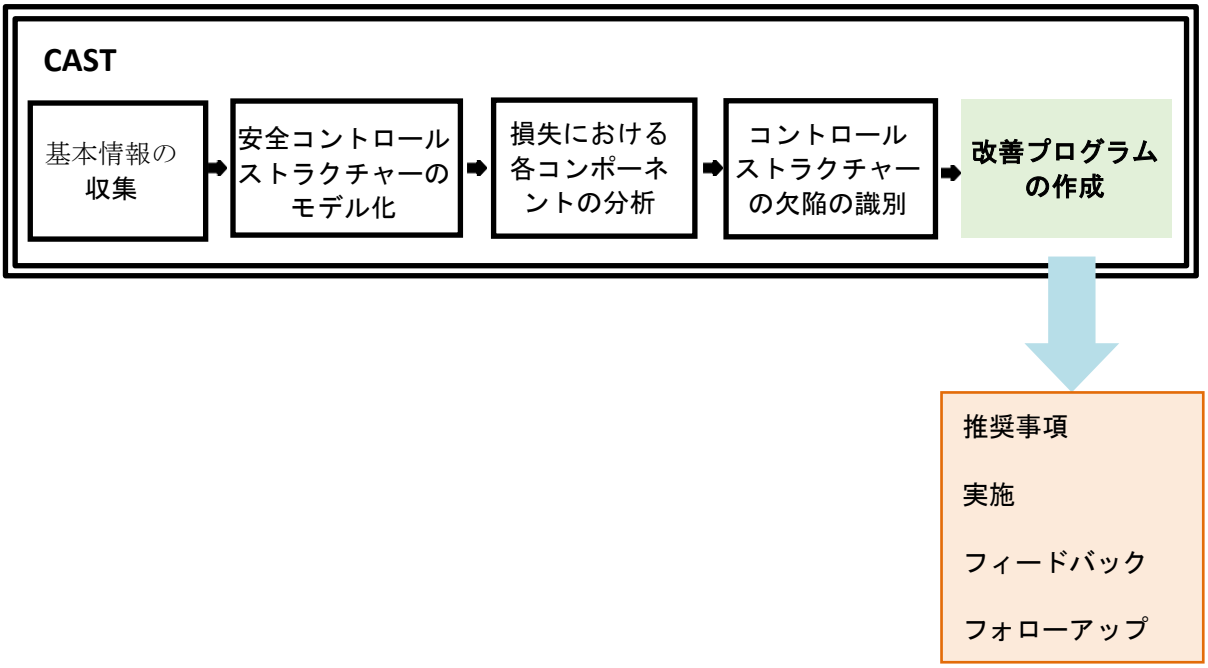
2005年に爆発したISOMタワーの隣に、従業員事務所を収容するトレーラーが建設されたテキサスシティ製油所で起きたように、時間の経過とともに、建設可能な土地としては、プラントの危険地帯の近くしか利用できなくなるでしょう。人口の増加に伴い、消防および医療資源のような地方の緊急設備は、資源やその他の相反する優先事項による制約により、増加する要件に遅れをとる可能性があります。

これらの要因は、個々のコントローラの分析でこれまでカバーされていなかったシステム環境、またはその他の普遍的な体系的要因、特に時間の経過に伴う変化やダイナミク

スに関連している可能性があります。個々のコントローラの動作は、これらの要因によってどのように影響を受けましたか？明らかな要因は、財政的および競争上の懸念、ならびに新製品および市場です。自明ではない要因としては、疲労とデューティサイクル、契約交渉による動揺、さまざまな要因による従業員の士気の低下、生産性向上に対する合理的水準を超えたプレッシャーなどがあります。

プロセスが自動化され、人間が実施している標準の安全コントロールが、自動化されたプロセスには実装されていない場合があります。ソフトウェアは「故障」しないため常に安全である、またはコンピュータは人間よりも信頼できるため安全性が高まる、といった単純な信念がよくあります。残念ながら、自動化されたシステムを導入すると、システムには他の変更が導入されます。多くの場合、以前は存在していなかった変更です。自己満足が高まり、既存の安全コントロールストラクチャーではコントロールできない新たな事故原因が発生します。

安全コントロールストラクチャーに対する推奨事項と変更の生成



5. *将来の同様の損失を防ぐために、コントロールストラクチャーの変更に関する推奨事項を作成します。必要に応じて、全体的なリスク管理プログラムの一環として、このハザードの継続的な改善プログラムを設計します。*

推奨事項の生成

分析の他のパートが完了したら、推奨事項の生成は簡単です。私たちが耳にするCASTについての最大の不満は、それがあまりにも多くの推奨事項を生成するということです。この不満は、事故調査の目的が、推奨事項をできるだけ少なくすることである場合にのみ正当化されます。事故調査は、長年、「根本原因」または「推定原因」を特定することを目的としてきているため、より多くの推奨事項を生成するより多くの原因要因を調べ始めることはカルチャーショックかもしれません。

多数の推奨事項を含めることに対して提起される反対意見の１つは、それらへの対応には圧倒されるということです。これは単なるロジスティクスの問題であり、各事故から学ぶことを少なくすることで解決すべき問題ではありません。指定された基準に従って推奨事項に優先順位を付けることができない理由はありません。また、すべての推奨事項をすぐに実施しなければならないということでもありません。推奨事項によっては、比較的簡単にすぐに実施できるものがありますが、もっと時間がかかる推奨事項もあります。実施するのに多大な労力とリソースを要するような大規模な変更を必要とする推奨事項があるかもしれません。後者の例には、新しい監督機関の設立や規制や法律の変更が含まれます。実施の難しさは、事故報告書から推奨事項を除外する言い訳にはなりませんが、それを即時の修正ではなく、より長期的な目的として分類するのには、十分な理由になるかもしれません。

「一時しのぎの（jury-rig）」短期的な解決策を講じることは、包括的で効果的な解

決策を際限なく遅らせる言い訳にはなりません。

継続的改善のためのストラクチャーの確立

推奨事項が作成されても、実施されない場合があります。推奨事項を確実に遵守するための方法が必要というだけではなく、目的の達成と安全コントロールストラクチャー強化の観点から推奨事項が効果的であることを確実にするためのフィードバックも必要です。

基本的に３つの要件があります:

1. 推奨事項を実施する責任を割り当てる
2. 推奨事項が実施されていることを検査する
3. 推奨事項が、コントロールの強化に効果的かどうかを判断するためのフィードバックシステムを確立する。

３番目の要件は、推奨された変更の有効性に関する証拠を収集する必要があることを意味します。このようなフィードバックは、監査と検査、および先の推奨事項が成功したかどうかを判断するためのその後のインシデントの分析から得られます。このような活動は、安全管理システムの重要な要素ですが、省略されることがよくあります。

後に起きた事故や損失は、特にCASTを使用して分析した場合、先の推奨事項が効果的ではなかった理由と、他に何が必要かを理解するための豊富な情報源を提供します。元の原因分析に欠陥があったのでしょうか？特定の改善の潜在的な有効性に関する想定が正しくなかったのでしょうか？安全コントロールストラクチャーを強化する試みを妨げる他の変更が発生したのでしょうか？計画された変更が予期しない結果をもたらしたのでしょうか？

ここでの目的は、組織がリスク管理の取り組みを継続的に学習および改善することを確実にし、時間の経過とともに損失の可能性が減少することです。

CASTの結果を形式化するための提案

STAMPでは、損失には、単純な事象連鎖や事象連鎖の組み合わせだけでなく、複雑なプロセスが含まれます。事象と原因要因の間の相互作用は、多くの場合、複雑で捕えにくい、または間接的です。結局、それらを別々の要因としてリストすることは実行不可能かもしれませんが、それらの間の関係を理解することだけは可能です。結果として、CASTの結果を表示するための形式は、単純なリストではなく、さまざまな原因要因間の関係を強調する必要がありますが、リストを避けるのが難しいことがよくあります。

CAST分析の結果を保存および整理するためのツールは、さまざまな要因と動作の関係、およびCAST分析全体で生成された質問への回答の場所を示すハイパーリンクを広範囲に使用することで簡単に作成できます。ただし、より難しいのは、CASTの結果を表示するための満足のいく標準表記を考え出すことです。

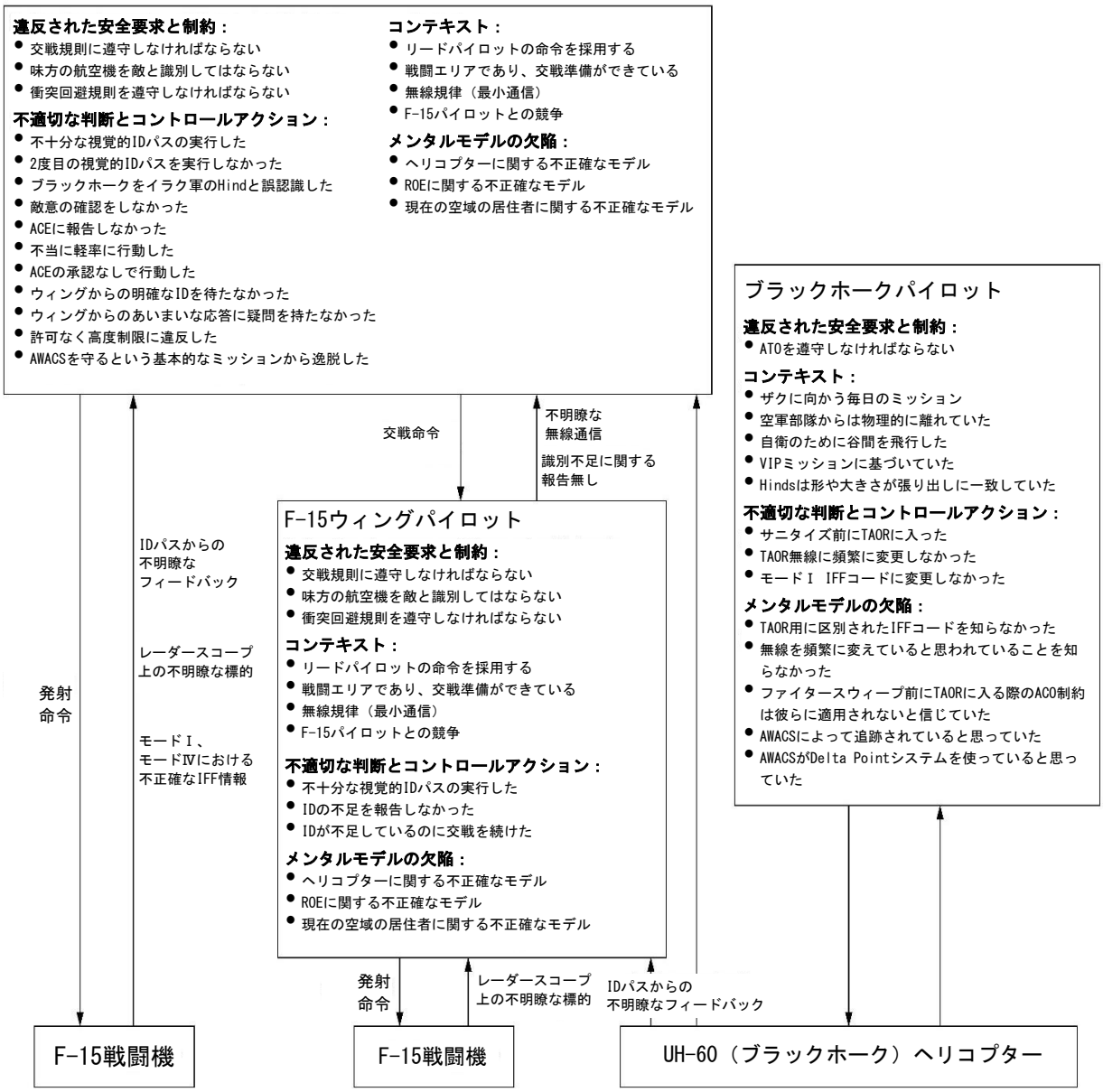
もちろん、目的は、関係するすべての原因要因と、それらすべてが互いにどのように関連しているかを読み手に理解してもらうことです。さまざまな表記法がそれぞれ異なる事故分析において利点を持っており、すべての事故分析に最適な表記法はありません。

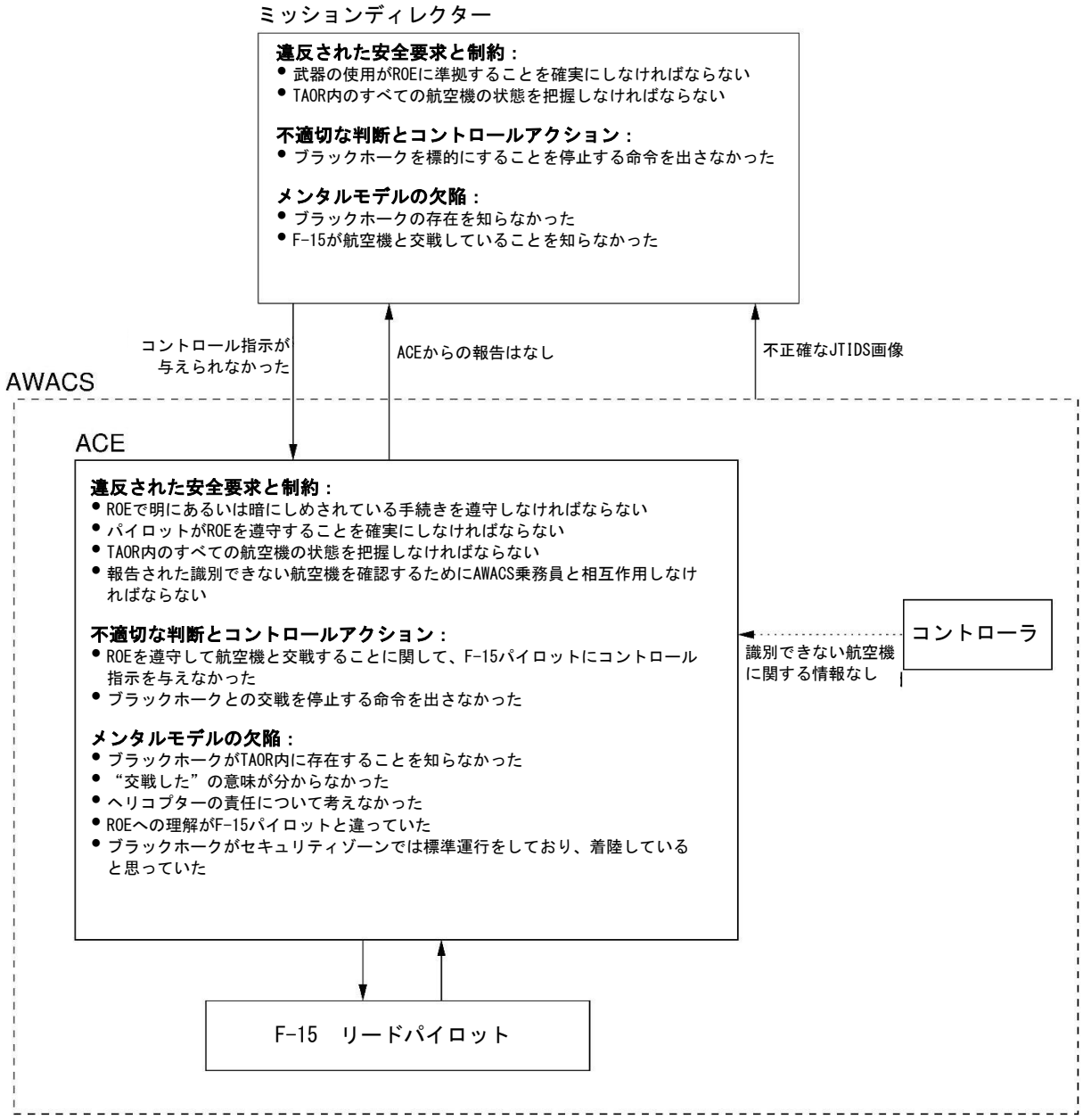
その結果、分析のすべての詳細の文書化において、さまざまな種類の表記法を使用できますが、事故原因の最終的な要約では、読みやすさと分かりやすさが重要です。すべての詳細が必要なわけではないかもしれませんが、重要な結論と議論を提示する方法が必要です。 （AcciMap分析のように）これをすべて１ページに収めようとすると、重要な情報が単純化されすぎて省略されます。一方、情報をあまりにも多くのページに分散させると、情報過多になり、全体像が失われる可能性があります。ここでは、私が使用した例だけをいくつか紹介し、他の人がより良いアイデアを思い付くようにします。

シェル ムールダイクの事故では、付録Ｂに示すように、色付きの安全コントロールストラクチャーを使用しました。これに付随させた表では、コンポーネントの要約分析へのリンクを色で表しています。

別の方法として、最も重要な要約情報をコントロールストラクチャー自体に挿入したことがあります。米国のF-15が米国のブラックホークヘリコプターを飛行禁止空域上空で撃墜したfriendly fire事故について、私が分析したものから図をいくつか示します。１つ目は、パイロット、つまりF-15リードパイロット、F-15ウィングパイロット、ブラックホークパイロットの分析を示しています。２つ目は、その地域の交通を指揮していたAWACS航空機のACE（空中コマンドエレメント）のディレクターの分析を示しています。ミッションディレクターは現場にいて、ACEの活動を監督していました。３番目の図は、AWACS乗組員の分析を示しています。これらの図はそれぞれ、実際のCAST分析レポートに付随するテキストとともにさらに詳細に説明されています。ただし、この表記により、分析の概要を把握できます。完全なCASTレポートにある追加のテキストは、重要ではあるがより詳細な情報を提供する必要があります。

F-15リードパイロット




ミッションディレクター
違反された安全要求と制約：
● 武器の使用がROEに準拠することを確実にしなければならない
● TAOR内のすべての航空機の状態を把握しなければならない
不適切な判断とコントロールアクション：
● ブラックホークを標的にすることを停止する命令を出さなかった
メンタルモデルの欠陥：
● ブラックホークの存在を知らなかった
● F-15が航空機と交戦していることを知らなかった
コントロール指示が
与えられなかった
ACEからの報告はなし
不正確なJTIDS画像
AWACS
ACE
違反された安全要求と制約：
● ROEで明にあるいは暗にしめされている手続きを遵守しなければならない
● パイロットがROEを遵守することを確実にしなければならない
● TAOR内のすべての航空機の状態を把握しなければならない
● 報告された識別できない航空機を確認するためにAWACS乗務員と相互作用しなければならない
不適切な判断とコントロールアクション：
● ROEを遵守して航空機と交戦することに関して、F-15パイロットにコントロール指示を与えなかった
● ブラックホークとの交戦を停止する命令を出さなかった
メンタルモデルの欠陥：
● ブラックホークがTAOR内に存在することを知らなかった
● “交戦した”の意味が分からなかった
● ヘリコプターの責任について考えなかった
● ROEへの理解がF-15パイロットと違っていた
● ブラックホークがセキュリティゾーンでは標準運行をしており、着陸していると思っていた
コントローラ
識別できない航空機
に関する情報なし
F-15　リードパイロット

AWACSミッション乗務員

違反された安全要求と制約：
- TAOR内のすべての航空機を識別し、追跡しなければならない
- 味方の航空機を敵と誤認してはならない
- 問い合わせがきたら、すべての航空機の状態を戦闘機に正確に知らせなければならない
- フローシートにどの航空機も現れていなかったら、戦闘機に警告しなければならない
- 戦闘機が味方の航空機を標的にしていたら、警告を失敗してはならない
- 空域とその居住者の正確な図面による領域を提供しなければならない（JTIDSを介して）

機能不全の相互作用：
- 航空機のコントロールが、エンルートからTAORコントローラに引き渡されなかった
- レーダースコープ上のヘリコプターの飛行追跡に関する、ASOとシニアWDの間の相互作用

不適切な判断とコントロールアクション：
- エンルートコントローラは、ブラックホークパイロットにTAORに頻繁に変更するように伝えなかった
- エンルートコントローラは、ブラックホークのコントロールをTAORコントローラに引き渡さなかった
- エンルートコントローラは、ブラックホークがTAOR内にいる際に、航路を監視しなかった
- エンルートコントローラは、ブラックホークの飛行計画の決定に、Deltaポイントシステムを使わなかった
- TAORコントローラは、TAOR内のヘリコプターの航路を監視しなかった
- 標的にしているヘリコプターが味方であることを、発射する前に、だれもF-15パイロットに警告しなかった
- 味方の航空機がその領域にいることを、だれもパイロットに警告しなかった
- 交戦を停止しようとしなかった
- 誤ったIFFコードをスコークしていることを、だれもブラックホークパイロットに伝えなかった
- 午前の指示において、MCCは、ヘリコプターに関するATOには無い情報を取り次がなかった
- シャドウ乗務員は、活動を監視していなかった

調整における欠陥：
- だれがヘリコプターを追跡するかについての混乱
- 監視と兵器のディレクターの責任についての混乱
- NFZにおけるヘリコプターの通行監視の責任は、だれにも割り当てられていなかった
- 交戦を開始する権限をだれが持っているかについての混乱

コンテキスト：
- 最小通信
- 不十分な士気、不十分な訓練、過度な労働
- 事故時の粗末な活動
- 端末故障により座席の配置が変更された
- 空域侵犯はまれであった

メンタルモデルの欠陥：
- OPCの空中作戦において、ヘリコプターが必須の部分であると思っていなかった
- 空域の居住者と彼らがどこにいるかについての不正確なモデル
- ヘリコプターはザクに向かっているとしか考えていなかった



