リスク・ベースの
意思決定の原則

2013 年 1 月 30 日

本書は SM ICG（Safety Management International Collaboration Group）の標準化ワーキンググループにより作成された。SM ICG の目的は、安全管理システム（SMS）／国家航空安全プログラム（SSP）の原則および要件に関する各国共通の理解を促進し、世界全体でそれらが適用されること繋げていくことである。

現在 SM ICG の中核メンバーとなっているのは、スペインの航空安全危機管理局（Aviation Safety and Security Agency：AESA）、ブラジルの国内民間航空局（National Civil Aviation Agency：ANAC）、オランダ民間航空庁（Civil Aviation Authority of the Netherlands：CAA NL）、ニュージーランド民間航空庁（Civil Aviation Authority of New Zealand）、オーストラリアの民間航空安全庁（Civil Aviation Safety Authority：CASA）、フランスの民間航空総局（Direction Générale de l'Aviation Civile：DGAC）、欧州航空安全局（European Aviation Safety Agency：EASA）、スイスの民間航空局（Federal Office of Civil Aviation：FOCA）、国土交通省航空局（JCAB）、米連邦航空局（FAA）航空安全機構（Aviation Safety Organization）、カナダ民間航空局（Transport Canada Civil Aviation：TCCA）およびイギリス民間航空局（UK CAA）である。また、国際民間航空機関（ICAO）がこのグループのオブザーバーを務めている。

SM ICG のメンバーは：

- SMS/SSP について関心のある共通のテーマに関して協力する
- 得られた教訓を共有する
- SMS の各国の調和を進める
- 得られた成果を航空産業全体で分かち合う
- ICAO などの国際機関や SMS を構築済みあるいはその途中段階にある民間航空当局などと協力する

SM ICG に関する詳細については以下宛てに尋ねられたい：

Regine Hamelijnck
EASA
+49 221 8999 1000
regine.hamelijnck@easa.europa.eu

Jacqueline Booth
TCCA
(613) 952-7974
jacqueline.booth@tc.gc.ca

Amer M. Younossi
FAA, Aviation Safety
(202) 267-5164
Amer.M.Younossi@faa.gov

Carlos Eduardo Pellegrino
ANAC
+55 213 5015 147
carlos.pellegrino@anac.gov.br

Peter Boyd
CASA
+61 2 6217 1534
peter.boyd@casa.gov.au

要約

本書ではリスク・ベースの意思決定を効果的に行うために必要な原則を紹介する。このほか、データの活用による意思決定を行うために必要となる、データ特性やデータ管理における留意事項について明らかにしている。

安全管理は世界中で航空安全の基準となりつつある。リスク管理は安全管理の主要な構成要素の 1 つであり、効果的なリスク管理プロセスの基幹となる要素は、ハザードの特定、これらハザードの結果に関連するリスクの評価、そして受容できないリスクの軽減である。業務提供者および航空安全当局のいずれもが航空におけるリスク管理の役割を担っている。両者ともにリスクを管理する必要があるが、ハザードやプロセスの性質および範囲は異なる。例えば業務提供者はそれぞれの組織に固有のハザードを特定する一方で、当局は様々なセクターから集められたデータを基に航空システム全体で見られる動向からハザードを特定する。

安全管理システム（SMS）や国家安全プログラム（SSP）のいずれに基づいて構築されるものであっても、安全管理のプロセスをうまく機能させるには、分析や評価の裏付けとなるデータ、ならびに当該データの特性、例えばデータの有効性、網羅性、適時性、可用性、正確性などを保証するための戦略が必要となる。加えて、安全管理はデータに基づいたシステムとなるため、効果的なデータ管理のプロセスにも依存する。データ管理とは、そのデータが、組織が必要とするものであり、整理され、信頼でき、適切なものであるという状態にしておくためのプロセスと手順の継続的な開発とその維持である。データ特性の要件設定およびデータ管理の計画策定により、効果的なハザード特定とリスク軽減が可能となる。

