

製品／サービスの安全・安心とその監査保証
米国大手航空機メーカーの組織事故事例からの教訓
Safety and security of products / services and its audit and assurance
-Warning from organizational accident of major US aircraft manufacturer

2021年6月11日

システム監査学会 IT監査保証の判断基準研究プロジェクト

株式会社 東芝 牧野博文

ITストラテジスト,システム監査技術者,RISS,ITCA,CISA

STC advanced, IoTExpert(MCPC)

この資料の内容は発表者個人及び研究プロジェクトメンバーの見解です。
発表者個人及び研究プロジェクトメンバーの所属組織等とは関係ありません。

IT監査保証の判断基準研究プロジェクトメンバー

主査; 松尾 明 (公認会計士, 公認情報システム監査人, TOGAF9認定アーキテクト)

※ 五十音順

メンバー名	所属など
石島 隆	法政大学経営大学院教授
遠藤 正之	静岡大学情報学部教授
杉山 哲男	コタエル信託(株) CIA, CISA
鈴木 夏彦	日本電気(株) システム監査技術者, CIA, CISA
成田 和弘	三菱UFJトラストシステム(株) システム監査技術者, CIA, CISA
牧野 博文	(株)東芝 システム監査技術者, ITストラテジスト, RISS, ITC, CISA, IoTエキスパート
水野 英治	システム監査人事務所イレブンス システム監査技術者, 公認システム監査人(CSA), MBA
米川 弘幸	日本年金機構 システム監査技術者, CIA, CISA

Agenda

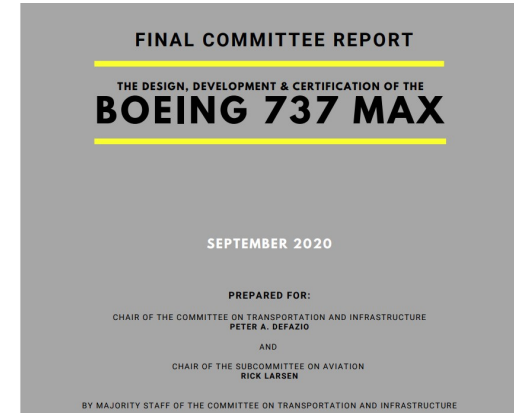
- 事故概要
 - インドネシア運輸安全委員会最終報告書 (Komite Nasional Keselamatan Transportasi, KNKT)
 - エチオピア事故調査局報告書 (Ethiopian Accident Investigation Bureau)
- 米国下院運輸インフラ委員会最終報告書および連邦地裁起訴猶予合意 (DPA)内容からの分析
 - スイスチーズモデルを用いた組織事故分析
 - 組織事故と安全文化の醸成
 - 高信頼性組織 (HRO)の研究
 - IAEAの安全文化向上のプロセス
 - 安全文化で重要とされる8 つの要素について

要旨

2018年10月、2019年3月に、インドネシアとエチオピアでそれぞれ新型旅客機の「737MAX」の墜落事故が発生し合わせて346人が犠牲になった。墜落にソフトウェアを巡る問題があると報じられた。事故後、インドネシア政府の最終報告、エチオピアの事故報告が公表され、その後2020年に連邦議会の報告書、FAA（連邦航空局）のレビュー、2021年に連邦地方裁判所の刑事訴訟の司法取引が行われた。司法取引（起訴猶予合意）では、製造メーカー側がFAA（連邦航空局）を欺いた事を認め遺族への損害賠償を含めた25億ドルの損害賠償を行う事に至った。事故とソフトウェアに関わる問題点について、各種報告書から読み解き、ソフトウェアの信頼性と組織事故の観点で再発防止策について考察した。

737max墜落事故の概要

- 2018年10月29日
LionAir Flight 610 (JT610) が、インドネシアのジャカルタで離陸した直後に墜落。乗客乗員189人全員死亡
- 2019年03月10日
エチオピア航空302便 (ET302) が、エチオピアのアディスアベバで離陸した直後に墜落し、搭乗していた157人全員死亡
- 2020年09月15日
運輸インフラ委員会最終報告書公表
- 2020年11月18日
連邦航空局から本事案のレビュー報告書公表
- 2021年01月07日
737MAXに関する情報の隠蔽（いんぺい）で米政府を欺いたとして起こされていた刑事訴訟で、同社は決着のため25億ドル（約2600億円）を支払うことに同意
- 亡くなられた方々の御冥福をお祈りいたしますとともに、御遺族の方々へ心よりお悔やみ申し上げます。



Final Committee Report on the Design, Development, and Certification of the Boeing 737 MAX (September, 2020)
<https://transportation.house.gov/download/20200915-final-737-max-report-for-public-release>

737MAX墜落事故航路

JT610フライトパス



Figure 23: The flight track of LNI610 based on ADS-B

インドネシア運輸安全委員会 (Komite Nasional Keselamatan Transportasi, KNKT) 最終報告書 (2018年)

http://knkt.dephub.go.id/knkt/ntsc_aviation/baru/2018/PK-LQP%20Final%20Report.pdf