多くの場合、体系的な要因は図によって効果的に説明できます。事故でのコミュニケーションの喪失は、２つの図（図16、図17）を使用して示されました。１つには、設計されたコミュニケーションリンクが示され、もう１つには、事故時に実際に動作可能だったリンクが示されました。レキシントンでのコムエアーの墜落について、フィードバックの欠落と欠陥が図18に示されています。図は、コントロールストラクチャーで時間の経過に伴う重要な変化を示す効果的な方法です。図20は、カナダのウォーカートンの水道の大腸菌汚染に関与する、当初の設計されたコントロールストラクチャーを示しています。ここでは詳細は重要ではありません。図21に事故当時のコントロールストラクチャーを示します。図21のグレー表示されたストラクチャーは、時間の経過とともにコントロールストラクチャーの中で削除された部分を示し、青いストラクチャーは追加を示しています。

システムハザード：公衆が水を飲むことによって、大腸菌、または衛生にかかわる汚染菌にさらされる
システム安全制約：安全コントロールストラクチャーは、公衆が汚染された水にさらされることを防がなければならない。
(1) 水質を危険にさらしてはならない
(2) 水質が危険にさらされたならば、公衆衛生の方策により暴露のリスクを下げなければならない（たとえば、告示や遵守すべき手続き）

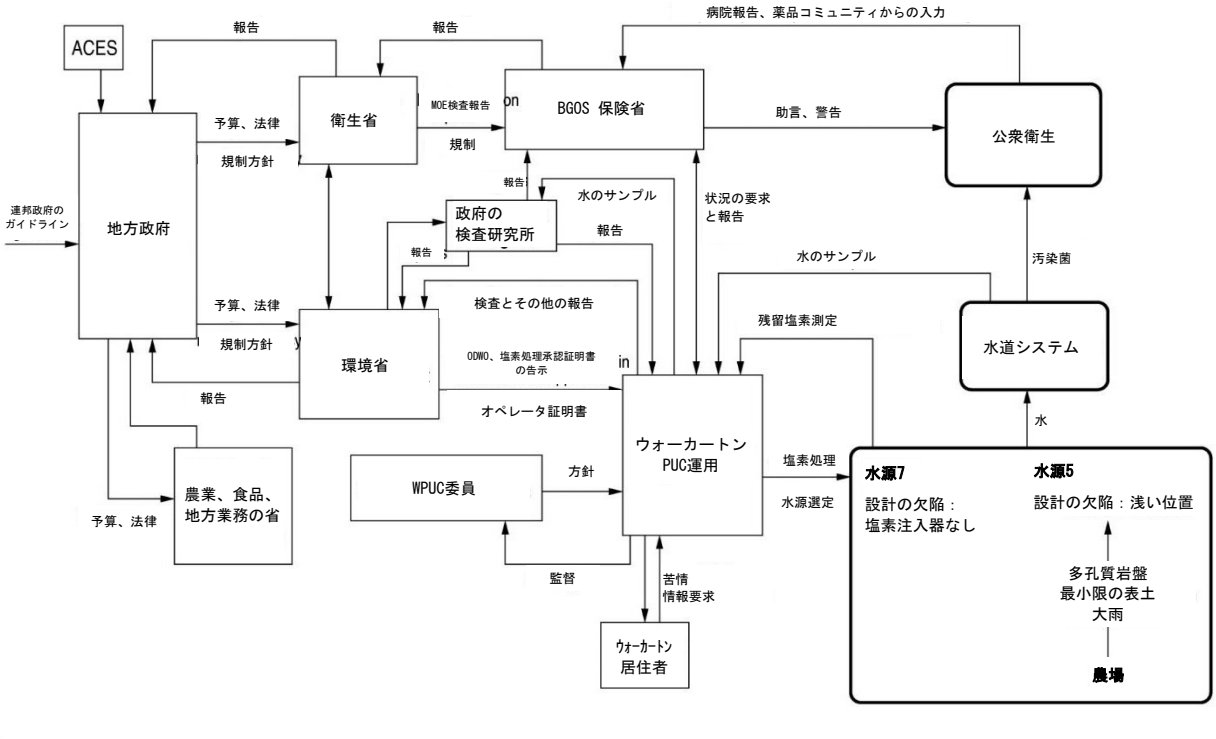


図 20：カナダ オンタリオにおいて水質をコントロールするために当初デザインされていたコントロールストラクチャー

この水質汚染事故では、保守的な政府が選出されており、政府の水質検査の研究所を民営化することを決定しました。民間の研究所が、水質検査の結果について政府に通知することが必要とされていたならば、この変更は問題なかったでしょう。しかし、形式的な手続きと見られるものや民間企業による過剰な報告を減らすための取り組みがなされため、民間の研究所は、ウォーカートンの給水業務を監督している、水が大腸菌で汚染されている可能性があることを理解していないオペレータに、直接結果を報告しただけでした。図21は、環境省によるウォーカートン運用の活動についてのすべてのフィードバックが、失われた結果を示しています。コントロールストラクチャーの消えた部分を隠すことで、問題が明確に示されます。保健省であれば問題を発見できたかもしれませんが、彼らは環境省が監視を提供していると想定し、介入しませんでした。コントロールストラクチャーの青い部分は、時間の経過に伴う追加を示しています。他の事故と同様に、説明は非常に複雑です。一つには、オペレータ認定が制定されていたにもかかわらず（ウォーカートンのオペレータには追加の教育が必要とされていました）、彼らは新しい教育と認定の要件から適用除外されていました。

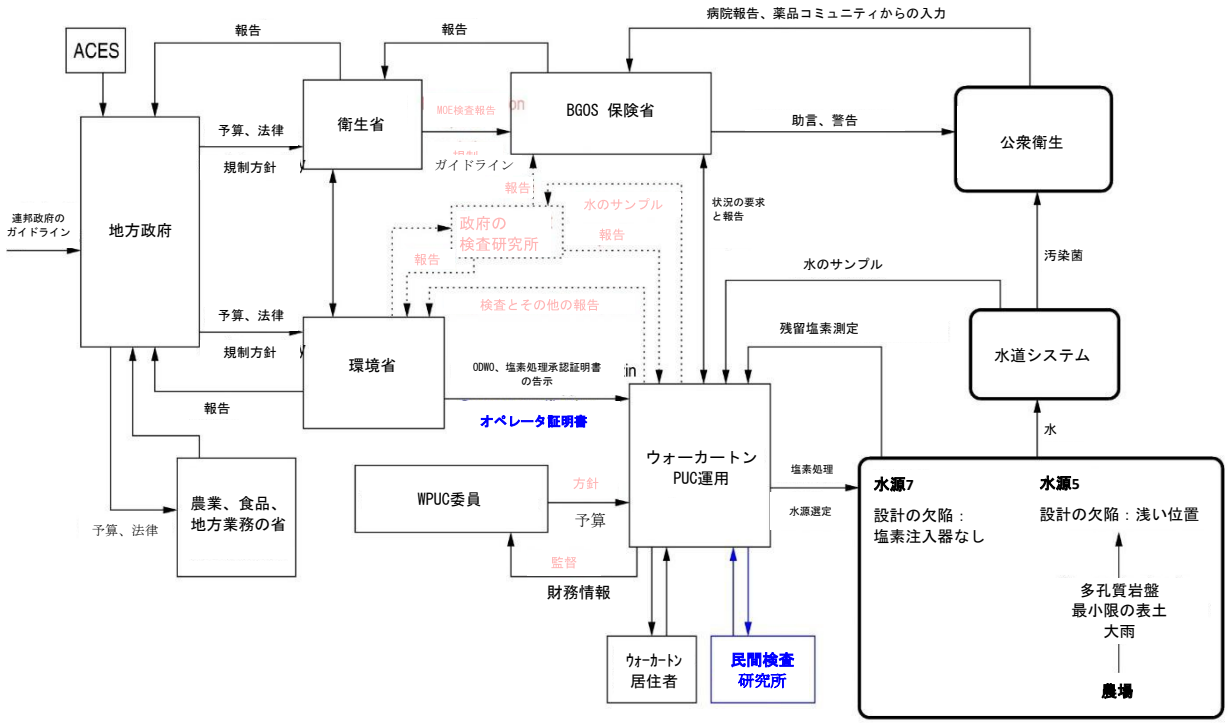


図 21：水質汚染事象の際のコントロールストラクチャー

第５章：職場と社会的な事故におけるCASTの利用

ここまでのハンドブックの例には、伝統的な工学的システムに加えて、それらをサポートする社会システムが含まれています。しかし、CASTは、あまり伝統的ではない用途で使用することができます。本章では、例として、職場の安全と、ハザードが主に社会システムに関係している状況での使用例を示します。

職場の安全

この章の例が示すように、職場での安全で利用されるCASTの方法は、他の種類のシステムと比べて違いはありません。この例は、実際の事故のものですが、重大ではない詳細は、機密保持のために省略されています。このハンドブックの他の例とは異なり、この事象の公の調査はありませんでした。

この事故は、巨大な製品を組み立てる製造工場で発生しました。ある部品が、あるべき時にまだ準備ができておらず、後から組み立てプロセスにおいて組み込む必要がありました。その目的を達成するため、新しい部品が入るように、その製品の構造物の一部を解体しなければなりませんでした。その解体作業には足場が必要で、最初の第１シフトで、その足場を設置しました。続く第２シフトで、４人のチームが事前タスク分析を行い、新しい部品を挿入するスペースを確保するために、構造物の一部を取り除く計画を考案しました。

この計画を実施する際に、外部構造物の除去を足場が邪魔しているため、製品を分解できないことがすぐに分かりました。４人のチームは、必要な場所を作るために、足場の中央の板の一部を取り除くことを決めました。

チームは、この構造物を解体して、足場の反対側の端に位置していたシザーリフトに向かって移動し始めました。構造物の部品を動かしているときに、整備士が足場の穴から落ちて肋骨を複数本折る重傷を負いました。

社内で実施した標準労働災害分析では、この事故調査チームが作成したレポートから、直接、以下の結論を導きました。

直接的な原因：従業員が高所から落ちました

寄与原因：

- 本作業の実施経験の欠如（通常の活動順序どおりではありません）。
- 作業者は、この種の仕事に利用できる職場の支援があることを知りませんでした。
- チームは、この仕事を実施する際に通常的に起こるリスクを認識しておらず、支援を求めることもしませんでした。

根本原因：足場からの床板の除去

短期的な是正措置（推奨事項）：

- 床板は足場から取り外すことができないことを知らせるアラートを作る。すなわち、作業者に、足場から床板を取り外さないことは非常に重要であると命令します。
- 工場内にある全ての床板が固定されていることを確認します。［CAST分析においては、床板を固定しないことには、安全上の理由があることが分かります。］

長期的な是正措置：

- 順序どおりではない作業のために、作業指示にツールの情報を追加します。

- この事例と他の事例を使い、許容できるリスクのレベルを再設定します。［*これは何を意味しているのでしょうか?*］
- 日々の作業者のキックオフミーティングにおいて、その日に割り当てられたタスクのために、潜在的なハザードについて議論し、安全作業の実施を確認します。一般的な安全上の話題からは離れます。［足場から床板を取り外してはいけないと作業者に伝えることを、後知恵バイアスだけで誰かが考えたと思われます。間違って行

この調査では、分析は、以下のような質問と回答のレベルでした。

質問：「従業員は何を間違ったのでしょうか？」回答：「隙間の穴に踏み込んでしまいました」

質問：「原因は何でしょうか？」回答：「状況認識の欠如でした。ミスをしました」

誤解を招く名前をつけた単なるフォールトツリーのように見える、現実チャート（Reality Chart）と呼ばれるものを使って、この例では原因を導出していました。客観的な「現実（reality）」のようなものはなく、個々の人が見ている現実しか存在しません。これは、その活動における個々の観察者や参加者によって大抵異なっています。このような「現実」は分析を行っている人の推測や偏見によってバイアスされるかもしれません。また不完全である場合もあります。何かを「現実」としてラベル付けすることは、単に誤った方向に導いてしまう販売ツールです。

この場合、「状況認識の欠如（lack of situation awareness）」は技術用語であり、「踏み込んだ時に、その人は、そこに穴があるとは知らなかった」という意味です。これは、かなり自明なことであり、そして、役立ちません。誰が、故意に、そのような穴に踏み込むでしょうか？ これはまた、おそらく誤っています。作業員は、その穴については知っていました。ですから、なぜそれでも踏み込んでしまったのかが分かりません。１つの推測としては、大きな構造部品が、別々のセクションを保持する４人によって動かされていたということです。その作業者は、他の作業者が部品を移動したことにより、穴に踏みこまざるを得なくなり、落ちてしまったのかもしれません。なお、この場合、その穴になぜ作業者が踏み込んだのかについて更に知っていても、事故を防ぐためのガイダンスを示してはいないことに注意してください。２番目の理由、「ミスをしました」は、もっと有益ではありません。

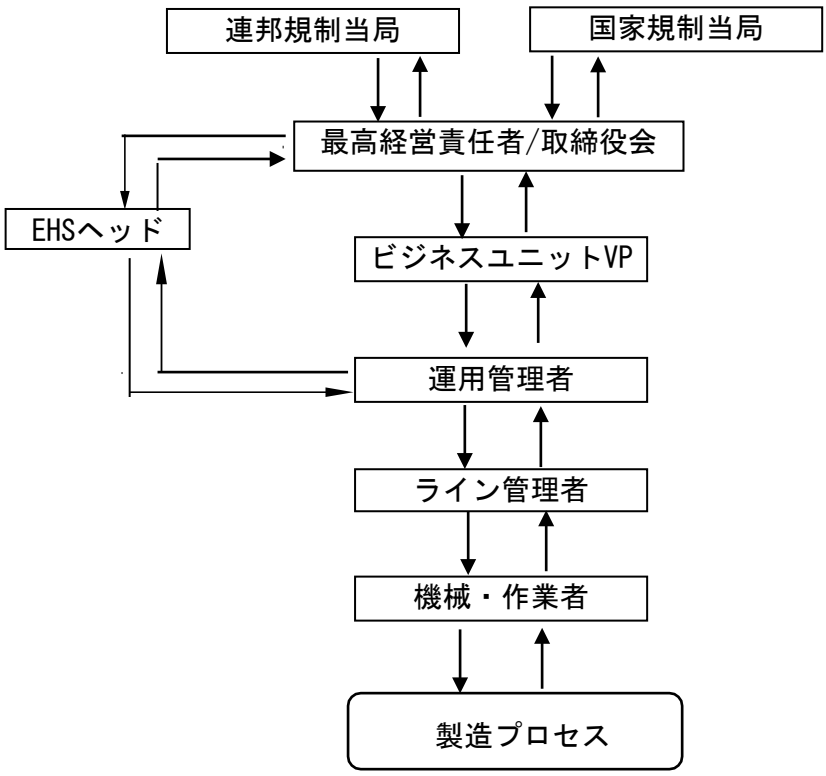
もう１つ注意することは、よくあるように、事故報告書は、被害者と、作業に直接関与している最下層の作業者に焦点を当てていたということです。

読者の皆様は、職場での障害の原因分析には慣れておらず、この例は特に悪い例であると思うかもしれませんが、これは非定型的なものではありません。この会社は、大規模で、高度に複雑なシステムを製造しており、この事故を分析するために使ったプロセスは、標準文書の手順、および、ほとんどではないにしても多くの会社で使用されているプロセスに従っていました。

是正措置（推奨事項）は、CASTによって生成されたものと比較するまでは、不合理なものには見えません。床板を取り除くことを許すことは、他の安全性と製造の目的を達成するためには必要ですので、是正措置の結果は他の目的と競合し、従って、特に時間経過とともに無視されがちであることに留意してください。工場内での特定の作業のためにツールの要件を追加することは、良いこと（驚くべきことにまだ達成されていませんが）のように見えますが、他の長期的な是正措置はあまり有用ではなく、また現実的ではないようです。そして再び、安全ではなさそうなものもありますが、記述されている指示に従う作業者へと、すべてが伝えられます。

足場事故のCAST分析：

公式の事故報告書に含まれる情報があまりにも少ないので、CAST分析の多くを、当時回答されるべきだった質問で十分に満たす必要があります。しかし、ここではもっとも基本的なシステムコンポーネントとCASTの生成した質問の概要を示します：



物理的：

故障：なし

非安全な相互作用：作業員が足場にある穴から落ちました。

第１シフトの作業者：

責任：

- 監督者の指示に従います。
- 文書化された標準的な手順に従います。

事故の寄与要因：

- 間違った種類の足場構成の設定をしました。

メンタルモデルの欠陥：

- 足場を要する作業は何かを知らない、あるいは、その作業の要件を知りません。

コンテキスト：

- 実施した方法で足場を設定するようにと指示されましたか？
- 完了するべき時間に完了していなかった、手順から外れた作業でした。
- その作業に必要なツールの文書化がされていませんでした、あるいは、その作業が何だったかを知らされていませんでした。［*足場を要する作業やその要件について何を知っていましたか？*］

第１シフトの監督者：

責任：

- 作業者に作業指示書を与え、彼らが正しく作業することを確実にします。

事故の寄与要因：

- 間違った種類の足場を設置するよう指示した、あるいは、正しい種類を設置したか調べませんでした。

メンタルモデルの欠陥：

- *どのような作業が足場を要するのかを知っていましたか？*
- *足場には特別な要件があることを知っていましたか？知らないのなら、なぜですか？*

コンテキスト：

- ある時間には完了しているはずだが、完了していない手順以外の作業。
- その作業に要するツールの文書がない、あるいはその作業が何であるか知らされていませんでした。

第２シフト作業者：

責任：

- 指示されたように作業を遂行します。
- 作業指示書で指示された標準的な慣行とツールを使用します。

事故の寄与要因：

- 非安全な足場（床板が取り除かれた）が使われました。
- *実施前に、監督者と、応急処置（jury rigging）について点検しましたか？*

メンタルモデルの欠陥：
- この作業に使用されるべき足場があることを知りませんでした。
- その作業に提供されていたツールを応急処置するために足場を取り除くべきではないことを知りませんでした。

コンテキスト：
- 指示された作業には許されていない非安全な足場が設置されていました。
- 正しいツールが文書化されていませんでした。
- *この作業を行うには、どのような経験がありましたか？ これを行うのは初めてでしたか？ 初めて行うのであれば、なぜ監督されていなかったのでしょうか？*
- 足場(床板)を取り外すことができる理由は、足場が分解されるのを防止するためにワイヤまたは他の材料を使用することにより、製品にとって重大な危険であるFOD（異物残屑)による悪影響の恐れが回避されるからです。
- 会社方針の中で記述されているこの会社の文化では、最優先事項は、どのようにやるかという他者からの指導を待つことなく、作業者が目標を達成する方法を見出すことです。他者からの指示や支援を求めることなく、問題に対処する方法を見つけることが奨励されています。

第２シフトの監督者：

責任：
- 作業者が作業に適した安全なツールを使用することを確実にします。
- 特に手順以外の作業時に、作業者がハザードについて認識していることを確実にします。

事故の寄与要因：
- 非安全な足場の使用を許可しました。
- 手順以外の作業の監督が適切に行われませんでした。

メンタルモデルの欠陥：
- *潜在的なハザードについて知っていましたか？*
- *このような作業のために設計されている足場があることを知っていましたか？もし知らなかったのであれば、なぜですか？*
- *作業者が床板を取り除いたことを知っていましたか？*
- *前のシフトによって設置された足場が適切であることを確認しましたか？*

コンテキスト：
- 適切なツールが文書化されていませんでした。
- 手順以外の作業は、工場では一般的です。

事故報告書に含まれる情報が不足しているので、事後に、この事故における上位レベルのコントロールに対する詳細で有益なCAST分析を提供することは不可能です。しかし、事故報告書には、興味をそそられる、理由が明白になっていない発言があります。例えば、「[順序どおりではない部品を提供した会社の] 従業員とのミーティングが、計画どおりには行われませんでした。」という発言があります。この発言は、なぜ間違った足場が使われていたのかを説明するために使われました。*その工場の手抜かりを直す方法について、計画されたミーティングはあったのでしょうか？なぜ行われなかったのでしょうか？作業の実施方法を計画するためのミーティングが遅れたのに、なぜその作業が発生したのでしょうか？*

CAST分析を完了し、この事故の原因を理解するには、次のような多くの質問に答える必要があります:
- *なぜ作業者は、経験のない作業を経験のある人の監視もなく、行ったのでしょうか？*

- *文書化の不足を超えて、なぜ彼らは、適切な作業の援助について知らなかったのでしょうか？このような作業について、どのような訓練が提供されているでしょうか？*
- *正しい装置が、使用可能であり、使用されることを確実にする責任は誰にあったのでしょうか？直属の監督者でしょうか？さらに上位のコントローラでしょうか？*
- *足場の設計が作業の実施を妨げているのに、なぜ作業者は助言を求めなかったのでしょうか？この答えは、おそらく企業文化に関連しています。*
- *順序どおりではない作業のための監督は誰が行なっていますか？*
- *順序どおりではない作業のハザードを誰が評価しますか？*
- *特定の作業に必要なツールを文書化し、作業者がそれらのツールが何であるのかを知ることを確実にすることに対して、責任があるのは誰でしょうか？なぜ、使用するツールを呼び出すことが標準的な慣行ではないのでしょうか？*
- *順序どおりではない作業のステップやツールは、どのようにして従業員に説明していますか？*
- *他者からのアドバイスがなく、作業者は、一時しのぎの解決策を使っているように見えます。本当のことでしょうか？どれほど頻繁に、起きていますか？過去に誰も、この慣行を止めなかったのはなぜですか？管理者に期待されているのでしょうか？*
- *関係するリスクを理解していないことの責任が、なぜ最下位にある作業者のせいにされ、管理者には向けられなかったのでしょうか？*
- *最初の段階で、間違った足場が組まれたのはなぜでしょうか？*
- *その部品が、本来挿入すべき時に、挿入されなかったのは、なぜですか？*
- *キャンセルされた作業をどのように達成するかについてのミーティングが計画されていました。なぜ、これは開催されなかったのですか？このミーティングが開催されるまで、なぜ作業を待たなかったのでしょうか？*
- *より高レベルの管理者は、これらの慣行について知っていましたか？知っていたのであれば、なぜこのような傷害が起こる前に何もしなかったのですか？知らなかったのであれば、なぜ知らなかったのですか？工場で作業がどのように達成されているのかを監督するための、監査やフィードバックはなかったのですか？*
- *順序どおりではない作業が一般的で、下位レベルの監督者はこれによって起こる傷害について心配していたのですが、それに対処する支援は何も提供されていませんでした。なぜですか？*