ET302フライトパス



出所: 外務省

エチオピア事故調査局 (Ethiopian Accident Investigation Bureau) 報告書に基づき、外務省エチオピア資料から筆者加筆

エチオピア事故調査局報告書 (Ethiopian Accident Investigation Bureau)
https://reports.aviation-safety.net/2019/20190310-0_B38M_ET-AVJ_Interim.pdf

外務省エチオピア連邦民主共和国

https://www.mofa.go.jp/mofaj/gaiko/oda/shiryo/hyouka/kunibetu/gai/ethiopia/pdfs/kn09_00_06.pdf

米国下院の運輸インフラ委員会の最終調査報告書による、主な事故原因(1/4)

1) 生産圧力 (Production Pressures)

- 競合他社との市場競争に打ち勝つため、結果的に財政的なプレッシャー
- 過度なコスト要求、生産日程遵守の強い圧力、製造ラインでの生産減少させないこと等の圧力
- 航空安全上危険性の高まる目標設定や生産現場への期待

Final Committee Report on the Design, Development, and Certification of the Boeing 737 MAX(September,2020) より筆者翻訳
<https://transportation.house.gov/download/20200915-final-737-max-report-for-public-release>

米国下院の運輸インフラ委員会の最終調査報告書による、主な事故原因(2/4)

2) 欠陥設計前提 (Faulty Assumptions)

- 重要な技術の根本的に欠陥をもたらす可能性のある設計条件の設定
- 誤った設計条件とは、特定の条件下で、自動的に機体をノーズダウン（機首下げ）させる設計
- 特定の条件下とは、2つある迎角センサ（AOAセンサ）の内の1つだけで可動する様にした設計条件
- ほとんどのケースでパイロットがシステムの存在に気づかずに（重心位置の不安定さに伴う操縦の複雑さ等の）課題を緩和する事ができるとした想定
- 安全上ミッションクリティカルなシステムであると分類しなかった事
- 独自の内部設計ガイドライン違反

※AOA：迎角センサー, Angle of Attack.

※MCAS：操縦特性補助システム, The Maneuvering Characteristics Augmentation System

Final Committee Report on the Design, Development, and Certification of the Boeing 737 MAX (September, 2020) より筆者翻訳

<https://transportation.house.gov/download/20200915-final-737-max-report-for-public-release>

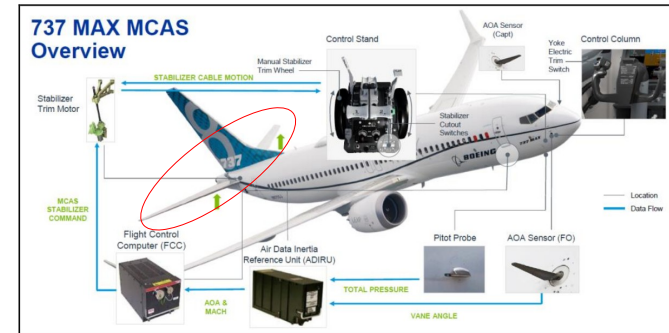


Figure 13: MCAS System configuration

インドネシア運輸安全委員会最終報告書 (Komite Nasional Keselam)
http://knkt.dephub.go.id/knkt/ntsc_aviation/baru/2018/PK-LQP%20Final%20Report.pdf



FIGURE 2: AOA SENSOR FIGURE 3: AOA LOCATION ON A BOEING 737

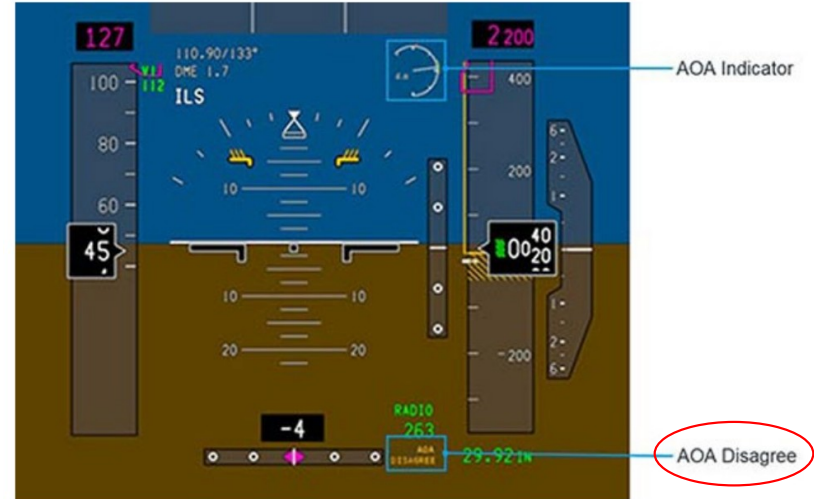
エチオピア事故調査局 (Ethiopian Accident Investigation Bureau) 報告書
https://reports.aviation-safety.net/2019/20190310-0_B38M_ET-AVJ_Interim.pdf

米国下院の運輸インフラ委員会の最終調査報告書による、主な事故原因(3/4)

3) 隠蔽文化 (Culture of Concealment)

- 連邦航空局 (FAA)、顧客及び737MAXの利用パイロットに対して重要な情報を隠蔽
- MCASシステムの存在そのものが、737MAXのパイロットに対して隠蔽
- AOA迎角不一致アラート機能の大部分が737MAXで動作不能であった事を隠蔽
- パイロットがMCASがアクティブになり起動した場合、数秒以内にその状況を分析して”スタビライザーランウェイ(水平尾翼を水平にする事)”にする事が必要な事を隠蔽

Final Committee Report on the Design, Development, and Certification of the Boeing 737 MAX(September,2020) より筆者翻訳
<https://transportation.house.gov/download/20200915-final-737-max-report-for-public-release>



cockpitのプライマリフライトディスプレイ(PFD)上のセンサ角度不一致のアラート画面

エチオピア事故調査局 (Ethiopian Accident Investigation Bureau) 報告書

https://reports.aviation-safety.net/2019/20190310-0_B38M_ET-AVJ_Interim.pdf

※AOA：迎角センサー, Angle of Attack.

※MCAS：操縦特性補助システム, The Maneuvering Characteristics Augmentation System

米国下院の運輸インフラ委員会の最終調査報告書による、主な事故原因(4/4)

4) (監督官庁との) 意見対立 (Conflicted Representation)

- FAAの利害を代表する事ができる特別な権限
- 航空機システムと設計がFAAの要求事項を満たすかどうかをFAAに代わって評価する事ができた
- 認定代表者達 (ARs)が空の安全を守るためにFAAの利害を適切に代表して活動する事ができなかった

5) 連邦航空局の監督体制における同社の影響

- FAA幹部がFAAの技術専門家の決定を覆す決定をしたとしている。
- 安全性に問題があり、FAAのレギュレーションから逸脱する可能性をFAAの技術的専門家および安全専門家が決定したが、FAAの管理者がそれらを却下し、代わりに同社を支持した。

Final Committee Report on the Design, Development, and Certification of the Boeing 737 MAX(September,2020)より筆者翻訳
<https://transportation.house.gov/download/20200915-final-737-max-report-for-public-release>

米国連邦地方裁判所の司法判断(起訴猶予合意,DPA)

DEFERRED PROSECUTION AGREEMENT, U.S. District Court

- 告発内容
 - 米国を欺くための共謀罪(Fraud Conspiracy)
- 認定された事実
 - 同社の737 MAXフライトテクニカルパイロットのうち2名は、誤解を招く記述、半真実、および省略により、MCASに関するFAA AEG※を欺いた。
 - テストパイロットの従業員不正※²として起訴猶予合意Deferred Prosecution Agreement (DPA) に至る。
- 再発防止策
 - 安全を管理する同社の方針および手順、ならびにFAAおよび他の政府機関および規制当局との相互作用を監督するために、取締役会の常設航空宇宙安全委員会を設立する。
 - 以前は全社に配置されていた安全関連機能を強化および一元化するために、製品およびサービスの安全組織を作成する。
 - すべてのエンジニア、および同社の飛行技術チームが、事業部門ではなくチーフエンジニアを通じて報告するように、エンジニアリング機能を再編成する。

※FAA AEG(連邦航空局 航空機評価グループ,Federal Aviation Administration, Aircraft Evaluation Group)

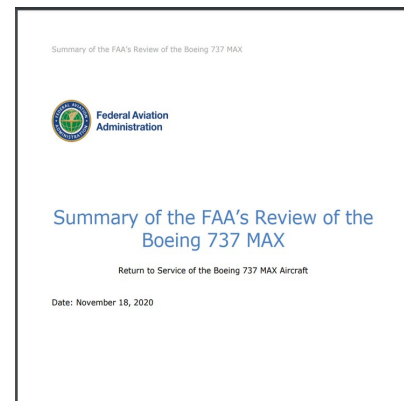
DEFERRED PROSECUTION AGREEMENT Case 4:21-cr-00005-O, January 7, 2021 KAREN MITCHELL CLERK, U.S. District Court
<https://www.justice.gov/opa/pr/boeing-charged-737-max-fraud-conspiracy-and-agrees-pay-over-25-billion>

組織事故に関する議論

- 本事案はスイスチーズモデルによる組織事故と考えられる
- 連邦地裁司法取引（DPA）では、従業員2名のFraud Conspiracy違反が認められたが組織として責任を問われていない様に見える
 - 従業員2名に明らかな違法行為があったことを認め、巨額の”和解金”の支払いに合意した
 - 今後訴訟や企業の社会的責任を果たしてゆく上で問題が発生する可能性が否定できない
- 不正のトライアングル
 - 熾烈な市場競争の最中の圧力（動機）
 - 監督官庁の品質認証を代行可能な立場にあった（機会）
 - 監督官庁の技術／安全の専門家の意見を覆した（正当化）