これらの質問や、その過程で起こる追加的な質問に答えることは、“作業者に、足場から床板を取り除かない、と命令する”よりも、もっと多くの推奨事項が得られるようです。CAST分析を完了しなくても、以下のような予備的な推奨事項があります：

- 作業に使うべきツールに慣れている監督者の監視が無く、適切な指示を与えられていなければ、作業者に、どんな作業も許可してはいけません。
- 順序どおりではない作業の安全を、現在行われているよりも、よりよくコントロールします。
- 順序どおりではない作業の発生を低減します。完全に排除することはできませんが、サプライチェーンにおいて取り組むべき問題が発生します。
- 順序どおりではない作業のための緊急時の活動を計画し、適したツールが利用できることを確認します。少なくとも、誰かがこのような作業を監督しなければなりませ

ん。

- この作業だけでなく、あらゆる種類の作業に使うべき、足場を含むツール類を文書化します。
- 危険な活動がどのように行われるのか、またハザードがどのようにコントロールされるのかについて、より良いフィードバックおよびパフォーマンス監査を提供します。
- より良い職場のハザード分析を実施し、識別されたハザードをコントロールします。

私がこの会社での職場トレーニングから学んだことの一つは、作業者が仕事のハザードを自分で識別し、それを緩和する手段を取るよう期待されているということです。驚くべきことに、同じような期待は、他の会社にもありました。一つの会社では、作業者に自分自身の仕事としてヒューマンファクタ分析を行うように求めていました。ほとんどの作業者は、大学教育を受けておらず、これらのタスクを達成するのに適任ではありません。これらのことを成し遂げる安全の専門家は、どこにいるのでしょうか？作業者に自分の安全性に対して完全に責任を持たせることは、もちろん、事故が起こった時に便利なスケープゴートを提供することになります。

CASTは、このプロセスを大幅に変更することなく、職場の事故にも簡単に適用することができます。

社会的損失の分析へのCASTの利用

我々の行なったCAST分析のほとんどは、複雑で危険な物理システムとプロセスを含んでいます。しかし、CASTは、社会的プロセスやその他の種類の損失を分析するために使うこともできます。このセクションでは、我々が行なった例を紹介します。他の多くの例と同様、完全なCAST分析へのリンクは、付録Ａで提供します。ここでは２つの例を取り上げます。米国の製薬の安全性と、2008年の金融システムの崩壊の原因です。

製薬の安全性の例

バイオックス（ロフェコキシブ）は、主に変形性関節症を患っている患者が使用する処方疼痛管理薬でした。1999年5月に食品医薬品局（FDA）により承認されました。市場では、この薬はメルク社の収入の主要源の一つで、2003年のメルク社の売上高の11%と概算されていました。米国の医薬品の安全コントロールストラクチャーによりこの危険な医薬品が許可され、5年以上にわたって市販された後、2004年9月に、メルクは安全性の懸念から自主的に医薬品を撤退しました。FDAの科学者の疫学調査によると、バイオックスは27,000以上の心臓発作や死亡と関連していました：「バイオックスは、この国の歴史や世界の歴史の中でも、唯一最大の医薬品安全の大惨事でしょう。[23]」

この例における損失は以下のように識別されます：

損失（「事故」）：

1. 患者は、自分の健康に負のインパクト、この場合は心臓発作や脳卒中などの致命的な心血管イベントですが、を与える投薬治療を受けます。
2. 患者が必要な治療を受けることができません。

この例で強調すべきことは最初の損失、すなわち、自分の健康にマイナスになるような投薬治療を受けたことです。なぜなら、結局、バイオックスは、通常の市販の鎮痛剤よりも効果

[23] 2004年米国上院,2004年11月18日David J. Graham,MD,MPHの証言

的ではなかったため、本来なら患者は必要とされる治療を受けることができたはずです。

ハザード：（全ての製薬に共通）

H1: 公衆が非安全な薬にさらされます。

1. 薬が、安全な使用法のための条件を正しく明記していないラベルをつけて、販売されます。
2. 承認された薬が、非安全であることが分かりますが、適切な対応（警告、市場から撤収など）が取られません。
3. 患者は臨床試験の間に許容できないリスクにさらされます。

H2:薬が非安全に摂取されます。

1. 適応症に対して間違った薬が処方されます。
2. 薬剤師が間違った薬を提供します。
3. 非安全な組み合わせで薬が摂取されます。
4. 指示どおり（投与量とタイミング）に薬が摂取されません。

H3: 患者が必要とする効果的な治療が受けられません。

1. 安全で効果的な薬が開発されていない、あるいは、使用が承認されていません。
2. 安全で有効な薬が、必要とする人にとって手頃な値段ではありません。
3. 開発とマーケティングに不必要な遅延が生じます。
4. 必要とされる薬を医師が処方しない、あるいは、その薬を提供することのできる人に患者がアクセスすることができません。
5. 効果がないと感じる、あるいは堪え難い副作用があるために、患者が処方薬の服用を中止します。

読者は、いくつかのハザードの矛盾が、製薬に関する意思決定を非常に複雑で困難にしていることが分かるでしょう。

これらのハザードは、安全要求や制約へと置き換えることができます：

医薬品の安全要求と制約：

1. 医薬品は、長期的に健康を向上させるために開発されます。
   a. 必要とされる薬の開発、市場に対して、継続的で適切なインセンティブ(報奨金)が存在します。
   b. 新薬の創出には、新しい科学的知識と技術が必要です。
   c. 新薬は、科学的、技術的な知識が利用可能である場合にのみ、開発、製造されます。

2. 市場に出回っている薬は、安全かつ有効です。
   a. 薬は、効果的でタイムリーな安全性試験を受けています。
   b. 新薬は、有効で再現性のある意思決定プロセスに基づいて、FDAによって承認されます。
   c. 医薬品の承認は必要以上に遅延しません。
   d. 薬に付けられるラベルは、安全性と有効性に関する正しい情報を提供します。
   e. 薬は、適正製造基準(Good Manufacturing Practices)に従って、製造されます。
   f. 市販薬は、既知および未知の有害事象、副作用、および潜在的にあるネガティブな相互作用について監視されます。
   g. 承認された後も、長期的に、または分集団で、FDAの承認決定（例えばフェーズIV調査）を検証するために長期的研究を行います。
   h. 潜在的な安全上のリスクについての新しい情報は、独立した諮問委員会で審査します。
   i. 承認後に安全ではないと判明した市販薬は、撤去、リコール、制限される、あるいは適切なリスク/メリットの情報が提供されます。

3. 患者は、健康のために必要な薬を入手し、使用します。
   a. 薬は、患者が入手できます。
   b. リスクとメリットについての意思決定を支援するために、正確な情報が提供されます。
   c. 患者は、健康のニーズのために手頃に最善の処置を受けます。
   d. 患者は、必要な投与量と純度の薬を入手します。

4. 患者は、安全かつ効果的に、薬を服用します。
   a. 患者は、投与量に関する正しい手順を取得して、それに従います。
   b. 患者は、薬物を危険な組み合わせで摂取することはありません。
   c. 患者は、治療を受けている間、適切に医師によって見守られます。
   d. 患者は、臨床試験中に、許容できないリスクにさらされません。

安全コントロールストラクチャーは、FDA、製薬会社、患者、学術系研究者、医療提供者といった主要な５つのコンポーネント、および、医薬品の安全性において役割を担っている様々な人々（議会、雑誌の編集者、患者団体など）で構成されています（図22）。コントローラの責任は、個々のコンポーネントのCAST分析の中で記述します。CAST分析の例を少しだけ、ここに示します。マシュー・クチュリエによる完全な分析については、付録Ａにあります。

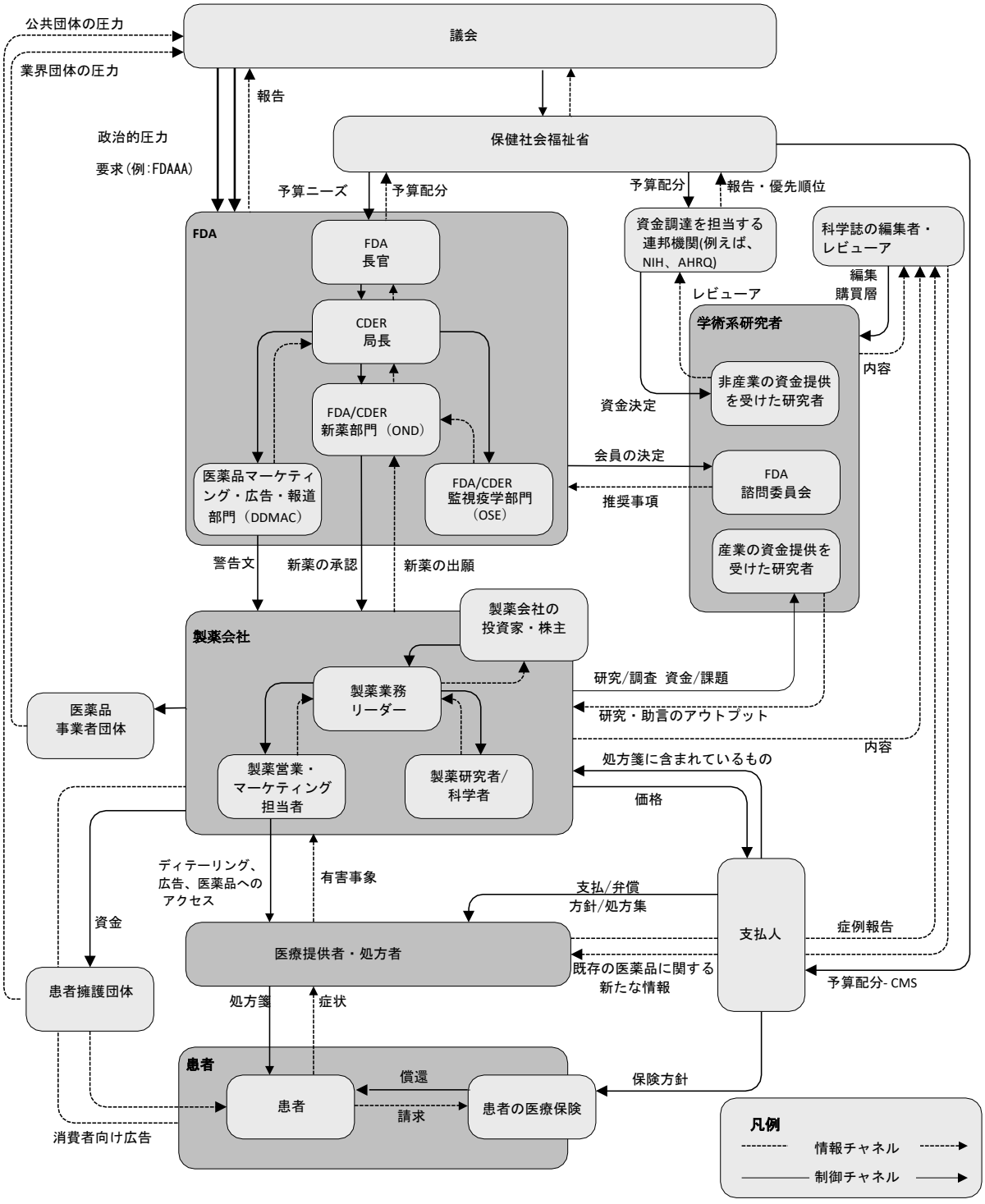


図 22：米国における製薬の安全コントロールストラクチャー

患者

責任：
1. 自分の健康と治療に対する限られた責任（実用的なものに限る）を受け入れます。
2. 医師の指示に従い、処方された薬を服用します。
3. 必要に応じて、医師の優れた知識に従います。
4. バイオックスのような薬の処方箋を入手するために、医師の診察を受けます。

損失の寄与要因：
1. 患者によっては、たとえ必ずしも彼らの特定のニーズに最も適切な治療でなかったとしても、バイオックスを処方するように医師に圧力を掛けることがありました。

メンタルモデル：
1. 患者は、その薬が実際よりも安全であると信じていました。
2. 患者は、より新しく、より高価な薬の方が、古い代わりの療法よりも良いと信じています。

決定がなされたコンテキスト：
1. 患者が得ることのできる、バイオックスの安全性と有効性についての情報は限られていました。彼らが得た情報のほとんどは、消費者向け（DTC）広告から来たもので、華やかで尊敬されている代弁者（例えば、アイススケーターのドロシー・ハミル）とともに、その薬のすばらしい効能を提供しているものでした。
2. 患者が得ることのできる、自分の病気や受けている治療に関する医学的知識は限られており、医師の意見やアドバイスに頼らなければなりません。
3. バイオックスは、FDAによって承認されており、これで安全性が「保証」されたと患者は思い込んでいました。この薬は、医学雑誌の中で医学界によって明らかに推奨されており、保険会社（新しい治療法に対して患者に償還しようする）によって、暗黙のうちに支持されていました。
4. バイオックスを服用している患者の多くは、胃腸障害のリスクが非常に少なく、従って非ステロイド抗炎症薬（NSAIDs）が処方されるべきであり、バイオックスを服用するべきではありませんでした。

医療提供者・処方者

責任：
1. 患者の最善の利益に基づいた治療法を決定します。
2. 治療することと治療しないことのリスクを比較します。
3. ラベルの制約にしたがって薬を処方します。
4. 処方されている薬のリスクとメリットの特性について、最新のメンタルモデルを維持します。
5. 治療下での有害事象とネガティブな相互作用について、患者の症状を監視します。
6. 処方されている薬の使用に関係する可能性のある有害事象を報告します。

損失の寄与要因：
1. 医師が、必要のない患者に、適正使用でも適応外使用でも、バイオックスを処方していました。

メンタルモデル：
1. 既存の治療よりも新薬が優れていると信じていました。
2. 製薬会社からの情報は正しいと信じていました。
3. バイオックスのリスク/メリットのトレードオフを理解していませんでした。特に、この薬の長期使用に伴う潜在的な心血管リスクについては知りませんでした。
4. バイオックスが処方されなかった場合に、患者は別の開業医に行くかもしれないと信じていました。

決定がなされたコンテキスト
1. 医師は、主に製薬会社自身から、新製品について学んでいます。
2. 医師は周知のごとく多忙で、医学雑誌を読み、最新の治療法に追いつき、また治療法のメリットとリスクについて議論するための時間が限られています。
3. 医師の偏りのない情報へのアクセスは限られています。
4. 新薬の研究は、一般的にプラセボと比較しながら行われます。承認された薬のどれが、特定の患者にとって、より適した治療法であるのかを決定するために必要な情報を、医師は持たないままとなります。
5. 医師はサービス業の一種であり、患者が求める薬を処方しないことによって患者と仲たがいしたくありません。
6. バイオックスのラベル（FDAによる）には、心血管リスクについて言及されていませんでした。

メルク

責任：

1. 回避可能なリスクから、患者を確実に保護します：
    a. 安全で有効な薬を提供します。
    b. 有効性について薬をテストします。
    c. 薬に正しいラベルを貼ります。
    d. 臨床試験中、試験を適切に監視し、患者を守ります。
    e. 薬の安全ではない使用を勧めません。
    f. もはや安全と考えられない場合、市場から薬を回収します。
    g. 適正製造基準に従って、薬を製造します。
2. 薬の安全性を監視します：
    a. FDAの要求に応じて、長期の承認後調査を行います。
    b. 潜在的な安全性のハザードをテストするために、新しい臨床試験を実施します。
    c. 有害事象の報告チャネルを、提供、維持、奨励します。
3. 医師やFDAに薬剤の安全に関する正確で最新の情報を伝えます：
    a. 医師を教育します。
    b. FDAに対して、薬の安全性に関する入手可能なすべての情報を提供します。
    c. 新たな安全上の問題の可能性について、適時、FDAに通知します。
4. 新薬や新治療法の開発に役立つ研究を行う、あるいは、そのスポンサーになります。

損失の寄与要因：

1. メルクは、心血管（CV）のネガティブな結果を発見する可能性のある研究を行いませんでした。会社の経営層は、バイオックスのCVリスクの研究をすることを却下しました。
2. メルクの研究と同社が発表した結果では、この薬のリスク/メリットの特性を十分には説明しませんでした。
    a. この研究は、マーケティングの目標によって動機付けされていました。
    b. 結果が発表されたとしても、公開は概して非常に遅い、あるいは、部分的にしか公開されませんでした。
    c. 結果は、実態よりも良く見えるように偏っていました。
    d. 実施された研究の中には、臨床試験を監視し患者を守るための、アクティブなデータ・安全モニタリング委員会（DSMB）を設けないものもありました。患者の安全性は、ただメルクの研究者の手中にあるのみでした。
3. メルクは、バイオックスの安全性プロファイルに関して誤解を招く情報を公開し、宣伝しました。
    a. メルクは、 CVの質問を避けるよう訓練された特殊任務部隊を用いて、薬の使用を積極的に促進しました。
    b. メルクは、偽りの、公正なバランスに欠けている、あるいは誤解を招くような、プロモーション活動と資料を使用しました。同社は、バイオックスを回収する１か月前まで、不利な結果を最小限に抑え続けました。
    c. メルクは、ゲストの著者やゴーストライターを使って、出版物を公開あるいは宣伝しました。この執筆過程でのメルクの従業員の関わりについては、あまり言及されておらず、主要な著者との金銭的な関係は必ずしも明らかにされませんでした。

d. メルクは、独立したピアレビュー誌に見えるように作られたジャーナルを作成しました。これらのジャーナルは、実際にはバイオックスとメルク社製の別の薬を宣伝する記事の編集物を、売り物にしていました。

メンタルモデル

1. メルクはもともと、バイオックスは、どのようなCV事象も引き起こさないと信じていました。
2. メルクは、ネガティブな結果の公表を効果的に制限して、潜在的なCVリスクがあるにもかかわらず、薬を処方する医師を納得させることができさえすれば、バイオックスは、大ヒットの薬になり重要な収益源になる可能性があると信じていました。
3. ネガティブな結果を隠すことによって、会社の評判を守ることができると信じていました。
4. CVリスクが潜在しているにも関わらず、薬の処方をする医師を納得させることができると信じていました。

コンテキスト：

1. メルクは、株主に対して投資の収益を提供する受託者の義務を負っており、出資者は、高い収益を要求します。さらに、製薬会社の幹部には、ストックオプションで部分的に支払われました。
2. 満足のいく決算は、バイオックスが大ヒットの薬であることに依存していました。
    a. バイオックスは、メルクの主な収益源であり、非常に収益性が高い状態でした。
    b. バイオックスは、これが承認される5ヶ月前にFDAによって承認されたセレブレックスとの熾烈な競争に直面していました。メルクはセレブレックスと競争力のある薬を積極的に促進しなければなりませんでした。
    c. メルクは、ネガティブな研究結果が売上に影響を与えることを許しませんでした。
    d. 製薬会社は多くの場合、大ヒットとなる薬を開発することに依存しています。バイオックスの成功は、会社の財務の将来のために重要であると考えられていました。
3. 比較研究では、バイオックスがナプロキセンよりも、心血管事象が高くなることを示唆していました。メルクは、その差について、バイオックスのネガティブな副作用ではなく、むしろナプロキセンが患者の心臓を保護するからである、と推測しました。
4. 製薬会社では、フェーズIV（承認後）の研究を行うこと、または内部の研究でのネガティブな結果を公開することには、何もインセンティブがありません。
5. 薬のほとんどの臨床研究は、それらを作っている会社がスポンサーになります。製薬会社は、現在、その研究の実施や報告の方法について、過去に比べてはるかに統制しています。
6. メルクには、保つべき評判がありました。市場からバイオックスを回収してCV事象について認めることで、その評判を損なうでしょう。
7. 薬の流通ルートは先細りになり、古い薬は特許保護を失っていました。メルクは最も収益性の高い特許を５個失おうとしていました。
8. 製薬会社は、たとえFDAによって要求された場合でも、フェーズIVの安全性テストを行うためのインセンティブを与えられていません。同様に、彼らはネガティブな社内研究を公開するためのインセンティブを与えられていません。

FDA/CDER

背景の情報

人への医薬品に責任を持つFDA内の部署は、医薬品評価研究センター（CDER）と呼ばれています。 CDERにおいて、新薬部門（OND）は、新薬を承認し、薬のラベルを設定し、必要であれば薬のリコールを担当しています。監視疫学部門（OSE）は、医薬品の承認時に検出されなかった有害事象を特定することに焦点を当てており、ONDに対して、ラベルの変更やリコールなどのアクションを推奨することができます。

責任：

委員会のスタッフ

1. 有能な諮問委員会のメンバーを選出し、利益相反規定を設定し遂行します。
2. 研究者に正確かつ有用な有害事象報告書へのアクセスを与えます。

新薬部門（OND）

1. 臨床試験の参加者の安全を確保するため、治験医療製品のためのすべての米国臨床試験および開発プログラムを監督します。FDAのためにこれらの機能を実行するIRB（治験審査委員会）の監視を行います。
2. 新薬の承認のための要求とプロセスを設定します。
3. 意図した使用においては、薬は安全であるとするスポンサーの主張を注意深く検討します。新薬の安全性と有効性を公平に評価し、適切と思われる場合は販売を承認します。
4. 承認後、薬にラベルを設定します。
5. 有益な効果を有する可能性がある薬を、不必要に遅延させません。
6. 長期的な安全リスクの可能性がある場合、フェーズIVの安全性試験を要求します。
7. 新たな証拠によってリスクがメリットを上回ることが示された場合、市場から薬を回収します。
8. 医薬品の安全性に関する新たな情報が発見されたときには、ラベル情報を更新します。