組織事故に関する議論

- 司法取引（起訴猶予合意）であり、今後、再発した場合の制裁が大き
く、責任も重い
- 課題として、人間である以上必ず失敗（エラー）は起こりうる、人間に
任せる完璧な対応策はないといった観点に基づいた対策を講じる必要が
あり、人間の認知など幅広い分野の研究を参考に、さらなる研究が必要
- システム開発不正に関して
 - 連邦航空局(FAA)報告書にあるようなシステム開発不正は考えにくく、
組織全体の不正（組織不正）として考えるべき（右図）
 - 要求仕様を歪めたシステム開発不正も同様に発生しており、制御シス
テムによるC S P時代の示唆を含んでいるのではないかと（時間の関係
で割愛）



Summary of the FAA's Review of the Boeing 737 MAX

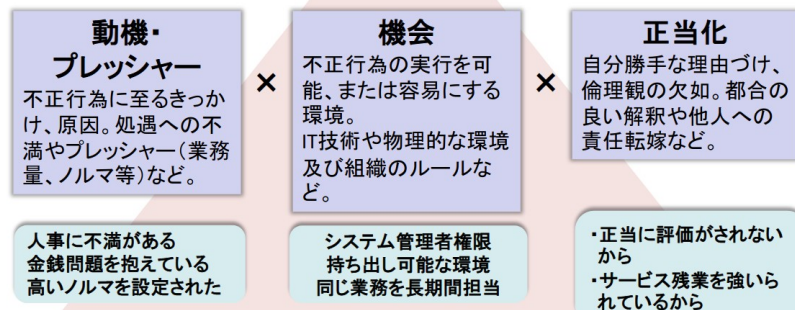
https://www.faa.gov/foia/electronic_reading_room/boeing_reading_room/media/737_RTS_Summary.pdf

不正のトライアングルとスイスチーズモデルによる組織事故

2. 内部不正の要因と対策

不正のトライアングル

- 内部不正は「動機・プレッシャー」「機会」「正当化」の3要因が揃った時に発生する



Copyright © 2015 独立行政法人 情報処理推進機構

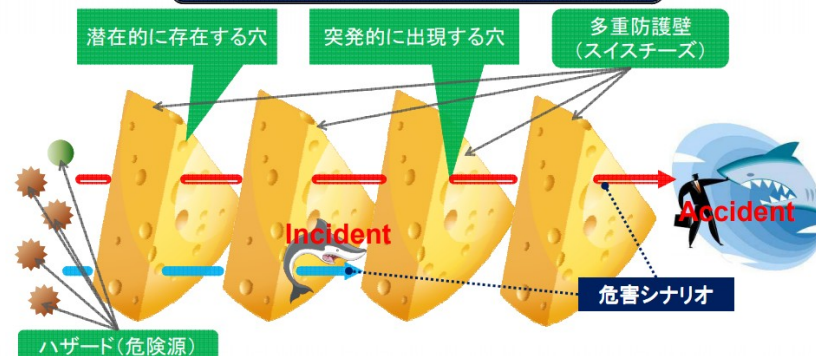
組織における内部不正対策内部不正防止ガイドライン（第3版）について（IPA,2015）

<https://www.ipa.go.jp/files/000047237.pdf>

IPA

スイスチーズモデルと危害シナリオ

James Reasonのスイスチーズモデル：
事故は多重防護壁の穴を貫通した時に生じる。



- ✓ 危害シナリオ：ハザード（危険源）からハーム（危害）に至る具体的なシナリオ（物語、筋書き）
- ✓ 事故の発生要因は多重防護壁にある複数の穴
- ✓ ヒヤリハットは一部の多重防護壁の穴を突破したが、人的被害が無傷であった危害シナリオ

8

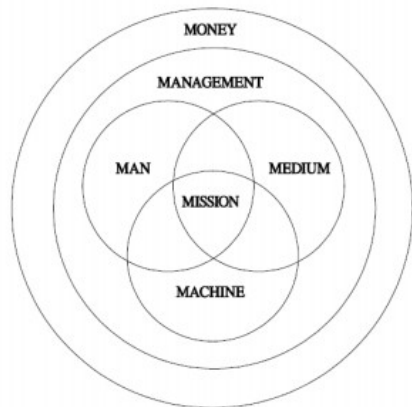
nite

N I T Eが選ぶ、製品事故の未然防止に向けた、典型的な危害シナリオ（独立行政法人製品評価技術基盤機構）

<https://www.nite.go.jp/data/000005695.pdf>

15

スイスチーズモデルを用いた事故の考察

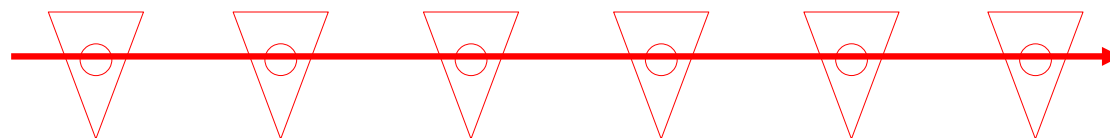


事故の再発防止に資する事故調査のあり方（国土交通省）

<https://www.mlit.go.jp/jtsb/>

fukuchiyama/kensyou/fu04-finalreport-part2-2.pdf

- 国土交通省の事故再発防止に資する事故調査のあり方（6 M）を元に、報告書原因をスイスチーズモデルとしてマッピング
- 6つのMにおいて全て当てはまる事を確認



①Money (財務状況や安全投資) ②Mission (経営理念や目標) ③Management (管理系) ④Media (環境系) ⑤Machine (機械系) ⑥Man (人間系)

1)生産圧力 1)生産圧力 1)生産圧力 2)隠蔽文化 3)欠陥設計 4)評価の代行 5)監督官庁意見を覆した

組織事故対策としての安全文化の醸成

- ジェームズリーズン(James Reason)「組織事故」,1997
 - 報告する文化
 - 公正な文化
 - 柔軟な文化
 - 組織の柔軟性とは変化する要求に効率的に適用できる文化をもつ事である
 - 高信頼性組織では中央集権型の管理から権力分散型の管理に切り替える能力がある
 - 学習する文化

エラーマネジメントの過去と未来～ヒューマンエラーから組織事故、そしてレジリエンス・エンジニアリングへ～（立教大学,芳賀繁,2016）
https://www2.rikkyo.ac.jp/web/haga/files/electrical_review_2016.pdf

高信頼性組織 (HRO)について

- 高信頼性組織に関する研究も行われている

高信頼性組織(HRO)とは

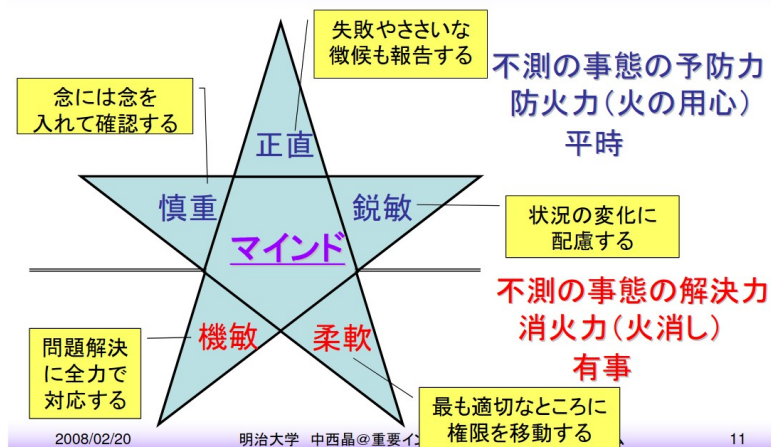
- HRO=High Reliability Organization
 - 複雑な技術システム
 - 関与者のさまざまな要求
- システムを動かす人も全体についての完全な理解が困難
 - 小さなミスやトラブルが重大な結果につながる危険性
- 不測の事態の“過剰”に直面
 - しかし、高い信頼性・安全性を維持

2008/02/20

明治大学 中西晶@重要インフラ情報セキュリティフォーラム

6

高信頼性組織のプロセス



2008/02/20

明治大学 中西晶@重要インフラ情報セキュリティフォーラム

11

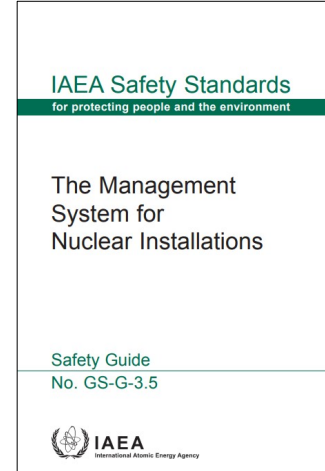
重要インフラ情報セキュリティフォーラム 重要インフラに求められる高信頼性組織の条件 (2008/02/20明治大学 中西晶)

https://www.jpccert.or.jp/present/2008/20080220MEIJI-Nakanishi_sama.pdf

18

スイスチーズモデルによる組織事故分析から高信頼性組織（HRO）へ

- IAEAでは、原子力プラントの安全文化の向上のプロセスが定義されている。
 - (a) 経営者のコミットメントを獲得する
 - (b) 安全文化の共通認識を構築する
 - (c) 望ましい安全文化を記述する
 - (d) 既存の文化のアセスメントを実施する
 - (e) 組織評価結果をすべての組織人員に通知する
 - (f) 改善のために、ギャップ、根本原因とキーとなるイニシアティブを明確にする
 - (g) 組織の目標を伝えて、管理者と従業員のコミットメントを得る
 - (h) 変更を実施する
 - (i) 安全文化の指針となる原則が受け入れられた業務になる事を確実にする
 - (j) 変更を継続する
 - (k) フォローアップアセスメントを実施する