医薬品マーケティング・広告・報道部門（DDMAC）

1. 医薬品のマーケティングと販売促進を監視します。広告の正確さとバランスを審査します。

監視疫学部門（OSE）

1. 製品の安全性、有効性、品質の評価を継続して行います。安全性の問題があるかどうかを判断するために、有害事象データについて統計分析を行います。
2. 薬が市販された後で得られた新しいデータに基づきリスクを再評価し、リスクを管理する方法を推奨します。
3. 医薬品の安全性の問題に関して、ONDのコンサルタントとして務めます。
4. 新しい証拠で重大なリスクが示された場合は、市場から医薬品を回収することを推奨します。

果たした役割：

FDA（省庁）全体

1. 諮問委員会メンバーの利益相反規定の放棄を許しました。
2. FDA従業員に対して、バイオックスの研究について結論と提言を変えるよう圧力をかけ、結果の公開を阻止しました。
3. 研究者が使用するための、品質有害事象報告を入手できませんでした。

OND

1. バイオックスが迅速審査の基準を満たしていないにも関わらず、迅速審査を行い、承認を与えました。
2. 臨床試験の安全要求が施行されていたかどうかを確認していませんでした（例えば、試験の実施要綱078にはアクティブなDSMBの要求があった）。
3. 長期的なリスクが不明だったにも関わらず、フェーズIVの研究を要求せずに、バイオックスを承認しました。
4. バイオックスのラベルを、タイムリーに更新しませんでした。
5. バイオックスのリコールを遅らせました。十分に早く、あるいは効果的に行動しませんでした。

DDMAC

1. 最初の警告文の後に、その後の警告はありませんでした。虚偽や誤解を招く販促資料は見直されませんでした。

OSE

1. 長期的なリスクについて薬を適切に監視しませんでした。影響を受けた集団内の薬による有害事象と、通常の有害事象を区別できませんでした。
2. 疑惑が最初に発生した時に、メルクが大規模な臨床試験を開始するように主張しませんでした。
3. 薬のリコールを要求しませんでした。

決定がなされたコンテキスト

FDA（省庁）全体

1. FDA長官の強いリーダーシップの欠如、高い離職率、空席のある役職。
2. 新薬部門（OND）と監視疫学部門（OSE）との間の対立。ONDはOSEよりもはるかに大きく、多くのリソースを持っていました。OSEが製薬のリコールを提案すると、それはONDの失敗として認識されます。
3. PDUFA：FDAは、監視や規制することになっている製薬会社から、部分的に出資されていました。これは、（a）承認時間の短縮への圧力、（b）承認におけるスタッフよりも、安全監視およびマーケティングの監督におけるスタッフの方が比較的少ない、ことにつながります。
4. 人員と予算のリソースが限られていました。
5. 諮問委員会への参加を求められている専門家の多くは、製薬会社と協力しています。そのような関係を持たない専門家を見つけることは困難です。
6. 政治と議会の圧力（例えば、規制への抵抗の風潮、特別な利権）。

OND

1. 市販前の審査において、FDAは、その会社によって提供された情報しか持っておらず、他の独立した研究データはありません。
2. 法律によって、情報の全面開示が阻害されています：臨床情報は秘密にされており、FDAは、独立した分析をするために機密情報のデータを共有することはできません。
3. FDAは、進行中の臨床試験を追跡することはできません。
4. 法律によって、FDAはラベル変更を要求することが難しくなっています。
5. 医薬品がリコールされる前には、その薬が危険であることに対して、非常に高い確実性を要求されます。
6. ONDが、製薬の承認とリコールの両方を担当しています。
7. PDUFAの手数料は、ODNの予算の50%以上を占めます；FDAは、PDUFAによる資金調達に依存しており、これは、意思決定プロセスに影響があります。

OSE

1. 独立した意思決定の責任はありません。
2. OSE責任者の高い離職率。
3. 選択的な公開に対する規制はありません（会社は、臨床試験の結果、あるいは臨床試験が行われていたという事実でさえ、公表する必要がありません）。
4. いったん薬が承認されると追加的な安全性試験を要求する法的権限はありません。市販後の安全性の要求はほとんど強制されません。
5. 有害事象の報告は限定されます：自発的に報告され、事象が実際にその製品によって起きたことは確実ではなく、使うには報告書に十分な詳細さがありません。研究者は、その薬を何人が服用しているのか知らないため、有害事象報告システム（AERS）を使用して集団内の発生率を算出することができません。
6. 有害事象に関する情報源が限定されています。

残りの分析については省略しますが、このテーマに関する論文へのリンクは付録Ａにあります。

2008年の金融危機の例

メリッサ・スペンサーは、2012年MIT修士論文で、2008年3月における、投資銀行ベアー・スターンズの経営破綻と急な買収の状況を理解するために、CASTが使えることを示しました。ここには、CAST分析の一部のみを示します。修士論文全体へのリンクは、付録Ａを参照してください。

損失の事象：銀行の破綻（Insolvency）

定義：支払い能力（Solvency）は、基本的な方程式です、資産=負債+資本　を満足するように定義されます。破綻（Insolvency）は、この方程式が維持できなくなったとき発生します。

ハザード：

H1: 銀行が、債務（流動性のない（現金化できない）資産）を支払うことができません。
安全制約：銀行は、期日までに債務を支払うことができなければなりません。
安全制約：銀行は、短期負債をカバーするために十分な短期の資産および/または資本金を有している必要があります。

H2: 銀行は、資産から資本を減じたものよりも負債の方が大きい状態にあります。
安全制約：銀行は、支払い能力（Solvent）の貸借対照表を常に持っている必要があります。
安全制約：銀行は、その資産と資本金を超える負債を取得してはいけません。

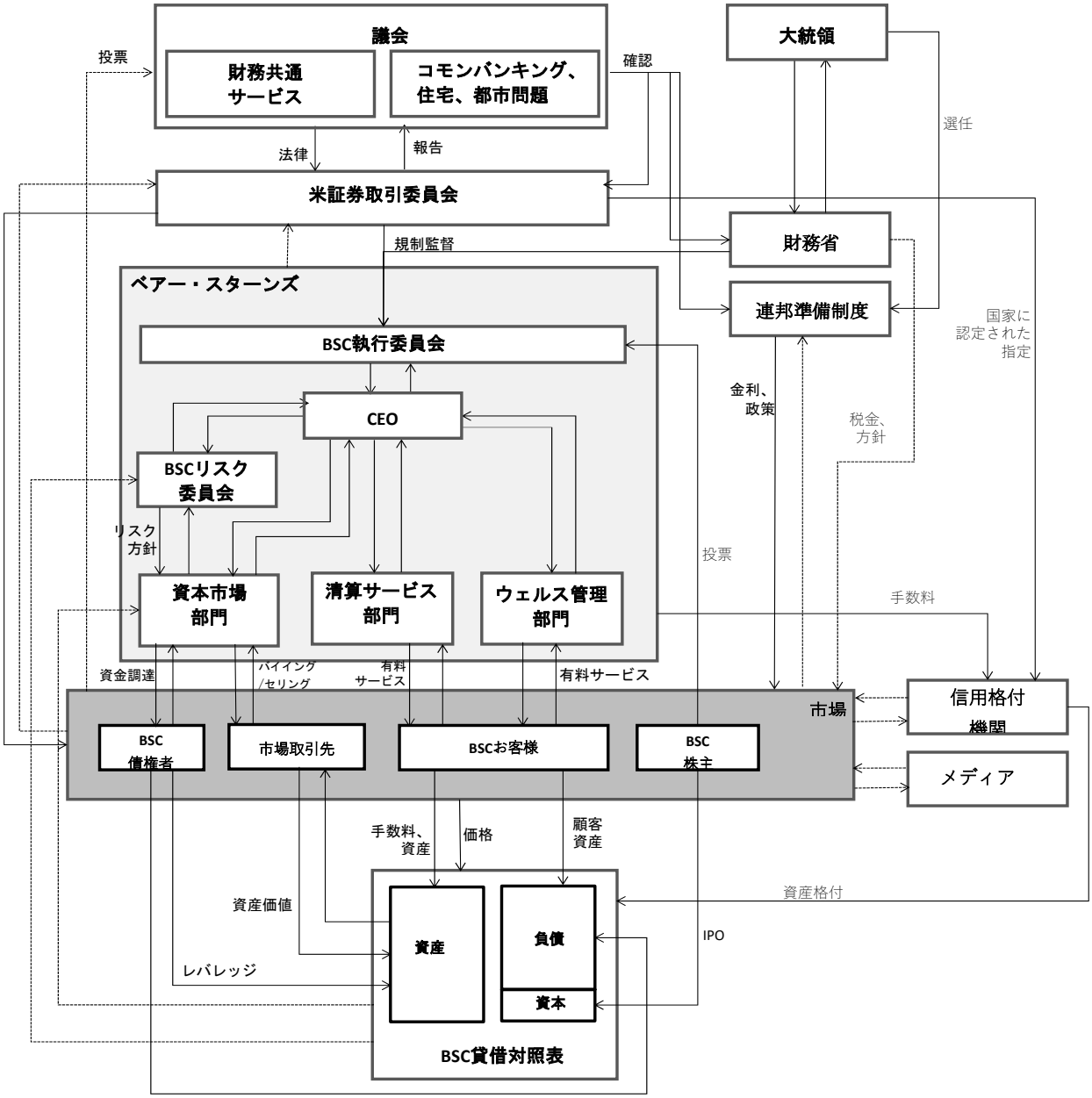
H3: 市場が、金融商品の価値を決定できません。
安全制約：市場参加者が、市場の商品の価値を決められなければなりません。
安全制約：市場で取引されるすべての金融商品には、固有の相対値を決めるのに利用できる有効な情報がなければなりません。

H4: 市場が、金融機関の信用力を判断できません。
安全制約：市場参加者は、銀行の信用力を判断できなければなりません。
安全制約：市場で利用可能である、銀行の健全性に関する情報について、明確かつ公平な情報源がなければなりません。

損失に関与する主要なコンポーネントは以下のとおりです。

- 資産提供者
  - 金融業者のトレーダー（市場で資産を売買）
  - 金融業者への債権者（会社への金銭や資産の融資）
  - 金融業者のクライアント（手数料や資産を提供）
- 債務コントローラ：
  - ベアー・スターンズの経営者（株主を保護し、リスクを管理する責任）
  - ベアー・スターンズのトレーダー（日々の貸借対照表に対する責任）
- 資本提供者：株主
- 連邦準備銀行：
  - 海外市場、金利の設定、商業銀行への最後の貸し手としての務め
- 証券取引委員会
  - 投資銀行の貸借対照表と健全性を監視
  - 市場での証券の詳細を監視
- アメリカ合衆国財務省

コントロールストラクチャー:



ここでは例として、一つのコンポーネントのCAST分析を示します。

投資銀行の連邦規制当局（連邦準備制度）：

責任：

- 銀行が、詐欺や搾取の実行に関係しないことを確実にします。
- 銀行が、顧客を保護するための基本的な慣行を実施することを確実にします。
- 投資に関する公的知識のための適切なメカニズムがあること、つまり投資家がリスクに関する十分な知識へのアクセスがあることを確実にする、銀行の慣行を監査する、市場を監視します。
- 国家全体の経済が安全であることを確実にし、金融システムの相互関連性を監視し、すべての機関および商品が適切に規制されることを確実にし、連邦政府の資産を保護します。
- 急速に変化する市場で生じる市場の外部性を検出して排除します。

損失の寄与要因：

- 商業銀行と投資銀行の規制上の保護に関して相応な変更を加えることなく、両機関の間の規制上の区別が失われることを許しました。
- システムの健全さと、システム内の銀行家と株主の健全さを区別しませんでした。
- 規制されたエンティティと規制されていないエンティティの間の相互関連性の構築を許しました。
- 公平な（銀行によって支払われていない）信用格付けメカニズムがあることを確実にしませんでした。
- 投資銀行の貸借対照表に関する規制要件を、十分迅速に更新しませんでした。
- 安全でない住宅ローンへとつながる住宅政策を促進しました。
- 独立した信用格付け機関から、運用上の開示を求めませんでした。

プロセスモデルの欠陥：

- 金融機関は競争力を維持するために“自主規制”すると信じていました。
- 規制されていない、および、ゆるく規制されている事業体の失敗は、直接これらにさらされた投資家にのみ影響を与えると信じていました。
- 住宅ローンに基づく保証は、投資家への正確なリスクプロファイルを反映しており、安全に作られていると信じていました。
- 単体の機関や商品の失敗は、金融システム全体に影響を与えることはないと信じていました。

コンテキスト：

- 別々の管轄区域における複雑な規制制度（Fed、SEC、FDIC、米国財務省など）。
- “自由放任主義”の経済政策に対する政治的圧力。
- 投資銀行はリスク選好で、より精通した投資家のためのものである一方、商業銀行は、（FDIC とFedの規制を与えられて）安全であるとみなされていました。
- 一般的に規制緩和を支持する銀行の、政治的・社会的圧力が大きくなっています。
- 規制する側と規制される側の間の補償には大きな違いがあります。
- 規制当局は、急速に変化する市場（新技術、新商品、新しいつながり）に追いつくことが難しくなっていました。
- 銀行は常に規制の抜け穴を探して（発見して）います。
- 1990年代と2000年代における、持ち家促進のための政治的圧力。

これまでのところ、非物理的なシステムにCASTを使った試みは少ししかありませんが、これは使えるようです。

第６章：組織や業界へのCASTの導入

CASTは、人が事故原因を考えて特定するように、パラダイム変化を生じさせます。組織にこれを導入することは、古いパラダイムの中で単に表記を変更したり、小さな変更を加えるよりも大きな労力を必要とするかもしれません。この変化を支援するアイデアを、いくつか以下に示します。

この種のパラダイム変化は、多くの場合、組織や業界の重要な関係者による自然におきる倦怠感に打ち勝つのに十分な現状への不平と不満を必要とします。大きなコストを伴う大事故は、このプロセスを促進するかもしれません。しかし、重大な損失を待つことが、事故調査が実施される方法を変化させる最適な方法ではないことは明らかです。新しいアプローチを過去の事故に適用した際にどれだけ効果的であるのかのデモンストレーションは、実用性と利点の両方を示す上で非常に役立つでしょう。

このアプローチは、元々見つからなかった原因を、CASTが明らかにした損失に適用した場合に、特に効果的です。米海軍にいた大学院生であるジョン・ヒッキーは、沿岸警備隊が航空事故率の増加を経験し、2008年から2010年までの22か月間に７回のクラスＡの事故が発生したことに気づきました。事故調査は、リーズンのスイスチーズモデルに基づいた事故原因分析技術であるヒューマンファクタ分析技法HFACSを用いて、パイロットを中心に行われていました。その調査では、共通の寄与因子や原因要因を見つけられませんでした。海軍提督であるヒッキーは、CASTを適用し、人為的エラーではなく、体系的な要因に焦点を当てました。彼は、CASTを使用して損失につながる共通因子を特定することができました。HFACS分析は、兆候を識別するところで止まってしまい、すべての事故で重要となる共通の体系的な要因を識別することができませんでした。[24]

新しい概念の導入は、常に、新しいアイデアの導入に消極的、保守的な政府組織の抵抗につながります。すでに構築されている事故調査のプロセスを変更する試みは、商業的、教育的、および契約上のコストに影響があります。成功裏に変化を達成する鍵は、新しいプロセスなら時間効率がよく、費用対効果がよく、最も重要なものは、将来の安全性をかなり改善できるという結果を示すことです。有効かもしれないアプローチの一つは、線形事象モデルに基づいた定評のあるグループ（例えばNTSBのような）が公開した事故報告書の結果と、CASTのようなシステムアプローチを使用した同じ事故の再分析を比較することです。このようなタイプの比較を行ってきましたが、まだ、より多くのことが必要とされています。

非難的アプローチに対して、非難することに焦点を当てない説明的アプローチの利点を示すことができれば、強力な構成メンバーの集団を作りだすことができます。事故に対して非難の矛先を向けられるパイロットのようなグループは、この新しいアプローチの影響力を発見し、支持しています。変化するよう圧力をかけることのできる、組合、ユーザー・グループ、および専門機関などの重要な団体のグループも、影響力が大きいかもしれません。

他のパラダイムの変化や文化の変化と同様に、上層部に賛同がなければなりません。高レベルのリーダーシップがなければ、低レベルで提案された変化を実施することは困難です。深刻な損失の後に、変化していく機会を進んで捉えるリーダーシップが特に有効となります。悲しいことですが、残念ながら、その大きな変化は、事象に依存した自己満足の崩壊を起こさずには、不可能であることも真実です。もっと楽観的には、大きな変化や改善は強い指導者によって引き起こすことができます。アルコア社のポール・オニールの事例は、事故を大幅に減らす一方で、同時に、第一の目的として、安全性に焦点を当

[24] Jon Hickey, A System Theoretic Analysis of U.S. Coast Guard Aviation-CG-6505 Mishaps米国沿岸警備隊航空-CG-6505災害のシステム理論解析, STAMP Workshop, March 26, 2013, http://psas.scripts.mit.edu/home/

てることによって利益を増加させることができた感動的な例です。基本的には、権限を持つ誰かが、彼らがいつもやってきていることを続けるよりも、損失を低減することが重要であるということを、決断しなければなりません。

業界の小さなプレーヤーによる重大なデモンストレーションも効果的かもしれません。CASTは、小さな事故調査当局に採用されています。これらの取り組みによって示される成功が、他の人へとつながる可能性があります。

回答すべき追加の実用的な質問があります。一つは、違う方法で考え、新しいアプローチを使用する人々を訓練するためのコストです。誰もがシステム思考を自然で簡単であると思うわけではありません。インシデントや事故の独自の内部調査を行っている大規模な組織の場合、CASTを使用した経験のある特別なグループは、最良の結果を得ることができるでしょう。調査チームは、事象が発生したグループの管理から独立して、経営のより高いレベルへ報告しなければなりません。安全組織のなかに訓練を受けたグループを作ることは、最も実用的なアプローチかもしれません。

付録Ａ：実際の事故に対する CAST分析の公開事例へのリンク

ここに含まれる分析のほとんどは、いくつかの例外を除いて、著者または大学院生によるものです。多くは少し前に作成されたものであり、CAST開発における最近の進歩の一部が含まれていない可能性があります。ただし、少なくともCASTがさまざまな業界でどのように使用できるかを示しています。MITの大学院生は、時間と情報が限られており、学習しているだけなので、学生が行った何百もの分析は含めていません。また、事故分析の財産的価値とプライバシーの懸念の理由から、他の人が行った業界の事例も含めませんでした。

CAST Analysis of the Shell Moerdijk Accident Nancy G. Leveson

Increasing Learning from Accidents: A Systems Approach Illustrated by the UPS Flight 1354 CFIT Accident Shem Malmquist, Nancy Leveson, Gus Larard, Jim Perry, and Darren Straker, May 2019

The Underestimated Value of Safety in Achieving Organization Goals: CAST Analysis of the Macondo Accident. Maria Fernanda Tafur Munoz, MIT Engineering and Management Master's Thesis, June 2017. http://sunnyday.mit.edu/tafur-thesis.pdf

Systems-Theoretic Accident Model and Processes (STAMP) Applied to a U.S. Coast Guard Buoy Tender Integrated Control System. Paul D. Stukus, MIT SDM Masters Thesis, June 2017 http://sunnyday.mit.edu/stukus-thesis.pdf

Learning from Accidents that are a consequence of complex systems. John Thomas and Shem Malmquist, ISASI Conference

A Systems Approach to Analyzing and Preventing Hospital Adverse Events Nancy Leveson, Aubrey Samost, Sidney Dekker, Stan Finkelstein, and Jai Raman. *Journal of Patient Safety*, in press, 2016

A STAMP Analysis of the LEX Comair 5191 Accident Paul S. Nelson, Master's Thesis, Lund University, Sweden, June 2008, supervised by Prof. Sidney Dekker.

Safety-Guided Design Analysis in Multi-Purposed Japanese Unmanned Transfer Vehicle. Ryo Ujiie, System Design and Management Master's Thesis, September 2016.

Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System. Blake Ryan Abrecht, MIT M.S. in Engineering Systems Thesis, June 2016. http://sunnyday.mit.edu/Abrecht_Thesis.pdf

Systems Theoretic Accident Analysis of an Offshore Supply Vessel Collision. John Michael Mackovjak, Master of Science in Technology and Policy, MIT, June 2016.

STAMP applied to Fukushima Daiichi nuclear disasteer and the safety of nuclear power plants in Japan. Daisuke Uesako, MIT Master's Thesis, System Design and Management Program, June 2016. http://sunnyday.mit.edu/Thesis_DaisukeUesako.doc

System Theoretic Safety Analysis of the Sewol-Ho Ferry Accident in South Korea Yisug Kwon, MIT Master's Thesis, December 2015.

A Systems Approach to Patient Safety: Preventing and Predicting Medical Accidents Using Systems Theory Aubrey Samost, MIT Master's Thesis, June 2015 http://sunnyday.mit.edu/papers/Samost-thesis-Final.pdf

Comparison of SOAM and STAMP for ATM Incident Investigation Richard Arnold, Master's Thesis, Lund University, Sweden, 2009, supervised by Prof. Sidney Dekker.