International Atomic Energy Agency
(2009) Management
The System for Nuclear Installations. IAEA
Safety standards series No. GS-G-3.5,
IAEA, Vienna. (P10)
https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1392_web.pdf
より筆者翻訳

安全文化に重要な 8 つの要素と評価

- 安全文化で重要とされる 8 つの要素
 - トップマネジメント
 - 組織統率
 - ミドルマネジメント
 - 資源管理, 業務管理
 - 現場
 - 危機認識, 動機付け, 学習伝承
 - トップをはじめ現場に至る各構成員
 - 積極関与
 - トップから現場に至る組織内および事業所外とのコミュニケーション等
 - 相互理解

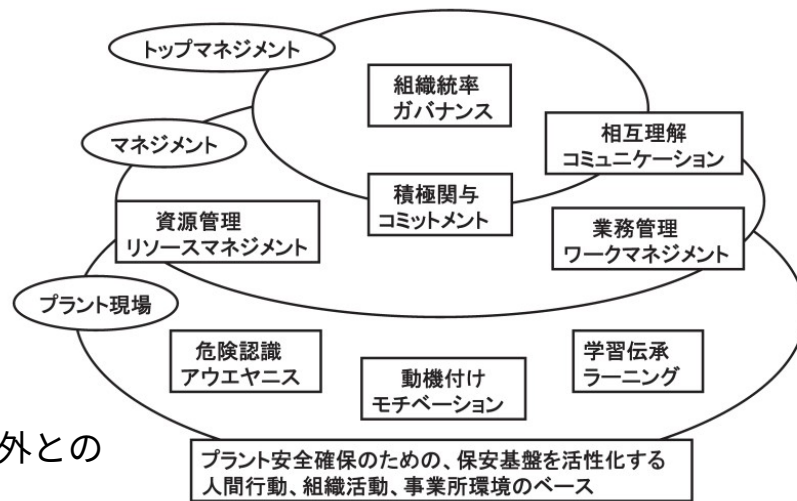


図4 安全文化のイメージ

安全文化を考慮した産業保安のあり方（安全工学、2010 年 49 巻 4 号 p. 205-211, 田村昌三, 2010年）

https://www.jstage.jst.go.jp/article/safety/49/4/49_205/_article/-char/ja

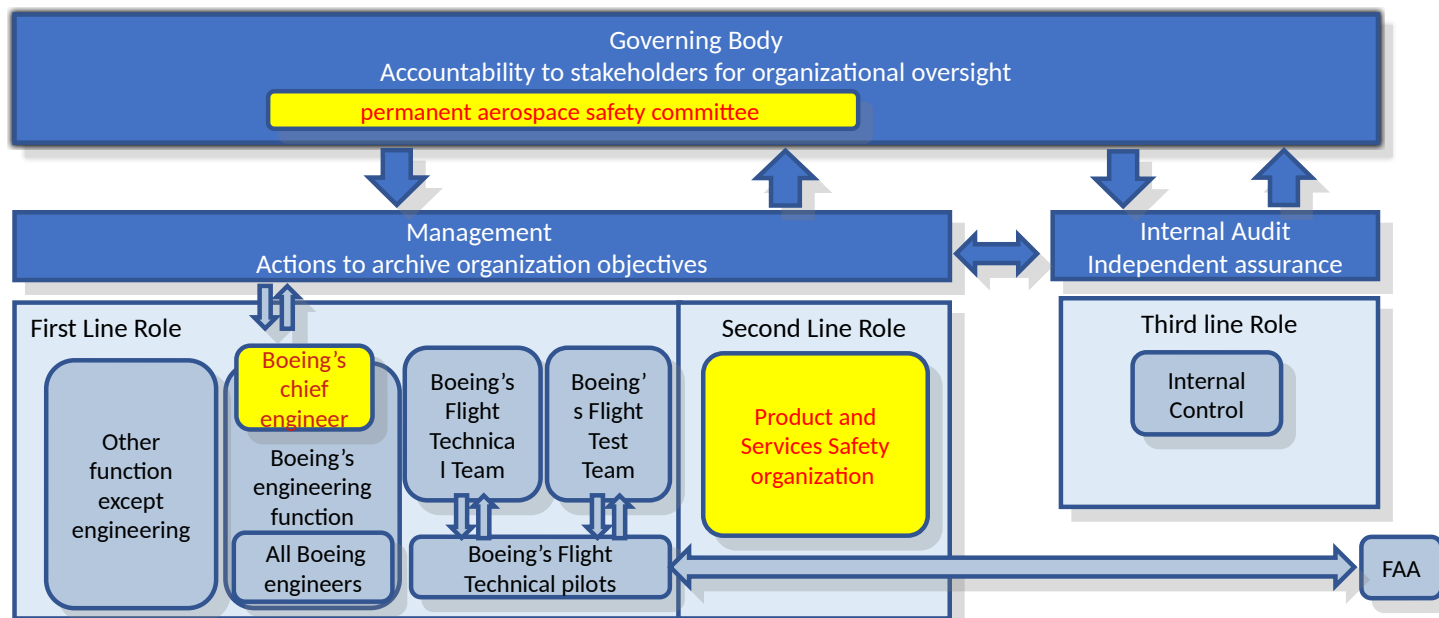
IAEA安全文化向上プロセスとのマッピング

- 現時点で確認できるのは、（a）経営者のコミットメントのみと考えられる。

No	IAEAの安全文化向上のプロセス	連邦地裁の再発防止計画	安全文化の8つの要素（田村,2010）							
			組織 統 率	積 極 関 与	相 互 理 解	危 険 認 知	学 習 伝 承	業 務 管 理	資 源 管 理	動 機 付