A CAST Analysis of a U.S. Coast Guard Aviation Mishap Jon Hickey, MIT Master's Thesis, May 2012, supervised by Dr. Qi van Eikema Hommes.

Application of CAST to Hospital Adverse Events Meaghan O'Neil, MIT Master's Thesis, May 2014

Application of CAST and STPA to Railroad Safety. Airong Dong, MIT Master's Thesis, May 2012

Engineering Financial Safety: A System-Theoretic Case Study from the Financial Crisis Melissa Spencer, MIT TPP (Technology and Policy Program) Master's Thesis, May 2012

A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices Vincent Balgos, MIT SDM Master's Thesis, February 2012, supervised by Dr. Qi van Eikema Hommes

Application of a System Safety Framework in Hybrid Socio-Technical Environment of Eurasia. by Azamat Abdymomunov, MIT SDM Thesis, 2011.
この論文は、MITで「最優秀SDM修士論文」賞を受賞しました。

A System Theoretic Safety Analysis of Friendly Fire Prevention in Ground Based Missile Systems Scott McCarthy, MIT SDM Master's Thesis, January 2013

Accident Analysis and Hazard Analysis for Human and Organizational Factors Margaret Stringfellow, October 2010

A System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident

2012年4月26日～28日にMITで開催された第１回STAMP/STPAワークショップで、中国・北京・清華大学コンピュータ科学技術学部のDajiang Suoが発表しました。

A Case Study of Vioxx using STAMP Matthieu Couturier, MIT Technology and Policy Master's Thesis, June 2010

Nancy Leveson, Engineering a Safer World, MIT Press, 2012には、いくつかの完全な事例もあります：

- Friendly Fire Shootdown of a U.S. Blackhawk Helicopter by a U.S. F-15 over the Iraqi No-Fly Zone, pp.103-167
- The explosion of a Titan IV booster launched from Cape Canaveral in 1999, pp. 469-493
- The E. Coli Bacterial Contamination of a Public Water Supply in Walkerton, Canada, pp. 497-515

最後に、一部の人々が興味を持つかもしれない事故分析について私が書いた学術論文があります：

Applying Systems Thinking to Analyze and Learn from Events Nancy Leveson, Safety Science, Vol. 49, No. 1, January 2010, pp. 55-64http://sunnyday.mit.edu/Safety-Science-Events.pdf

付録Ｂ：シェル ムールダイク損失の背景情報とCAST分析の概要

背景：

2014年6月3日に、オランダのシェル ムールダイク工場で爆発と火災が発生しました。ムールダイク石油工場は、プラスチック製品の製造に使用されるエチレンやプロピレンなどの化学物質を生産しています。軽油、ナフサ、LPGをさまざまな化学物質に変換するために、熱が最初に使用されます。これらの化学物質は、とりわけ、シェル ムールダイクで他の製品を生産するための原材料として使用されます。これらの製品には、事故に関与したスチレンモノマーおよびプロピレンオキシド（MSPO）のプラントによって生産されたものが含まれます。

シェル ムールダイクには、２つのMSPOプラントがあります：MSPO1（1979年に委託）とMSPO2です。この事故はMSPO2プラントで発生しました。このプラントは、プロセスのライセンスを所有している、現在のシェル プロジェクトアンドテクノロジー[25]の前身の組織によって、1996年に設計されました。ユーザーの同意に基づいて、シェル ムールダイクは、MSPO2プラントの運用を担当しています。

MSPOプラントでは、原料としてエチルベンゼンを使用して、スチレンモノマーとプロピレンオキシドを製造しています。スチレンモノマーは、ポリスチレンの製造に使用されます。ポリスチレンは、発泡スチロールなどの幅広い製品に使用されるプラスチックです。プロピレンオキシドは、食品、化粧品、医薬品、その他の製品に使用されるプロピレングリコールの製造に使用されます。

シェルには、世界にさらに３つのプラントがあり、MSPO2プラントとほぼ同じプロセスでスチレンモノマーとプロピレンオキシドが製造されています。シンガポールのセラヤと呼ばれる場所に２つのプラントがあり、中国の南海に１つのプラントがあります。

一般的に、スチレンモノマーとプロピレンオキシドは次のように生成されます：エチルベンゼンは酸素と反応して、チルベンゼンヒドロペルオキシドに変換されます。次に、エチルベンゼンヒドロペルオキシドは、プロピレンと触媒[26]を通した反応で、プロピレンオキシドとメチルフェニルカルビノールおよびメチルフェニルケトンに変換されます。なお、メチルフェニルケトンは、反応の副産物です。最後に、メチルフェニルカルビノールがスチレンモノマーに変換されます。副生成物のメチルフェニルケトンも、別の触媒を用いてメチルフェニルカルビノールに変換されます。事故が発生したプロセスは、この最終段階でした。

爆発は、MSPO2プラントの水素化ユニットで発生しました。ユニット4800の反応器では、メチルフェニルケトンをメチルフェニルカルビノールに変換するための触媒とともに水素が使用されます。ユニット4800内の水素の反応で熱を放出します。熱は、反応器内で液体エチルベンゼンを触媒に沿って流すことで、放散します。このプロセスは「発熱性水素化反応」と呼ばれ、反応器の圧力の増加が必要です。水素は高圧力では非常に引火性があるため、水素漏れが発生すると火災が発生する可能性があります。ユニットの設計と操作の安全要件上、このハザードは重要となります。

一般的に、ユニット4800は、２つの反応器、２つの分離容器、液体を加熱または冷却できる複合設備、およびガス流を凝縮する設備で構成されています。Unit 4800の設置のさまざまな部分は、パイプと１つの中央ポンプで相互接続されています。図B.1を参照してください。

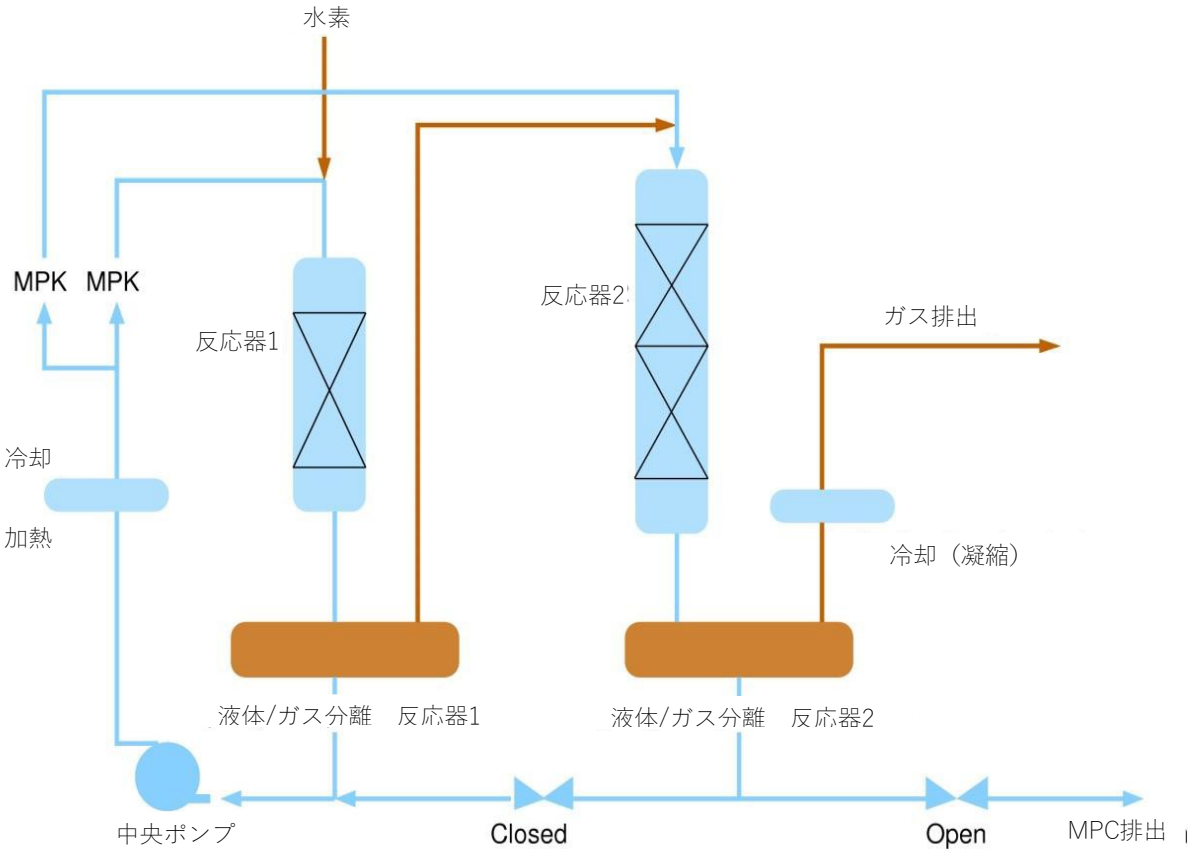
反応器からの液体とガスは、分離容器で分離されます。最初の分離容器からのガスは反

[25] 前身の組織の名前がわからないため、この分析では現在の名前であるシェル プロジェクトアンドテクノロジーと呼びます。

[26] 触媒は、特定の化学反応の速度に影響を与える物質です。

応器2に行き、２番目の分離容器からのガスは、フレア（燃焼）へ送られます。分離容器が適切に機能するためには、ガスと液体の正しい比率を達成することが重要です。正しい比率とするために、さまざまな安全装置が使用されています。

反応器には触媒が含まれています。触媒は、反応器にある物質間の反応を促進するために使用されます。ユニット4800では、触媒は円筒形の触媒ペレットの形をしています。これらは、銅、クロム、バリウムなどのさまざまな元素で構成されています。稼働後、数年が経過すると触媒の効果は低下するため、交換していく必要があります。触媒ペレットは、短時間の保守停止中に交換されます。このケースでは、ペレットの交換は問題ありませんでした。



図B.1：通常生産時の4800ユニット[オランダ安全委員会報告書より採取]

触媒ペレットを交換した後、ユニット4800を再起動する必要があります。この再起動は、次の手順です：（1）ユニットから酸素を放出し、漏れを確認します。（2）汚濁物を除去するために、ユニットをエチルベンゼンで洗い流します。（3）ユニット内をエチルベンゼンで満たし、エチルベンゼンの循環を開始します（循環段階）。（4）ユニットを加熱します（再加熱段階）。（5）水素を使用して触媒を還元します（還元段階）。

触媒ペレットを湿潤の状態にし、触媒の還元を促進するレベルまでユニット内の温度を上げるには、エチルベンゼンを循環させ（ステップ３）、ユニットを加熱する（ステップ４）必要があります。事故は、再加熱段階（ステップ４）の間に起こりました。

トリクルベッド反応器[27]の中で触媒ペレットを湿潤の状態に保つことが重要です。湿潤

[27] トリクルベッド反応器（ユニット4800で使用）には、触媒で満たされた「開放」カラムがあり、重

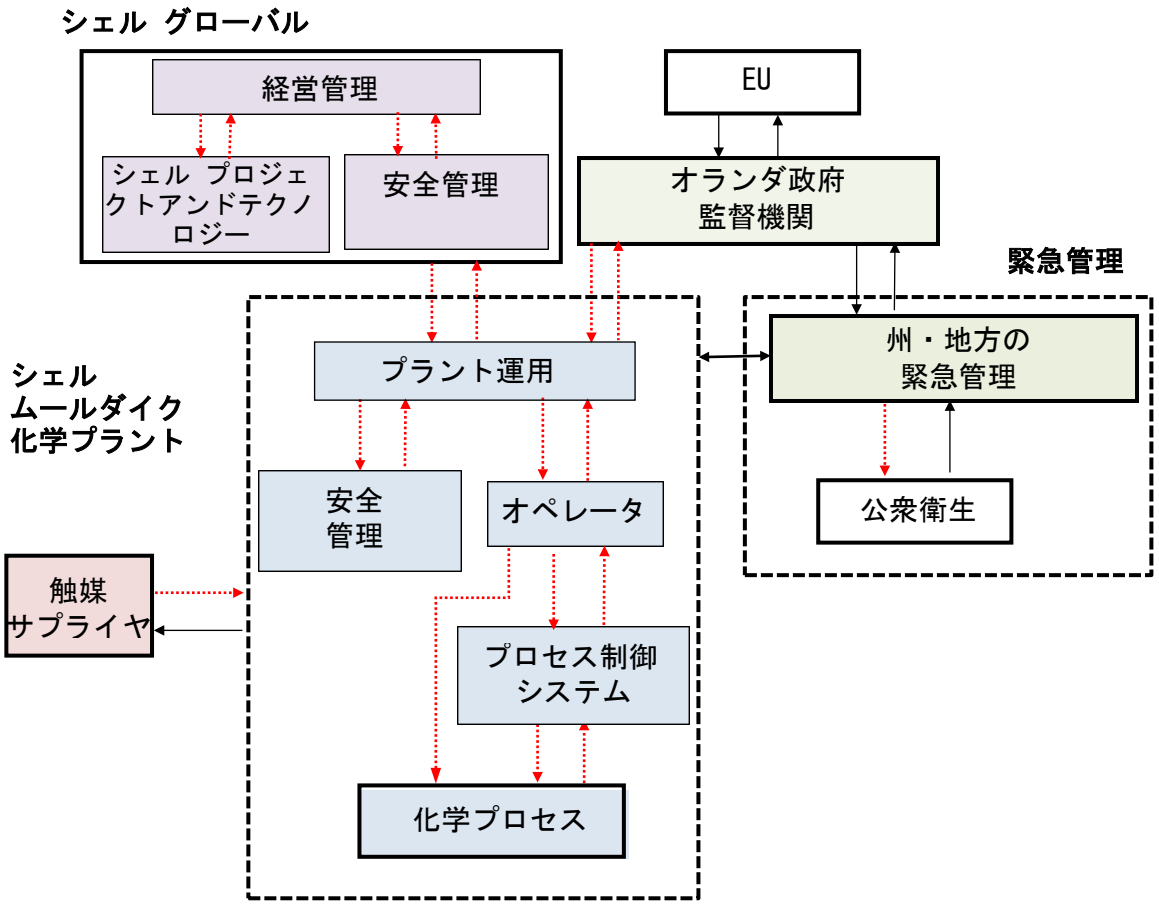
には、触媒をエチルベンゼンに完全に浸し、ペレットを継続的に湿潤状態に保つことが含まれます。局所的な乾燥があると、化学反応による熱を放出できません。その結果、反応器の温度が上昇してしまうことになります。触媒ペレットを湿潤状態に保つためは、十分なエチルベンゼンと窒素を反応器に流し、エチルベンゼンを十分に散布する必要があります。これを達成するためは、エチルベンゼン（液体）と窒素（ガス）を正しい比率で反応器の散布プレートに供給し、液体を触媒ペレット全体に最適に散布する「シャワー効果」が必要です。

触媒還元（反応器の再起動のステップ５）は、プラントが正しい温度になり、高温のエチルベンゼンが最低6時間以上循環した後に、始まります。ユニット4800の事故は、加熱段階での爆発と火災であり、この段階には到達していません。

CAST分析による原因分析と推奨事項の最終的な要約

シェルの安全管理システムと、シェル グローバルおよびシェル ムールダイクのほとんどのコンポーネントの動作には、非常に多くの欠陥があるため、シェルとシェル ムールダイクの安全管理システムと安全情報システムには、包括的な設計のやり直しが必要です。加えて、安全文化の欠如を是正する必要もあります。監督当局の手続きや規制は、事故を防止する効果が無かったので、監督手順のレビューと再設計が適切でしょう。

図B.2は、CAST分析による安全コントロールストラクチャーを示しています。事故の原因となった欠陥のあるコントロールとフィードバックが、点線で示されています。図から分かるとおり、事故原因には、ほぼ全体のストラクチャーが含まれています。



力の影響下で同じ方向にガスと液体が一緒に流れます。

図B.2：想定される安全コントロールストラクチャーにおける欠陥のある相互作用。赤い点線は、コントロールまたはフィードバックが、欠落しているか、または不十分であることを表す。ほぼすべての相互作用は何らかの方法で欠陥があった。

次の表は、CAST分析結果の概要として、事故における各コンポーネントの役割と、そのコンポーネントに対して生成された推奨事項をまとめたものです。CAST分析の詳細において提示した未回答の質問が事故報告書に含まれていれば、事故におけるコンポーネントの役割の理由を、おそらくさらに抽出できるでしょう。

化学プロセス	**役割**：物理的なコントロールはなにも失敗しませんでした。圧力が臨界レベルに達した後の反応器および分離容器の最終的な物理的崩壊は、想定外の、制御できない化学的および物理的な相互作用から生じました。これらの非安全な相互作用の多くは、反応器または安全関連のコントロールの設計上の欠陥によるものです。 **推奨事項**：物理的な設計制約と不適切な物理的コントロールを、修正する必要があります。（潜在的かつ詳細な修正は、ここには含まれていません;それらは、化学技術の専門家が判断する必要があります。
プロセス制御システム	**役割**：プロセス制御システムは、起動中にオペレータに必要な支援を提供したり、オペレータが緊急時にプロセスを容易に停止できるように構成されていませんでした。このような設計判断の理由は、主に、事故シナリオがありえないと考えた設計者による誤った想定にあります。 他の同様の工場で事故が発生し、この想定が誤っていたことが判明した後でも、その想定は疑問視されず、再検討されませんでした。 **推奨事項**：オペレータの知識とスキルは、非定常時に最も試されます。ほとんどの事故は、非定常時の間や変更が行われた後に発生します。プロセス制御システムは、（この再始動シナリオだけでなく）すべての安全上クリティカルな非定常時の動作において、オペレータを支援するように再設計する必要があります。手動操作の場合、意思決定、および監視や時間制限の負荷の低減に必要なすべての支援を、オペレータに提供することを目的とすべきです。
オペレータ	**役割**：オペレータの行動は、不正確な作業指示（彼らが従った）、および作業を実行するために必要な訓練の欠如という状況を考慮すると、適切、または少なくとも仕方がありませんでした。さらに、彼らの作業の多くは、集中力、正確性、精神的な忍耐、プロセス変更の深い洞察、および絶えず変動するプロセスに対する頻繁な調整が必要であったが、プロセス制御システムからはほとんど支援を受けていませんでした。リスクは適切に伝達されませんでした。 管理者は、オペレータが何かを見つけてプロセスを停止することに頼っていましたが、それを行うために必要な情報やトレーニングを提供しませんでした。 **推奨事項**：オペレータは、割り当てられた活動を実施するために適切なスキルと専門知識を有していなければならず、そして、この要件を確実にする責任を割り当てられた者がいなければなりません。オペレータがストレスの多い条件下で適切な判断ができるように、必要な情報と作業状況を彼らに提供することを確実にするには、作業分析中に人的要因の調査が必要です。ま

	た、運転のすべての段階においてより良い自動化された支援が提供されるべきであり、起動のような危険な活動についてのトレーニングが提供されるべきであり、作業指示や作業指示を作成するためのプロセスが改善される必要があります。
プラントの安全管理	**役割**： (1) 使用された安全分析手法が、適切ではなかったか、適用されなかったか、または誤って適用されたかのいずれかでした。ただし、その安全分析手法は、シェルの要件およびオランダの規制当局が要求する最小要件には準拠していました。安全管理は、いくつかの技術関連情報を考慮せず、触媒と反応するエチルベンゼンが爆発を引き起こす可能性があることを調査しませんでした。多くの場所で一般的であるように、シェル ムールダイクの安全管理には、ほとんど効果のない多くの活動があり、その活動の多くは政府の規制への最小限の遵守に注力しています。かれらの活動を少し説明すると、全ての人が、エチルベンゼンと触媒との間の反応は不可能であり、起動プロセスは低リスクであると信じていたということです。 (2) シェルの安全管理システムには、変更に対処するための要件が含まれていますが、MOCの手順に従わなかったか、効果的に実施されませんでした。プラント、触媒、プロセス、および手順に加えられた変更から生じるリスクは、特定されず、管理されませんでした。 (3) 漏出数は、プロセスの安全の主要な先行指標として使用されました。この慣行は、石油化学産業においては一般的です。 (4) 南海およびシェル ムールダイクの同様な事故からの教訓は、リスクを軽減するためには生かされませんでした。 (5) 作業指示の作成に対して、適切な監視がなかったため、オペレータは非安全な作業指示を使用することになりました。 **推奨事項**：2014年6月3日の爆発に特有の問題は解決されるべきですが、オランダ安全機関の公式な事故報告書とCAST分析で特定された、シェル ムールダイクの安全管理設計、特に慣行には多くの欠点がありました。それらは改善する必要があります。 さらに、以下の改善が必要です: (1) シェル ムールダイクは、より効果的な安全管理を行う必要があります。安全エンジニアリングは、形だけのもの、標準を最低限遵守するだけのものではありません。 (2) ハザード分析の情報を用いて、すべての作業指示書の安全性について、有識者がレビューする必要があります。[この場合、ハザード分析にも欠陥がありましたが、これは修正すべき別の問題です。] (3) MOCの手順は、強制され、遵守されなければなりません。変更が生じた場合、過去の想定を再評価する必要があります。 (4) ハザード分析およびリスク評価方法を改善する必要があります。 (5) リスクに対するより適切な先行指標を設定し、適用する必要があります。 (6) 学習した教訓を取り入れて、適用する手順を確立または改善する必要があります。

運用管理	**役割**： (1)運用管理は、実施されたリスク分析またはそのリスク分析に使用された手順の欠陥を特定しませんでした。リスク分析は、オランダの規制当局の最小限の要件、および明らかにシェルの要件に準拠していました。 (2)経時的な変化は、MOC手順に従って評価されませんでした。 (3)作業指示書は、安全エンジニアリングの監督を受けずにオペレータによって作成されました。作業指示書は、シェルの標準に準拠しておらず、加熱速度や窒素流量などの作業のための重要な基準が含まれていませんでした。 (4)運転管理は、プロセス制御システムを、通常の生産段階ではプラントを制御し、生産時以外及び保守段階では制御しないように構成すると決定しました。彼らは、これらの活動が高リスクとは考えていなかったため、手動操作で十分でした。この決定の理由は事故報告書にはありません。 (5)起動時に、異なる請負業者の従業員2名が隣接するユニットで働くことを許可していました。これはおそらく、その段階が危険だと信じていなかったためです。 (6) 起動時に、安全報告書で要求された資格を保有するオペレータを割当ていませんでした。このような事態になった理由は、事故報告書に示されていません。 (7)かれらは、同様のプラントや1999年のシェルムールダイクで学んだ教訓が、ユニット4800の設計と運用に反映することを実施しませんでした。 (8)彼らはMOC手順に従わなかったか、または、この場合には手順が不要であると思ったかのいずれかでした。これを判断するための情報は、報告書に含まれていません。 (9)かれらは、シェル ムールダイクの内部監査を行いましたが、手順とその実行における明らかな欠点を、何も検出しませんでした。監査が効果的でなかった理由を判断できる十分な情報は、提供されていません。 **推奨事項**： (1)適切なMOC手順を確立し、実施します。変化が発生した場合、その変化から影響を受ける想定を再検査します。これは、想定は記録する必要があること、その想定が正しいか識別するために主要な先行指標を確立すること、その想定に影響する可能性のある変化を検査して対応するためのプロセスを確立することを意味します。 (2) この事故を防ぐことができなかった理由に重点を置いて、シェル ムールダイクのSMSを徹底的に見直します。この事故の主な要因は、SMSがコントロールすべきであった基本的な活動にあります。 (3)事故原因を排除するために手順を更新します。例えば、作業指示書の作成と監視プロセスの管理や監督の欠如、不適切なハザード分析やリスク評価手順、定期補修工事実施へのスキル不足のオペレータの配置、過去から学んだ教訓の不十分な活用、事故前の欠点を特定できなかった監査手順などの事故原因を排除します。 (4)プロセス制御システムを改善し、通常の生産以外の機能を実行するオペレータに適切な支援を提供します。

シェル プロジェクトアンドテクノロジー	**役割**：ライセンスを受けた側に提供された設計データは、その技術を使用したプラントにおいて作業指示書を作成する者には使用できませんでした。設計には、初期設計段階のハザード分析では発見されなかったセーフティクリティカルな設計上の欠陥があり、一部のシェル プラントでの運用における重大な問題に関する情報を受け取った後でも修正されませんでした。これらの設計上の欠陥には、不十分な数の温度センサや、発生した圧力を処理できない圧力リリーフバルブの使用が含まれます。シェル ムールダイクのユニット4800の定期補修工事のために、非安全で不完全な作業指示書は、シェル プロジェクトアンドテクノロジーによって承認されました。 シェル社で運用に関する詳細情報がなければ、非安全な制御が発生した理由を正確に判断することは困難です。 CAST分析によって、答えよりも次のような質問が多く生じます。*なぜ設計上の欠陥が埋め込まれ、設計プロセスをどのようにとおり抜けたのでしょうか？　シェル プロジェクトアンドテクノロジー（または別の組織が分析した場合）、どのような種類のハザード分析を実行しています？ 1999年のシェル ムールダイクおよび2011年の南海での事故後、特定された設計上の欠陥が修正されなかったのはなぜですか？ シェルのプラントでの運用中の設計の安全性について、（インシデント以外に）他にどのような種類のフィードバックが提供されていますか？　シェル プロジェクトアンドテクノロジーからライセンスを受ける側に対して、プラントの設計の安全面（ハザード）に関するどのような情報が提供されますか？　設計書にはどのような情報が含まれていますか？ オペレータではなくエンジニアが作業指示書を作成する場合、ライセンスを受ける側が安全な作業指示書を作成するのに十分な設計データを提供していますか？　彼らは、誰がこの作業をするのか、知らなかったのでしょうか？ なぜ彼らは、要求されているシェルの形式に準拠していない、非安全な作業指示書を承認したのですか？　設計書では、特に起動時とその危険性について、どのような情報が提供されていますか？ 設計プロセスでは、どのような種類のハザード分析が実施されていますか？ 変更時の安全確保のためのプロセスは、どのようなものですか？　安全に関する想定はどのように記録され、これらの想定の再分析を開始する条件は何ですか？ 設計者は、彼らの設計の運用に対して、どのようなフィードバックを受け取りますか？* **推奨事項**：事故の原因となる設計特性を修正します。これらの欠陥が設計プロセスをどのようにとおり抜けたのかを判断し、設計および設計レビュープロセスを改善します。設計書を改善し、作業指示書を作成している人が理解できるように、そして、ライセンス提供した技術の安全な運用に必要なすべての情報を含めるようにします。シェル プロジェクトアンドテクノロジーによる作業指示書に対するレビュープロセスを改善して、指示内容が完全かつ安全であることを確実にします。シェル プロジェクトアンドテクノロジーが使用するハザード分析プロセスをレビューし、改善します（または、本組織が独自でハザード分析を行わない場合は、行っている他の組織のハザード分析を改善します）。

企業の 安全管理	**役割**： シェルのプラントにおける、リスク判断と安全管理システムの有効性に関して、不足している観点があったようです。 欠陥のあるプロセスモデルは、不適切なフィードバック（監査や先行指標を含む）に関連している可能性が高いです。 繰り返しますが、CAST分析では、事故における企業レベルの安全管理の役割を理解するため、答えるべき多くの質問が上げることにより、将来、より効果的な安全管理が提供できるようになります。事故報告書には、企業レベルでの安全管理については、ほとんど何も含まれていません。 **推奨事項**：シェルの安全監査を改善します。すべてのリスク評価およびハザード分析プロセスをレビューし、一般的には、安全分析と安全管理の両方のアプローチを改善します。大規模な石油会社の中で、シェルだけが方法の改善が必要というわけではありません。石油化学産業には、回避できる事故やインシデントが多すぎます。 具体的には、事故報告書では、「シェルは、リスク分析の実施方法を評価し、変更すべきです。これには、早期の仮定や想定の再評価を必要とする手順や方針を含める必要があります。新たなリスク分析を実施し、適切な対策を講じ、これらの分析を実施するチームが十分に重要な能力を有することを確実にしなさい。以前には除外されていたリスクに基づく想定には、特に注意を払いなさい。」と述べています。 企業の安全管理システムを評価し、改善します。 プロセスの安全に関するインシデントから学習する手順を改善します。インシデントから学習するためのより良いフィードバックメカニズム（監査と先行指標を含む）とその手順を作成します。
経営層の 企業管理	**役割**: 企業管理は、効果的な安全管理システムが構築されることを確実にする責任があります。シェル社とシェル ムールダイクの両方で、安全管理システムで必要とされる常識的な方針が、明らかに破られました。シェルでは、企業レベルで安全を監督する組織が機能していませんでした。事故報告書には、企業管理に対する安全関連の責任に関して、何も記載されません。テキサスシティの爆発に関するベーカー・パネル（以降、BP）社の事故報告書では、BPの企業管理に対しては安全の責任は割り当てられておらず、現地の責任として扱われていたことが分かりました。会社としての責任放棄（HROによって推進され、BPが従う慣行）が、テキサスシティの爆発の主要な要因と特定されました[Baker 2007]。 これは、石油化学業界において、一般的な問題なのでしょうか？ 　また、事故報告書には、安全に対する基本的な経営層の責任を遂行していなかった理由を説明するコンテキストについては、何も含まれていません。しかし、シェルには安全文化の問題があるように思われます。これは、石油およびガス産業全体の問題ではないでしょうか？ 　事故報告書では、シェル ムールダイクにおいて、安全管理システムがビジネス管理システムと統合されていたことを指摘しています。これは企業レベルにも当てはまりますか？　これは非常に好ましくない慣行です（ディープウォーター・ホライゾンの事故も同様の要因でした）。 安全リスク評価は、高レベルの経営上の意思決定者に情報を隠蔽されないように、ビジネスリスク評価とは別にしておく必要があります。 **推奨事項**：SMSの設計を見直し、安全調査、変更管理、事故からの学習にお

	ける欠点や規制（例：経験豊富なオペレータを雇い、作業指示書の形式に従う）に準拠していないといった、明らかな方針違反を防げなかった理由を解明します。監査において、明らかな手順違反を検出できなかった理由を解明します。このような違反は初めて発生した可能性もありますが、ほとんどの場合そうではありません。 単なる漏出数（結果）ではなくリスクが増加したことを示す先行指標を設定することで監査方法の強化を行い、安全管理システムが当初の想定から外れてリスクが増加していることを特定するフィードバックを構築します。リスクの特定に有効なフィードバック・チャネルを確立して、変更手順の管理や安全ポリシーが確実に守られるようにします。

触媒 製造業者	**役割**：触媒の変更は、シェル社には通知されませんでしたが、新しくなった安全情報シートには含まれていました。 触媒製造業者は、その変更が顧客に与える影響を判断することはできませんが、文書内の情報を変更するだけでなく、触媒の利用顧客がその変更を認識できるよう明確に警告するべきです。 **推奨事項**：シェル社とそのサプライヤ間の契約関係を見直して、重要な変更が確実に伝達されるようにします。情報シート内の変更内容は、明確で理解しやすいようにすべきです。

オランダの 規制当局	**役割**：事故報告書は、規制当局がシェル ムールダイクに、違反の可能性のある行動を許可したことを示唆しています。プラントのシナリオの欠陥は違反と考えられるべきでしたが、そのようにはなりませんでした。そのシナリオは最新の状態ではないか、不完全なものでした。限られたリソースや時間の下で、プラントを監督することは、どの監督モデルでも困難ですが、システムレベルの監督には、公共の安全を確保する上で大きな限界があります。事故調査の結果、提出されたシェル ムールダイクの運用安全管理には多くの欠陥がありました。では、規制当局がその欠陥を検出しなかった監督モデルは、何が間違っているのでしょうか？ **推奨事項**：定期補修工事を含めたリスクが最も高い活動に対しては、優れた監督が必要です。規制当局は、最も危険な活動に対して厳格な手順が使用されていること、および安全管理システムが効果的に機能し、規則に準拠していることを、監督し、確実にする必要があります。限られたリソースが、効果的な行動を妨げることはありません；単に、実施される活動について、より知的な選択を必要とするだけです。安全管理システムの有効性に対する、よりよい評価手順と監視が必要です。規制当局は、シェル ムールダイクの爆発や火災のような事故を防止する上で、効果的な監視の提供を確実にするために、システムレベルの監督を再考する必要があります。

緊急 サービス	**役割**：緊急サービスは、責任を果たす上で非常に効果的に機能しましたが、事故対応において特にコミュニケーションにはいくつかの欠陥が発見されました。 **推奨時刻**：この事故では、LCMSおよびNL-Alert通信プロトコルでいくつかの欠陥が発見されました。本事故の性質上、この欠陥が生命の損失につながることはありませんでしたが、他の状況下ではそうとは限りません。多くの人がLCMSの代わりにWhatsAppを使用した理由、および公式システムがこれらの機能をどのように組み込むことができるかを含め、本事例から学んだことを利用して、システムを改善するべきです。事故は、高負荷時のシステムが実際にどのような動作となったのか確認する機会を作り出し、無駄にすべきではない学習の機会を提供します。

コントロールストラクチャー全体に及ぶ要因について、事故報告書からは、CAST分析に必要な情報はあまり提供されていませんでした。但し、含まれているものによっていくつかの弱点が暗示されており、一般的な推奨事項は導き出すことができます。

安全管理 システム	全体的に不適切な安全コントロールシステム、ゆえに安全管理システムである証拠として、報告書には以下が含まれています：安全でない状況が見落とされた、内部手順が適切に守られていなかった、過去の事故からの教訓が得られていなかった、基本的な化学反応に関する誤った想定が、それが正しくないという証拠が表面化した後も再評価されなかった、変更が管理、コントロールされなかった、不適切なハザード分析とリスク評価手順が使用されていた、過去のインシデントおよび事故からの推奨事項が実行されなかった、重要な行動の監視が欠落していた。まとめると、シェル ムールダイクの安全管理システムは、危険な状況の見落とし、内部手順が守られないことを防止できませんでした。事故報告書には、だれがSMSを作成したか、またはSMSが適切に機能していることを確実にする責任がだれにあるかに関する情報はありません。 **推奨事項**：安全管理システム全体の設計を評価し、改善する必要があります。さらに、ハザードとリスク関連の情報が意思決定者に効果的に伝達され、不適切に低レベルで停止しないことを確実にするために、安全管理システムとビジネス管理システムの統合は慎重に検討すべきです。
安全情報システム	安全情報システムに関する情報は提供されておらず、関係者は適切な情報を持たずに意思決定を行っていたようです。 **推奨事項**：安全情報システムは、高い安全性を達成するために非常に重要であるため、シェル社とシェル ムールダイクは、既存のシステムを評価し、再設計する必要があります。

安全文化	事故報告書は、安全文化について詳細に触れてはいません。しかし、「コンプライアンス文化」と名付けられたものが含まれているようです。そこでは、取り組みの大部分は、単に規制と規制当局の要求に遵守するだけで、安全性を向上させるために積極的な対策を講じているわけではありません。事故報告書は、安全性の優先度が高くなかったことを示唆していると思われる、非安全な行動や警告の見落とし、内部手順の非遵守、過去の事故を参考に変更を行わないこと、変更が生じた後に想定の評価をしないこと、といった非安全な行動を指摘しています。 シェルが使用している「心と精神の安全文化プログラム」には、深刻な欠陥があります。「文化のはしご」は漠然と定義されています（「事故が発生するたびに多くのことを実行します」）。不思議なことに、同社は、この打算的なプログラム（事故報告書では「必須」レベルとして記述されている）の中で自己評価した現在のレベルに満足しているようです。しかし、そのレベルでさえ達成されていないようです（いわゆる「より低い」レベルでもない）。 推奨事項：シェル ムールダイクとシェル社は、それぞれの安全文化を徹底的に調査し、2014年の事故を防止できなった理由を特定する必要があります。
コミュニケーションと調整	**推奨事項**：コミュニケーションチャネル、特にフィードバック・チャネルを調べて、安全に動作するために必要な情報を効果的に伝達しているかどうかを判断する必要があります。これの重要な部分には、オペレータに提供される情報のヒューマンファクタ分析の実行、およびプロセスの設計、特にプロセス制御システムの設計によって作成されるヒューマンエラーの可能性が含まれます。
変更管理	**役割**: 事故の原因となる、計画的および計画外の多くの変更に対して、そのリスクは評価されませんでした。 **推奨事項**：変更管理手順を評価して、このケースで機能していなかった理由を特定し、適切に改善する必要があります。

付録Ｃ：事故原因の腐ったリンゴ理論

事故調査において、運用者を非難することは時代遅れであり、誤った「腐ったリンゴ」理論[28]です。この概念は、システム内のいくつかの「腐ったリンゴ」、すなわち何人か人々が、大部分の事故の原因となっていることを表しています。この見方に立つと、ごく少数の信頼できない人達がいなければ、安全が成立することになります。

この概念は、ドイツとイギリスの心理学者が、組織内の腐ったリンゴを特定して取り除くことで安全性の問題を解決すると確信していた、1925年にさかのぼります。彼らは、「事故を起こしやすい」労働者の特性が存在することを決定づけるために、50年にわたる統計分析を使用しました。その労働者とは、間違いを犯し、それによって事故を引き起こす素質を有すると彼らが主張した、個人の特性を持った人々でした。この統計データは、少数の人々が大部分の事故の原因となっていることを暗示しているように見えました。それらの人々をやめさせれば、システムははるかに安全になります。

腐ったリンゴ理論は第二次世界大戦まで存在しました。第二次世界大戦では、人が設計しなければならないシステムの複雑さが劇的に増加しました。この理論は、アルボスとカーリッヒの２人の統計学者によって1951年にようやく完成しました。

この理論は、論拠に統計上の大きな欠陥があるため、機能しませんでした。事故を起こしやすい、または腐ったリンゴの理論が機能するためには、すべてのシステムにおいてエラーと事故のリスクは等しくなければなりません。しかし、もちろんそうではありません。事故原因の新しい見解では、個人の特性は、事故が発生する理由について、コンテキストほどの説明力を持たないと結論づけています。

> *ヒューマンエラーの問題に直面したとき、「なぜ彼らは気をつけなかったのか？ どうして気付かなかったのでしょうか？」人にもっと注意するように、悪者探しを行い新しいルールや手順を発行することで、ヒューマンエラーの問題を解決できると考えています。*
> *それらはすべて「腐ったリンゴ理論」の表現であり、少数の信頼できない人々がいなければ、システムは基本的に安全であると信じています。 このヒューマンエラーの古い見方はますます時代遅れであり、どこにも導かれません。」*-Sidney Dekker, *A Field Guide to Understanding Human Error*, 2002.

腐ったリンゴ理論は、特に医学で普及していますが、ほとんどの事故は人間のオペレータによって引き起こされるという議論の形で、医学業界に浸透しています。たとえば、もし、悪い医者の５%がほとんどの事故を引き起こすと仮定した場合、最も多くの苦情を抱え、有害事象に関与している医者を特定して排除することだけで、医療ミスを大幅に減らせるはずです。残念ながら、そうはなりません。それは単に、本当に難しい、きわどい仕事をする医師のグループを排除する可能性があります（例えば、予後が悪い腫瘍学的症例）。

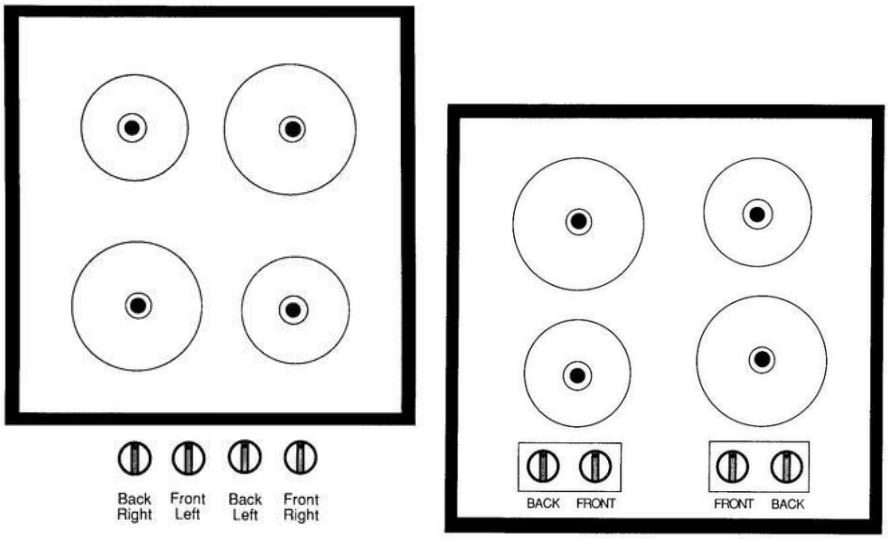
一般的には、特定の状況下（例：限定されたリソース、高負荷時、貧弱な環境等）で人

---

[28] この付録の情報の多くは、シドニー・デッカーによるものです。私たちは医学へのシステムズアプローチについて一緒に論説を書きました(Dekker, S. and Leveson, N. The systems approach to medicine: Controversy and misconceptions（医学へのシステムアプローチ：論争と誤解）, British Medical Journal: Quality and Safety,2014および"The bad apple theory won't work（腐ったリンゴ理論は機能しません）", British Medical Journal: Quality and Safety, Nov. 2014)。Dekkerはまた、2002年の書籍The Field Guide to Understanding Human Error, Ashgate Publishers, 2006において、ヒューマンエラーの「新しい見方」および「腐ったリンゴ」理論について書いています。

的ミスを引き起こす可能性のあるシステム機能がある場合、人員の交代となりますが、誤った動作を引き起こしているシステム機能は変更しないため、事故率にほとんど影響がありません。システムの設計には、さまざまな種類のエラー（モードの混乱等）を発生させる可能性や、逆にエラーを減らす可能性があることが分かっています。驚くべきことに、ほとんどの人は自分たちが環境に影響されていることに気づいていません。目の錯覚が存在することが分かっていても、その錯覚にだまされていることを考えてみてください。

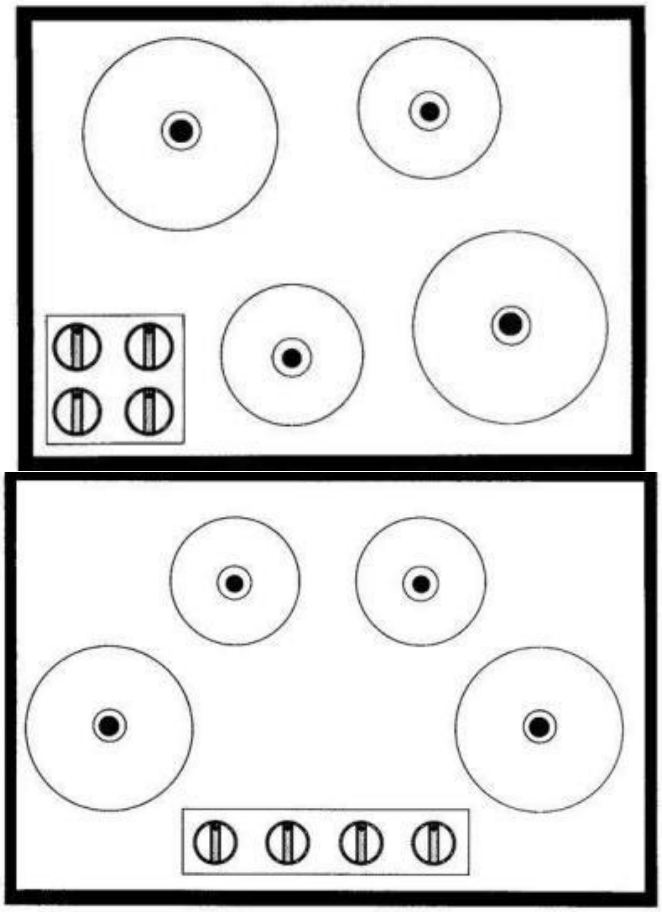
簡単な物理的な例として、図C.1に示すドン・ノーマンのThe Design of Everyday Things（Basic Books、2013）のコンロのデザインを考えてみましょう。現在においても一般的であるこの設計では、つまみと調理箇所を対応付けたラベルが必要です。長年使い慣れたとしても、適切に対応付けるためにはラベルを読む必要があります。そうしないと、急いでいる場合には、間違ったつまみを操作してしまいます。