1	(a) 経営者のコミットメントを獲得する	取締役会の常設航空宇宙安全委員会 製品および安全組織の統合と強化 チーフエンジニアを通じた報告	X					X		
2	(b) 安全文化の共通認識を構築する									
3	(c) 望ましい安全文化を記述する									
4	(d) 既存の文化のアセスメントを実施する									
5	(e) 組織評価結果をすべての組織人員に通知する									
6	(f) 改善のために、ギャップ、根本原因とキーとなるイニシアティブを明確にする									
7	(g) 組織の目標を伝えて、管理者と従業員のコミットメントを得る									
8	(h) 変更を実施する									
9	(i) 安全文化の指針となる原則が受け入れられた業務になる事を確実にする									
10	(j) 変更を継続する									
11	(k) フォローアップアセスメントを実施する									

起訴猶予合意で示された組織体制の安全強化対策

- 取締役会に航空宇宙安全委員会 (Permanent Aerospace Safety Committee)を設置
- 製品サービスの品質部門(Product and Services Safety Organization)を強化

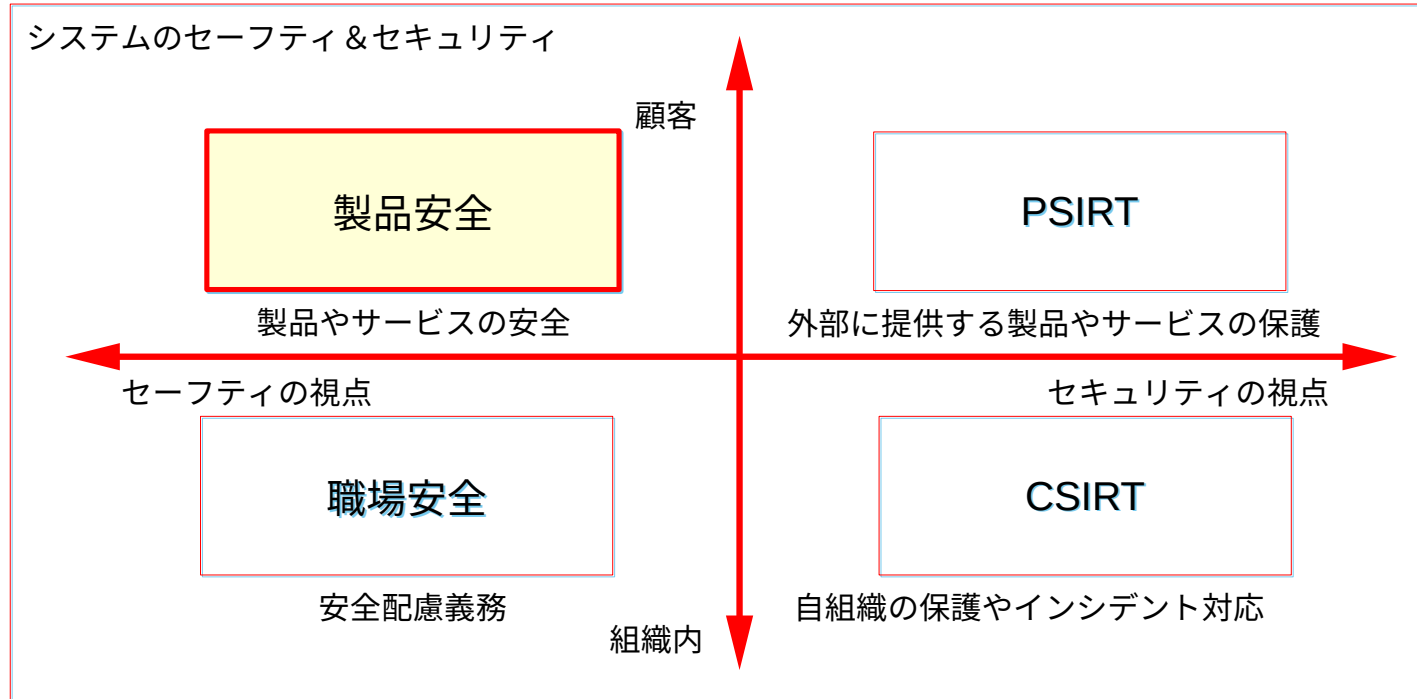


DEFERRED PROSECUTION AGREEMENT Case 4:21-cr-00005-0, January 7, 2021 KAREN MITCHELL CLERK, U.S. District Courtより筆者作成
<https://www.justice.gov/opa/pr/boeing-charged-737-max-fraud-conspiracy-and-agrees-pay-over-25-billion>