図C.1：エラーが発生しやすいコンロの２つのデザイン（Don Norman, The Design of Everything, Basic Books, 2013）

図C.2の設計では、これらのエラーの大部分が取り除かれており、実際に、ラベルの必要性は排除されています。

図C.1に示されている、人為的エラーを引き起こす（または少なくともそれらを防止しない）設計例は、システム設計で回避するのが比較的容易です（これは、現在も多くのコンロがまだエラーを起こしやすい設計を使用する理由を説明していません）。しかし、オペレータが認知的に複雑な意思決定を必要とする場合、問題は大幅に悪化します。現在のほとんどのシステムでは、人は、システムの状態や自動化の状態についての不正確なメンタルモデルをより容易に生じさせやすい、コンピュータおよび他の複雑な設計を用いて作業する必要があります。誤った行動が発生した理由や背景を分析せずに、その行動を非難しても、欠陥のあるシステム設計による事故を減らすことはできません。たとえば、今日のパイロットは、自動化における一貫性のない動作、自動化の設計方法に対する誤解、航空機やその自動化の現在のモードに関する混乱などの要因により、特定の状況において間違ったことを行っています。単に「オペレータエラー」で停止するのではなく、事故原因分析中にエラーを誘発する設計機能を識別することは、現在のシステムと将来の設計の両方で安全性を向上させることができます。



図C.2：エラーが発生しにくい設計（Don Norman, The Design of Everything, Basic Books, 2013）

付録Ｄ：損失における安全コントロールストラクチャーの役割を評価する際に考慮すべき要素

下記のリスト（「Engineering a Safer World」、第13章より）は、インシデントと事故の分析を行う際に、不適切なコントロールやコントロールストラクチャーを特定する際に使用できます。このリストは網羅的なものではなく、個別の産業や安全プログラムに合わせて補完が必要です。

このリストには一般的な責任だけが含まれており、割り当て方法は示していません。組織内の特定の人や場所への、責任の適切な割り当ては、各組織の管理構造に依存します。それぞれの一般的な責任は複数の個別の責任に分割され、１つのグループが責任を実際に果たし、その上に位置する他のグループがその活動を監督、指導、指揮、監視することで、安全に関するコントロールストラクチャー全体に割り当てます。もちろん、各責任は、関連する権限と説明責任の必要性、責任を実施するために必要なコントロール、フィードバック、コミュニケーションチャネルを前提としています。

総合管理

- 組織のあらゆるレベルで、リーダーシップ、監督、安全管理を提供します。
- 企業または組織の安全指針を作成します。安全に関する重要な決定の評価と安全管理の実施を行うための基準を確立します。指針を浸透させる経路を確立します。フィードバック・チャネルを確立して、従業員がそれを理解しているかどうか、従っているかどうか、そしてそれが効果的かどうかを判断します。指針は必要に応じて更新します。
- 企業または組織の安全基準を定め、それを実装、更新、実施します。開発および運用における安全工学の最低要件を設定し、請負業者の活動を含め、それらの要件の実施を監視します。危険な操作のための最小限の物理的および操作上の基準を設定します。
- インシデントと事故の調査基準を確立し、勧告が実施され有効であることを確実にする。フィードバックを使用して標準を改善します。
- 安全に関するコントロールストラクチャーの変更を含む、安全への影響に関するすべての変更を評価するための変更要件の管理を確立します。計画外の変更やよりリスクの高い状態への移行については、安全に関するコントロールストラクチャーの監査を行います。
- 組織的な安全コントロールストラクチャーを作り、監視します。安全のための責任、権限、説明責任を割り当てます。
- 作業部会を設置します。
- 強固で信頼性の高いコミュニケーションチャネルを確立し、開発システムの設計と、運用プロセスの状態の正確に管理するリスク認識を確実にします。このチャネルには、請負業者の活動を含めるべきです。
- 安全に関する活動のために物理的資源および人的資源を提供します。安全上重要な活動を行っている人が、適切なスキル、知識、および物理的なリソースを有していることを確実にします。
- 使いやすい問題報告システムを構築し、必要な変更と改善を加えるために監視します。
- 全従業員を対象とした安全教育と訓練を確立し、その安全教育、訓練および継続的改善のプロセスが有効かどうかを判断するためのフィードバック・チャネルを確立します。教育には、過去の事故や原因の振返り、教訓からのインプット、トラブル報告などを含まなければなりません。有効性の評価には、監査中の知識評価から得た情報を含めることが可能です。
- 安全性に関連した技術的意思決定が、費用やスケジュールなどのプログラム上の考慮事項とは無関係であることを確実にするために、組織体制および管理体制を確立します。

- 安全関連の技術的決定とプログラム上の考慮事項との間の対立について、明確で透明かつ明示的な解決手順を確立します。対立の解決手順を使用し、確実に効果をあげます。
- 安全に関する意思決定を行うマネージャーが十分に情報を得て熟練していることを確実にします。すべての従業員（現場の作業員を含む）および請負業者が安全関連の意思決定に貢献できるようにし、奨励する仕組みを確立します。
- 安全に関する意思決定のための評価と改善プロセスを確立します。
- 組織の安全情報システムを構築および更新します。
- 安全管理計画を作成し、更新します。
- 従業員および請負業者が適切に機能していないシステムまたは安全コントロールストラクチャーの一部について、安全性に関する苦情や懸念を表明できるよう、コミュニケーションチャネル、解決プロセス、裁定手続を確立します。懸念を報告する際の匿名性の要求を評価します。

開発

- 開発者や開発マネージャー向けに、安全に配慮した設計やその他の必要なスキルに関する特別なトレーニングを実施します。イベントが発生したときにこのトレーニングを更新し、さらに経験から学びます。トレーニングのフィードバック、評価、改善プロセスを整備します。
- ハザード・ログを作成し、維持します。ハザードとその状態の文書化と追跡を確立し、維持します。
- 作業部会を設置します。
- システムのハザードと安全性の制約を使用して、システムの安全を設計します。設計プロセスが進むにつれて、設計と安全制約を繰り返して洗練します。システム設計では、非安全なオペレータの行動を引き起こすか、それに寄与し、さらにシステムのハザードにつながるコンテキスト要因を排除または低減する方法の検討を確実にします。注意散漫、疲労などは、そうした状況で通常の人間と同様に行動するのではなく、設計者が想像したように人間が振る舞う設計となっていることから生じるリスク要因となります。
- 運用上の想定事項、安全制約、安全性に関する設計上の特徴、事業上の想定事項、安全性に関する運用上の制約、訓練と操作に関する指示、監査と性能評価の要件、運用手順、安全性の検証と分析の結果を文書化します。安全制約と設計上の特徴の間におけるトレースを含め、「何を」と「なぜ」を、それらを実施するために文書化します。
- 安全に関する意思決定が必要な場合に利用可能な高品質かつ包括的なハザード分析を実施します。ハザード分析は早期の意思決定から始め、システムのライフサイクルを通して継続して行います。ハザード分析の結果は必要な人に適時に伝達します。コミュニケーションが下向き、上向き、横向きに（すなわち、サブシステムの間で）なされることを可能にするコミュニケーション構造を確立します。 設計が進展し、検証の経験を積むにつれて、ハザード分析を更新します。
- エンジニアおよびマネージャーが、意思決定においてハザード分析の結果を使用するように指導します。
- 経験を積む中で、ハザード・ログとハザード分析を維持し、使用します。開発に関わるすべての人に安全関連の要求と制約を確実に伝えます。
- 運用（事故とインシデントの報告を含む）における教訓を収集し、開発プロセスの改善に使用します。運用の経験を使用して、開発における安全コントロールの欠陥を特定し、改善を実施します。

運用

- 運用の安全管理計画を作成します。
- オペレータや運用管理者向けに特別なトレーニングを開発し、必要なスキルを教育し、事象が発生してさらに経験から学んだときに、このトレーニングを更新します。このト

レーニングのフィードバック、評価、および改善プロセスを整備します。従業員が安全に仕事を遂行し、安全装備の適切な使用を理解し、緊急時に適切に対応できるように指導します。

- 作業部会を設置します。
- 経験を積む中で、運用時のハザード・ログとハザード分析を維持し、使用します。
- 危険な作業中は、すべての緊急用装置および安全装置が常に作動可能であることを確実にします。安全上重要で、非定常的で、潜在的に危険を伴う運用作業を開始する前に、警報装置のテストを含め、すべての安全装置を点検し、動作可能であることを確実にします。
- 危険な状態（水に反応する化学物質を含むタンク内の水など）や事象を含む、あらゆる動作異常の詳細な調査を実施します。潜在的な危険を伴う運用作業が開始または再開する前に、そうした動作異常がなぜ発生したのかを特定します。この種の調査を実施するのに必要なトレーニングと、管理者への適切なフィードバック・チャネルを提供します。
- 変更管理手順を定め、手順が遵守していることを確実にします。これらの手順には、提案されたすべての変更についてのハザード分析と、安全上重要な運用作業に関連するすべての変更の承認を含む必要があります。安全上重要な機器の無効化についての指針を作成し、実施します。
- ハザード分析の結果を運用と保守の前提条件として使用し、安全監査、性能評価、および検査を実施します。安全に関する方針と手順が守られていること、そして安全に関する教育訓練が有効であることを確実にするためにデータを収集します。増加するリスクの先行指標のフィードバック・チャネルを確立します。
- 開発中に作成され、よりリスクの高い状態に移行する先行指標を特定するために運用に引き渡されたハザード分析と文書を使用します。先行指標を検出し適切に対応するためにフィードバック・チャネルを確立します。
- 運用経験についての情報を戻すために、運用から開発へのコミュニケーションチャネルを確立します。
- すべての体系的な要因を含め、インシデントや事故の詳細な調査を実施します。すべての推奨事項を実施するための責任を割り当てます。推奨事項が完全に実施され有効であったかどうかを判断するために追跡調査を行います。
- 安全上重要な活動が適切に実施されたかどうかを独立して確認します。
- 安全上重要であると特定された項目の保守を優先させます。保守をスケジュールに沿って実施します。
- 安全上重要な装置の無効化および物理システムの変更についての指針を作成し、施行します。
- 以前にシャットダウンしたユニットの運転、あるいは保守作業後の運転を開始するための特別な手順を作成し、実行します。
- 擬似警報の頻度を調査し、削減します。
- 誤作動している警報と計器にはっきりと印を付けます。一般に、現在誤作動しているすべての機器に関する情報をオペレータに伝達する手順を確立し、その手順を確実に遵守します。誤作動した機器の報告に対するあらゆる障害を取り除きます。
- 安全上重要なすべての機器および警報手順について、安全運用範囲を定義し、伝えます。オペレータがこの安全運用範囲を認識していることを確実にします。緊急事態が発生していなくても、オペレータは運用範囲と緊急時の手順に従うことで称えられるようにします。必要に応じて、時間の経過とともに運用範囲と警報手順をチューニングします。
- 安全上重要な物品のスペアの在庫を保有しており、迅速に入手できるようにします。
- 安全関連のすべての事象や活動について、プラント管理者に連絡するチャネルを確立します。管理者が運用に関する安全な決定を下すために必要な情報とリスク意識を有して

いることを確実にします。
- 怪我をした作業員を処置するために緊急装置と対応が備わっており、操作可能であることを確実にします。
- 地域社会へのコミュニケーションチャネルを確立し、ハザード、必要なコンティンジェンシー対応、および緊急対応要件に関する情報を提供します。

付録Ｅ：非エンジニアのための工学と コントロールの基本的概念

STPA HANDBOOKの初期の草稿をレビューした際、私たちはすべての読者が持っているとは限らない工学のバックグラウンドを前提としていたことに気づきました。STPAおよびCASTのユーザーは、必ずしも工学の訓練を受けているとは限りません。この付録では、このハンドブックの一部のユーザーに馴染みのない工学の基本的概念を紹介します。

私は、読者が興味のあるセクションを選ぶことができるよう、この付録の中のセクションを独立させてみることにしました。以下のトピックについて述べる上で、特定の教育バックグラウンドは想定していません：

- 「システム」とは何か？
- システムエンジニアリングの基本的概念と用語
- 工学における「コントロール」の概念
- システム理論vs.複雑性理論

「システム」とは何か？

このハンドブックのすべての根底にある最も基本的な概念は、システムの概念です。

> システム：共通の目的や目標を達成するために全体として作用する一連のもの（システムコンポーネントと呼ばれる）。

システムの定義の中には、「目的」または「目標」を除外し、本質的にシステムと統合された全体を形成する、接続された一連の物または部品であると述べているものもあります。この定義は、「システム」という用語の通常の使用方法を踏まえていません。靴、星、機関車はシステムの一連の物あるいは一連の潜在的部品ですが、ほとんどの人はこれをシステムとは通常考えていません。これらの個々の物を一緒に考えるために「目的」も考慮するならば、それはシステムとして考えることができます。「目的」はシステムという概念の基本であります。

他の定義では、システムのコンポーネントが相互依存関係にあるか、接続されているか、相互作用していなければならないと述べられていますが、そうした条件はシステムを構築するために実際に必要なものではありません。また、これらの条件は、システムとして通常考えられている物を除外する形で、定義を制限してしまいます。システムコンポーネントは、直接的または間接的に相互に接続しており、後者の場合は、システムの目的のみの接続、および、様々なタイプの間接的な相互依存関係を含みます。

この定義の結論は、「目的」や「目標」はシステムにとって基本的なものであるということです。しかし、システムを定義し捉えるには異なる「目的」があるかもしれません。このセクションではさまざまな点を説明するために空港を取り上げます。旅行者にとっては、空港の「目的」は、他の場所への航空輸送を提供することでしょう。地方自治体または州政府にとっては、空港は政府の歳入および空港地域における経済活動を増やすための手段となるでしょう。航空会社にとっては、空港の「目的」は乗客と貨物の乗降となるかもしれません。空港事業にとっては、空港の「目的」は製品やサービス販売相手として顧客を引き付けることに違いありません。したがって、システムについて話すときは、考慮するシステムの「目的」を必ず特定する必要があります。

システムとは抽象化されたもの、すなわちそのシステムを見る人が捉えたモデルである。

システムを見る人は、設計者とは異なるシステム目的を捉えたり、さまざまな関連特性に焦点を当てたりすることがあります。システムの「目的」を含む仕様は、システムエンジニア

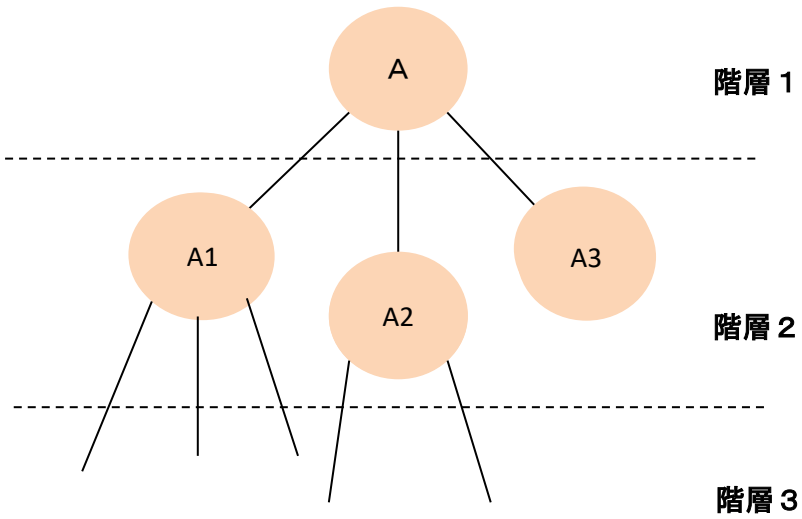
リングにおいて非常に重要です。仕様は、システムを設計、使用し、あるいは見る人々の間でそのメンタルモデルの一貫性を保証し、コミュニケーションを強化します。１つの「空港」システムには空港のさまざまなコンポーネントが含まれていることを考えてみてください。例えば航空会社の視点から空港を見ると、乗客のチェックインカウンターや飛行機のタラップ、誘導路があります。一方、商業的に見ると店舗や顧客があります。これらは、人間の心によって実際の物理世界に置かれたモデルまたは抽象化されたもの、すなわち、システムは見る人の目の中にあることに再度注意してください。あらゆる「空港システム」あるいはサブシステムにおいて考慮されるコンポーネントと、システム全体の中でコンポーネントが果たす役割は、空港システムまたは空港サブシステムの各コンセプト（モデル）ごとに異なる場合があります。ここでの基本的な考え方は、あるシステムのモデリングと分析を行う人々は、考慮するシステムの「目的」または「目標」を特定し合意しなければならないこと、およびシステムのこれらの側面は、システムを見る人々が現実世界の事物に投影する抽象物またはモデルであるということです。

設計された（人工の）システムの場合、システムを見る人々はシステムの「目的」を設計者が意図したものと異なる形で解釈することもあるが、システムの「目的」は通常、システムが作られる前に特定されています。自然のシステムでは、動作はシステムを見る人によって意図的に解釈されることがあります。

システムの概念の根底にはいくつかの基本的な前提があります：

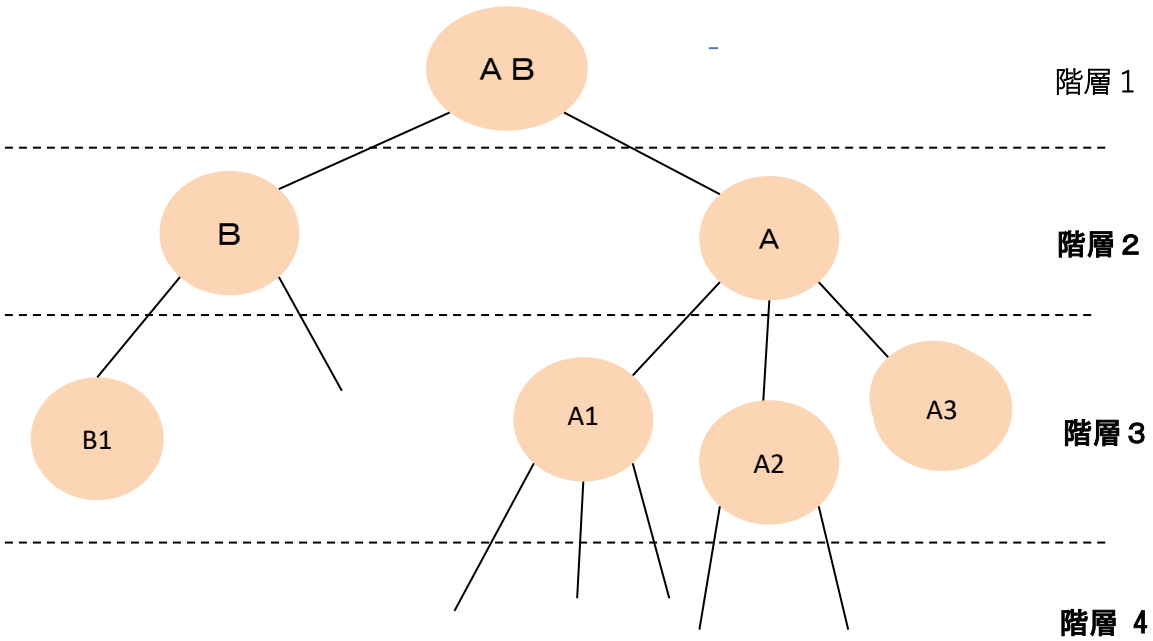
- システムの「目的」は定義することができる。
- システムは原子的である。つまり、相互作用が直接的か間接的かにかかわらず、コンポーネント間で相互作用の関係を持つコンポーネントに分けることができる。

システムそのものは、より大きなシステムの一部であっても、サブシステム（全体システムのコンポーネントと見なされる）に分割されてもよい。ここでの定義は、数学とコンピュータサイエンスにおいて「再帰的」と呼ばれるものであることに注意してほしい。つまり、定義はそれ自体でなされます。システムは通常、より大きなシステムの一部であり、サブシステムに分割することができます。図E. 1は、Ａと名付けられたシステム（例えば、「空港」システム）および３つのサブシステム（各サブシステム自体も、システムとして考えられる）について、典型的な抽象階層を示しています。



図E. 1：抽象システムＡは、３つのサブシステムで構成されているとみなすことができる。各サブシステム自体がシステムである。

図E. 1は接続図ではありません。階層的に抽象化したものであり、異なる階層で抽象化したものあるいはモデリングにおける、システムの異なるビューを示しています。階層１は、システム全体を想定しています。階層２は、システムを３つのサブシステムで構成されているものとして視覚化してします。図E. 2は、Ａ自体がより大きなシステムＡＢの一部である場合の抽象化を示しています。



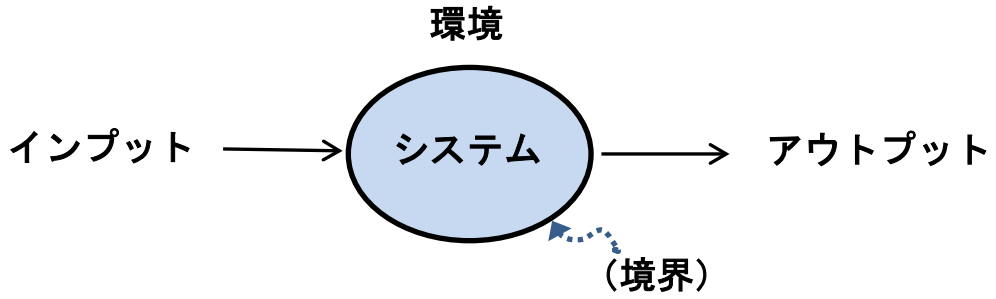
図E. 2：システムＡはより大きなシステムＡＢのコンポーネント（サブシステム）とみなすことができる

システムの定義の再帰的な性質は重要です。なぜなら、多くの人々が「システムオブシステムズ」はシステムとは異なる扱いをしなければならないと述べているためです。実は、一般的なシステムエンジニアリングと分析の手法および技術は、すべてのシステムに適用可能です。「システムオブシステムズ」は、システム理論で定義されているシステムの定義を使用する場合、およびその概念が工学において使用される場合には、単なる「システム」です。複数のシステムを組み合わせると、システムオブシステムではなく、まったく新しい独自のシステムが得られます。これは、いくつかのシステムの合計ではありません。

システムには状態があります。状態とは、任意の時点におけるシステムを記述する関連特性の集合です。航空輸送システムと見なされる空港の場合、状態の特性とは、航空機が停まっている特定のゲートにおける乗客の数であり、彼らが何をしているか（乗客の搭乗、タキシング、離陸または着陸）であると言えます。関連する状態のコンポ—ネントは、システムとその環境との境界がどのように引かれるかに依存します。

環境は通常、システムの一部ではなく、その動作がシステムの状態に影響を与える可能性のある一連のコンポーネント（およびその特性）として定義されます。したがって、システムは特定の時点における状態を有し、環境も状態を有します。 環境という概念は、システムとその環境との間に境界が存在することを意味します。ここでも、この概念はシステムを見る人によって生み出された抽象的なものであり、物理的境界である必要はありません。

何がシステムの一部あるいは環境の一部であるかは、その特定のシステムとその時点でそのシステムがどのように使用されるかに依存します。



システムの入力と出力はシステムの境界を横断します。この概念は通常、*オープン・システム*と呼ばれます。*クローズド・システム*（入力と出力がない）という概念もありますが、この概念は、私たちがシステムの安全において最も関心のある設計されたシステムとはあまり関連性がありません。

工学における「コントロール」の概念

コントロールの概念は、システムの構想、設計、および運用において重要です。システムはその動作を何らコントロールすることなく機能すると考えられますが、望ましくない悪影響が生じないように目的達成の方法を制限しながら、同時にシステムがその目的を満たしていることを確実にするのは困難です。

コントロールは工学、特に複雑なシステムの基本です。エンジニアは、生き物ではなく、何らかの目的を達成するために作られた人工物を扱っています。例えば自動車、ダム、航空機、化学プラント、宇宙船、洗濯機、ロボットなどです。それらが自力で動かないもの（橋のように）ではない場合、それらの状態に関して、動きを操作またはコントロールする必要があります。

非エンジニアは、「コントロール」という言葉を工学で使用されるのとは違う方法で解釈することがあります。コントロールとは、個々人が特定の役割と手続きを遵守するようある種の軍事的スタイルの権限によって強制するものではありません。むしろコントロールはここでは非常に広い意味で使用されており、インターロックやフェイルセーフ設計などの設計管理、保守や製造手順などのプロセスコントロール、あるいは文化、インセンティブ構造、個人の自己利益といった社会構成物を通じてなされます。何らかの形のコントロールを課さなければ、システムの目的と制約を確実に達成することはできません。

コントロールとして機能するシンプルなデザイン機能は、複雑さとコストを増加させることなく安全性を向上させることができますが、通常は設計プロセスの早い段階で安全性を検討する必要があります。デザインを通して安全性を高める最も効果的な方法は、危険な状態を排除する設計を用いることです。次善策は、危険が稀で、発生した場合も取り扱いが容易であるように設計することです。結果として生じる被害を最小限に抑えることによって危険の発生に対応する設計は、ハザード制御の最も望ましくない形態であることは明らかですが、そのようなコントロールを含める必要はしばしばあります。

コントロールループは、結果としてコントロールの唯一の形態です。「Engineering a Safer World」はそのことを強調しています。なぜならば、私の前著「Safeware」で、安全のための基本的な設計のその他の側面を広範にカバーしていたからです。さらに、システム

理論はコントロールループまたは能動的コントロールの概念を強調しています。本付録では安全設計技術を教えることはできませんが、受動的コントロールと能動的コントロールの区別のようないくつかの基本的な概念は、一般的な安全設計技術の理解に役立つでしょう。

安全を「コントロールする」には、３種類の設計手法があります。１つ目は、本質的に安全な設計を採用することです。本質的に安全な設計は、懸念されるハザードを生じさせない設計です。例えば、爆発を引き起こすのに十分なエネルギーを有さないようなシステム設計とする方法が考えられます。潜在的に有害な物質の使用に懸念がある場合、毒性のない代替物質を使う方法が考えられます。通信ネットワークを介して情報が失われる恐れがある場合、可能であればより直接的な通信を使用する方法が考えられます。

本質的に安全な設計が不可能な場合、受動的なコントロール機構を使う方法がある。受動的コントロールは能動的アクションを必要とせず、その代わりに重力のような基本的な物理的原理を用います。明白なコントロールアクション無しにシステムが危険な状態に入ることを防止する物理的なインターロックは、受動的なコントロール機構です。以下のような例があります：

- 誰かが近づいた場合にロボットや危険な機械の電源を遮断する感圧マットやライトカーテン
- バルブのターンオフとターンオンの正しいシーケンシングを確実にする、または、２つのバルブを同時にオンまたはオフにしないようにする物理デバイス
- ブロック内の水が凍った場合、シリンダに亀裂を生じさせず、拡張してプラグを押し出す自動車のエンジン冷却システムの凍結プラグ
- 過度の熱が発生し、水が所定のレベル以下になると露出するボイラーの可溶性プラグ。その場合、プラグが溶け、開口部が蒸気を逃がし、ボイラー内の圧力を低下させ、爆発を防止する。
- 一定限度以上の速度超過を防ぐ調速機や、圧力を危険レベル以下に保つリリーフ弁

受動的コントロールは、システムが本質的に安全な状態になるように設計されることが多い。事実、航空機の安全に対する基本的なアプローチは、システムをフェイルセーフになるよう設計することです。フェイルセーフ設計は以下のような例があります：

- （信号装置をコントロールする）ケーブルが破損した場合、アームが自動的に停止位置に落ちるように重力を利用した旧型の鉄道信号装置。
- 空気圧によってオフ位置に保持されるエアブレーキ。 ブレーキラインが破損すると、空気圧が失われ、自動的にブレーキがかかる。
- オペレータが継続的に圧力をかけるデッドマンスイッチ。オペレータに何かが起こり、圧力が加えられていない場合、システムは安全な状態になる。
- バラストが磁石によって適所に保持されているバチスカーフ（深海探査艇）。電力が失われた場合、バラストは解放され、バチスカーフは表面に上昇する。
- 隣接するコンポーネントに影響を与えないように、故障の影響（航空機エンジンが故障したときにファンブレードが排出されるなど）が含まれた設計

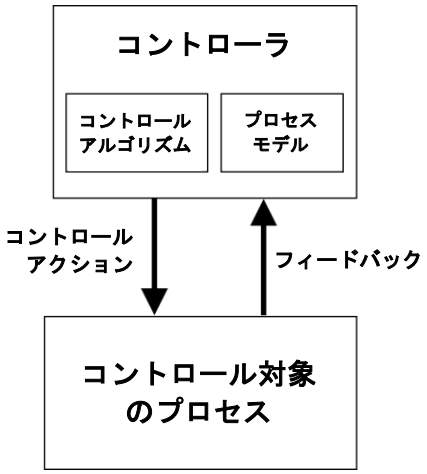
対照的に、*能動的コントロール*は、危険な状態を検出して修正することを必要とします。今日の能動的コントロールにおいては、多くの場合、コンピュータの使用と、このハンドブック全体で記述され使用されている基本的なコントロールループが含まれています。たとえば、障害や危険な状態が検出されないか、検出されても修正されないか、または損失を防ぐために時間内に修正されないなど、能動的コントロールには誤りがある可能性があることに留意してください。受動的コントロールは、通常、物理的な原理やよりシンプルな設計に依存するため、能動的コントロールよりも信頼性は高いです。一方で、能動的コントロールは、信頼性の低い検出および回復機構と、通常ははるかに複雑な設計に依存します。しかしながら、受動的コントロールは、設計自由度の点でより制約を受ける傾向があり、複雑なシステムでは常に実現可能とは限りません。

能動的コントロールには通常、コントロールループが存在します。

コントロールループとは何か？

コントロールシステムは、コントロールループを使用して他の機器またはプロセスの動作を指令、指示、または規制します。このようなコントロールシステムは、ボイラーを制御するサーモスタットを使用する単一の家庭用加熱コントローラから、複雑なプロセスおよび機械をコントロールするために使用される大型の産業用制御システムにまで及びます。

非常に基本的なコントロールループを以下（およびこのハンドブックの他の箇所）に示します：



プロセスをコントロールするためには、コントローラは、コントロール対象のプロセスの動作に対する制約を維持することを含む、１つまたは複数の目的を持たなければなりません。さらに、コントローラは、コントロール対象のプロセスの動作、すなわちコントロール対象のプロセスまたはシステムの状態に影響を及ぼす何らかの方法を持たなければなりません。これらは図中で、コントロールアクションとして示しています。工学では、コントロールアクションは*アクチュエーター*によって実装されます。どんなコントロールアクションが必要であるかを知るために、コントローラはシステムの現在の状態を判定できなければなりません。工学用語では、システムの状態に関する情報は*センサ*によって提供され、*フィードバック*と呼ばれます。最後に、ハンドブックの他のパートでも説明しているように、コントローラにはコントロール対象のプロセスの状態のモデルを含まなければなりません。

一例として、単純なサーモスタットは、温度を特定の範囲内に維持するという目的を有しています。フィードバックは、コントロール対象のプロセスの現在の状態、この場合は室内の空気の温度に関する情報をコントローラに提供します。フィードバックは、コントローラのプロセスモデルを更新するために使用します。環境情報（外気温度）や自然温度の変動に関する基本情報などの他の情報が、プロセスモデルの一部である可能性もあります。コントローラは、プロセスモデルを使用して、どのようなコントロールアクションを提供するかを決定します。例えば室温（コントロール対象のプロセス）の状態を調整し必要な範囲内に維持するために、温風または冷風を適用します。

コントロールループには一般的に、フィードバック制御とフィードフォワード制御の２つの動作モードがあります。 *フィードバック制御*は、上記の段落で説明したものです。 運転するとき、ドライバーは速度計（フィードバック）を読み取り、自動車の速度を自分が望む水準に保つためにブレーキあるいはアクセルを踏むことを決定します。

*フィードフォワード制御*の一例は、運転者が坂道に近づくときに発生します。ドライバーは、車が減速を開始するまで待ってアクセルを踏むことができます。しかし熟練したドライバーは、坂を上る際に一定の速度を維持するためには加速が必要であると予測し、車が実

際に減速する前にアクセルを踏みます。したがって、フィードフォワード制御では、コントローラはプロセスの現在の状態（この場合は車の速度）のモデルと、（傾斜上で動作している）将来のモデルを使用し、必要性を特定する明確なフィードバックなしでコントロールアクションを提供します。

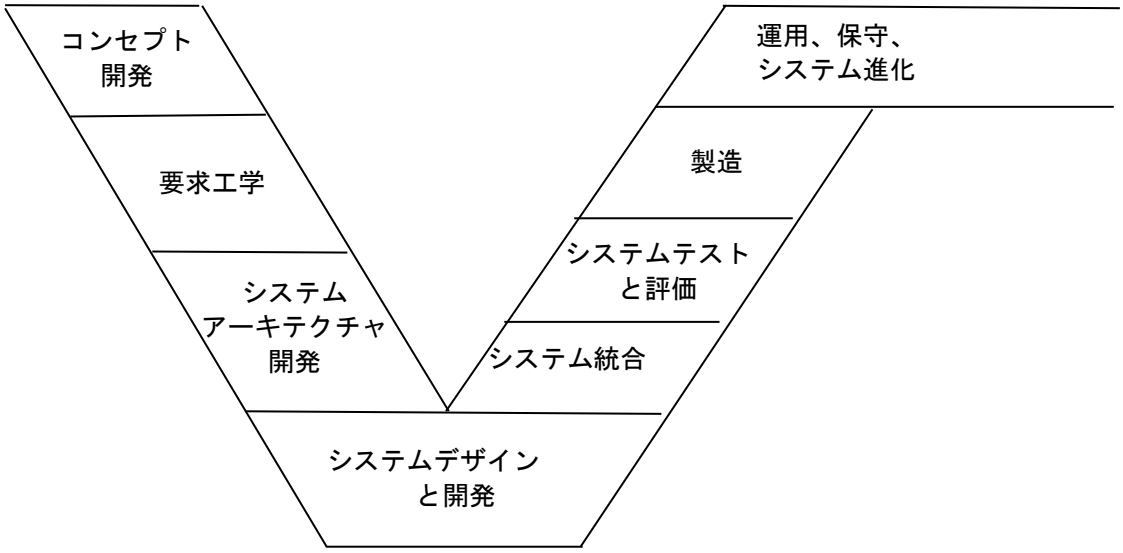
多くの場合、フィードバックとフィードフォワード制御は並行して使用します。この例では、ドライバーはフィードバックを受け取る前にアクセルを踏む必要があると、フィードフォワード制御を使用して予測します。しかしフィードフォワード計算が完璧ではない場合、フィードフォワード・コントロールアクションを調整して傾斜上で一定速度を保つためにフィードバックも使用されます。

システム理論に基づくコントロールの工学的概念は、社会システムや組織システムにも適用することができ、経営理論や社会科学で広く使われています。

システムエンジニアリングとは何か？

システムエンジニアリングとは、設計作業の結果を向上させるために設計に構造を与え、システムを構築する試みです。比較的シンプルなシステムであれば、システムエンジニアリングは必要ないかもしれません。システムエンジニアリングは第2次世界大戦後に生まれました。より複雑なシステム、特にミサイルやその他の防衛システムの構築が始まった頃です。またその頃人々は、非公式な設計や構築プロセスでは、システムに想定された「目的」を満たすようなシステムは構築できず、潜在的な行動に対する制約、すなわち目的達成の制約になることに気づきました。構造化されたプロセスの欠如は、プロジェクトの遅れと予算の超過にもつながりました。

システムエンジニアリングは大きなテーマですが、このハンドブックを理解するのに必要なのは２つの概念のみです。１つ目は、システムエンジニアリングのフェーズとプロセスの概念です。これらのフェーズの最も基本的なモデルを図E. 3に示します。



図E. 3：基本的なシステムエンジニアリングの「Ｖモデル」

このモデルはＶモデルと呼ばれますが、さまざまな要素に異なる名前が付けられることがあります。場合によってはフェーズが直線で描かれることもありますが（直線が下に傾いている場合は「ウォーターフォール」モデルと呼ばれる）、表記方法を除いて違いはありま

せん。基本的な考え方は、構造化されたプロセスが使用される場合には、最良の結果が得られるというものです。そこではシステム概念が最初に開発され、システムの基本的な目的と制約が定義されます。開発の初期段階では、手戻りを防ぐためにさまざまな実現可能性やその他の分析が行われます。要求工学が、通常、プロセスの次のステップであり、事前に合意された基本的な目的と制約を考慮して、システムの詳細な要求が開発されます。システムアーキテクチャ開発とは、詳細な設計と開発を行う前に、システムの基本アーキテクチャまたは上位レベルを設計することを意味します。「V」の左側は、基本的な設計プロセスを表します。

Vの右側は、保証と製造を行う開発の後半段階を示しています。図E.3で示すように、システムの運用も含まれる場合があります（したがって、ライフサイクル・モデルと呼ばれます）。Vモデルプロセスの右側では、設計および構築されたさまざまなコンポーネントが統合され、テストおよび評価フェーズに進みます。その後製造され、運用されます。

上記の図は、乱雑さを減らすために意図的に簡略化しており、総括的なプロセス要素のみを反映しています。フェーズ間では常に多くの行き来があり、１つの直線プロセスではありません。たとえば、設計プロセス自体が、解決する問題をより深く理解し、元の要求と制約を追加または変更する結果となるため、要求は当初、完全には特定されません。開発中に深刻な問題が発生すると、プロジェクトが完全に前の段階に戻る必要が生じることがあります。しかし全体的には、この段階的なプロセスに則って進められます。

さらに、このモデルは文字どおり理解されるべきではありません。フェーズの名前付けはフェーズが並行して進行するのが不可能であることを意味するものではなく、実際には一般的に並行して進行します。例えば、すべてのテストが行われるのを最後まで待っているのは、プロジェクトにとって非常に大きなリスクです。様々な種類のテストは、最も初期の概念フェーズから（おそらく、シミュレーションやプロトタイプの形で）始まり、通常は各フェーズで継続して行われます。また、設計中のシステムのタイプに応じて、様々な名前が各フェーズに付けられます。目的とは単に、特定のプロジェクトのさまざまなニーズに合わせて調整される構造化プロセスを定義することです。

事故調査官やアナリストが理解するために、これらすべてが必要なのは、なぜでしょうか？事故は運用中に発生しますが、事故につながる設計上の欠陥は開発中に発生します。B737 MAXの問題は、パイロットを単に非難することが不可能な場合（人々は非難を試みましたが）の例です。事故調査は、なぜ損失につながった設計上の欠陥が導入されたのか、および、なぜそれらがシステムの運用使用前に識別されなかったのかを特定する必要があります。今後、システムの複雑さが増して、設計上の欠陥が事故の重要な要因になるにつれて、事故の原因を工学や開発に遡って追跡することがますます重要になります。なぜ事故が起きたのかを十分に理解するためには、設計上の欠陥がどこに導入されたのか、また、システムが使用される前になぜそれらが識別されなかったのかを理解する必要があります。開発プロセスには、システムが動作可能になる前に設計上の欠陥を見つけるべき多くの手順が設計されています（または少なくともそうでなければなりません）。そのような手順が有効でなかった理由を調査することは、開発プロセスにおける継続的な改善の大きな重要な要素です。

システム理論vs.複雑性理論

STAMPは複雑性理論（complexity theory）ではなくシステム理論に基づいています。システム理論に貢献してきた人々は多いですが、オーストリアの生物学者であるルートヴィヒ・フォン・ベルタランフィ（Ludwig von Bertalanffy）は、彼が一般システム理論と呼んだものの創始者の１人として認められています。ノーバート・ウィーナー（Norbert Weiner）は、数学と工学への応用を探りました。ウィーナーは自分の理論を*サイバネティクス*と呼びましたが、この用語は時間が経つにつれ消えてゆき、今日ではベルタランフィの用語が一般的に使われています。

このハンドブックなどで述べているシステム理論は、自然システムあるいは人工システムを問わず、複雑なシステムの動作を理解するために活用できる一連の原則です。*システム思考*は、システム理論の原則を適用するときに人々が何をしているかを記述するためによく使われる用語です。これらの原則は、このハンドブックの第３章で簡単に説明しています。

*複雑性理論*は1960年代にシステム理論やその他の概念から生まれ、サンタフェ研究所や同研究所の研究者との関連で通常語られています。システム理論と複雑性理論には共通点があります。それは出現（emergence）のような用語を含んでおり、コンポーネントの削減や分解ではなく複雑なシステムの動作全体に焦点を当てている点です。システム理論の基本的な要素は、出現、階層、コミュニケーション、コントロールであり、これらは複雑性理論にも含まれています。またシステム理論と複雑性理論はともに、フィードバック制御とフィードフォワード制御、適応性、非線形相互作用、制約の概念を含んでいます。どちらもシステムの動作を理解するための原則として、還元主義（reductionism）または分解を拒んでいます。

しかし、大きな違いがあります。複雑性理論は自然システムを記述するために生み出されたものです。ここでは一見独立したエージェントが、我々がまだ完全に理解していない自然法則を使用して自分自身を自発的に順序付けし、また一貫したシステムに順序変更します。対照的に、システム理論は人工的に構築・設計されたシステムにより適しています。ここでは人間が何らかの工学的プロセスまたは設計プロセスを使用して意図的にシステムを構築します。基本的な設計は既知であり、変更はコントロールされています。

もう一つの大きな違いは、システム理論はすべてのシステムを創発した動作を表すものとして捉えている一方、複雑性理論はシステムを単純（Simple）、込み入った（Complicated）、複雑（Complex）、カオス （Chaotic）の４つのタイプに、出現の度合いやタイプによって分けていることです。

このように、システム理論は設計されたシステムに最も適しているようです。一方、複雑性理論は、天気などの設計が不明な自然システムや、設計がなされておらず秩序が欠如しており創発した動作を予測することが困難あるいは不可能な、コミュニティなどの社会システムに最も適しています。複雑性理論は、設計はできないが、しかし発生したときに経験と学習を行わなければならないような動作を扱います。

少なくとも私にとっては、システム理論の方が複雑性理論よりも理解し使用するのが容易です。複雑性理論の枠組みは、適用および理解が困難で混乱する可能性があり、安全性およびシステムのその他の創発特性を向上させるという工学の目的には過剰である可能性があります。したがって、STAMPの基礎としてはシステム理論が選択されました。