22

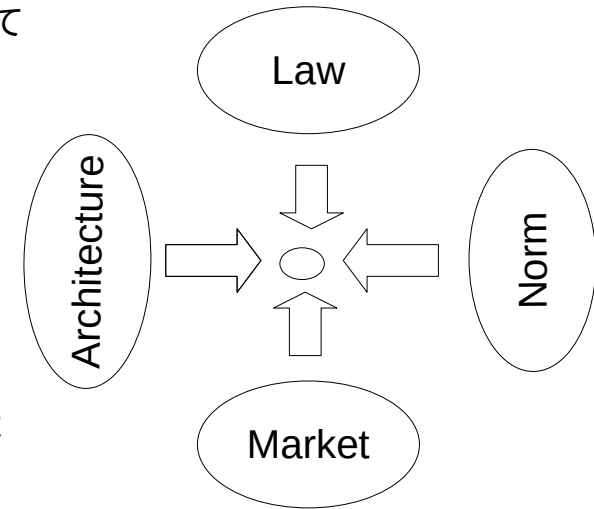
常設航空宇宙安全委員会の設置に関する考察

取締役会の安全委員会の設置による製品安全の経営者のコミットメントの強化



ソフトウェアによる安全文化の評価の検討

- 従業員2名の不正が共謀罪(Fraud Conspiracy)違法行為として認定された。
- 同社は、司法取引前に社会的制裁を受けた
 - 内部告発やメディアから倫理上の批判
 - 株価や債権者等市場からの改善要求
- 組織体にとって、司法判断以外のみに依拠するのではなく、Code(ガイドライン)、市場(Market)、倫理(Norm)によるリスク対策、ガバナンスが必要になるのではないか
- 違法性のみで捉えるのではなく、ソフトウェアや倫理、市場の状況から予見可能性を踏まえた監査保証の判断基準がCPSでは一般化するのではないか



レッシングの4つの制約要素
Pathetic dot theory

考察および教訓

- スイスチーズモデルによる防御壁にあいたチーズの穴が貫通する様に組織事故が引き起こされた
 - ①生産圧力、②隠蔽文化、③欠陥設計前提、④監督官庁に代わって評価できた体制、⑤監督官庁の技術専門家の決定を覆した経験
- 組織事故と安全文化の醸成
- 高信頼性組織（HRO）の研究
- IAEAの安全文化向上のプロセス
- 安全文化で重要とされる8つの要素について

参考

- 安全工学と信頼性工学の接点（佐藤吉信,2002）
- 日本企業における企業不正防止策の機能不全の原因と企業倫理・コンプライアンス担当者の意識調査（上）芳澤輝泰
- 安全文化についてもう一度考えてみる（立教大学,国公私立大学附属病院医療安全セミナー,2013/5/10,芳賀 繁）
- 安全文化とレジリエンス工学（加藤淳,産業・組織心理学研究 2015 年,第 28 巻,第 2 号,119-132）
- スイスチーズモデルを発展させた船舶事故のモデル化と体系的事故防止策の提言(神戸大学,福岡, 幸二,Model of marine accidents developed by the Swiss cheesemodel and recommendations for systematic accident prevention)
- 不正の防止策と発見手法の探求~樹木医目線で「不正の木」の観察点を探る~研究会 No. a9（不正研究会）,月刊監査研究2016 . 8（No.513）
- CGS研究会（コーポレート・ガバナンス・システム研究会）事務局説明資料（グループガバナンスにおける「守り」の論点について）（経済産業省 2018年6月22日）
https://www.meti.go.jp/shingikai/economy/cgs_kenkyukai/pdf/2_007_04_00.pdf
- 日本的経営における内部不正行為抑止の研究（北野 晴人,情報セキュリティ大学院大学,2015年）
- 組織文化を背景とした企業不祥事の背景要因—単語ネットワークを用いた分析—(首都大学東京大学院,白石賢)
- 組織における内部不正防止ガイドライン(IPA)
- 日米比較：共謀罪（テロ等準備罪）と税務専門職：アメリカの税務専門職・納税者に対する共謀罪適用事例に学ぶ（石村耕司、清水晴生,白鳳大学）
- 重要インフラに求められる高信頼性組織の条件(明治大学 経営学部 中西 晶)