ハザードの特定は、体制や仕組みの設計やそれらの変更過程において行うべきであり、また、その体制や仕組みが運用されている中での継続的なモニタリングによっても実施しなければならない。ハザードの特定においては、可能性のあるすべての発生源を考慮すべきである。そして、それぞれのハザードにおいて発生する恐れのある結果に関連するリスクを、重大度および可能性の積として評価ないしは分析する。その後、組織が受容できないとみなすリスクを軽減しなければならない。

本書では、リスク・ベースの意思決定、データ特性、データ管理、および安全・リスク管理の諸要素について概要を説明する。最終章では安全管理国際協力グループ（SM ICG）メンバーの各機関が現在行っているデータ収集、ハザードの特定、および分析方法を例として紹介する。

目次

1. 目的

本書の目的は効果的なリスク・ベースの意思決定プロセスにおいて必要となる基本原則を紹介することである。データを活用したリスク・ベースの意思決定を行うために必要な関係データの特性、ならびにこのデータの総合的な管理方法などについて説明する。本書は安全管理の策定／実施プロセスの初期段階に関わる当局や業務提供者に使用されることを意図している。本書は基本原則のみ紹介するものであるので、追加資料も併せて使用することが推奨される。

2. 序文

安全管理は世界中で航空安全の基準となりつつある。これは管理者が組織または環境に存在するリスクに基づいて意思決定を行うための手段である。安全管理には組織がさらされる安全上のリスクの評価と軽減が含まれているため、リスク管理は安全管理の主要な構成要素の１つとなっている。

業務提供者と航空安全当局は航空リスク管理においてそれぞれ役割を担っている。両者ともにリスクを管理する必要があるが、ハザードおよびプロセスの性質や範囲は異なる。例えば業務提供者はそれぞれの組織に固有のハザードを特定する一方で、当局は様々なセクターから集められたデータを基に航空システム全体で見られる動向からハザードを特定する。

リスク管理プロセスにおける基幹要素とは：ハザードの特定、これらハザードの結果に関連するリスクの評価、そして受容できないリスクの軽減である。これらはいずれも、効果的なリスク管理を行うためにデータを必要とする。したがって一連のリスク管理を通じて適切なデータの管理が、堅固な安全管理プロセスを支えるために必須であるといえる。

本書ではまず、一般的なデータ活用の概念について説明する。次にデータ特性、データ管理、ハザードの特定、リスク分析、そしてリスク軽減プロセスに関して詳しく説明する。最後に、各機関が現在行っているデータ収集、ハザードの特定および分析方法を例として紹介する。

組織の安全管理プロセス／または安全管理の手段の複雑さや精巧度は、特定の国や、対象とする組織内の航空セクターの規模、成熟度ならびに複雑さに応じて変わってくる。したがって本書に記載される原則は、特定の航空セクターないし業務提供者の規模、成熟度および複雑さに合わせた安全管理が実施されることが前提となっている。例えば比較的小規模かつ／単純な航空セクターの場合、複雑な情報技術（IT）ツールを使用するのではなく、手作業によるデータ収集、分析および蓄積によってリスク管理を行っても構わないのである。

3. リスク・ベースの意思決定とは

リスク管理の第一目的は、安全に関連するデータを活用して事故または重大インシデントが発生する前にハザードによって生じる恐れのある結果を特定し、抑制することである。多面的なデータ観察によって効率的なハザード発見が可能となる共通の分類法を用いて安全データを分類することで、はるかに効果的なリスク管理が可能となる。データ分析においては 1 つないしは複数の航空セクターから得られた航空安全関連のデータ（インプット）を使用する可能性があるため、共通の分類法を用いることは重要である。データ分析プロセスから得られた結果（アウトプット）がリスク管理の選択肢（オプション）となる。図

1 は各種のインプットとアウトプットの例を示す。

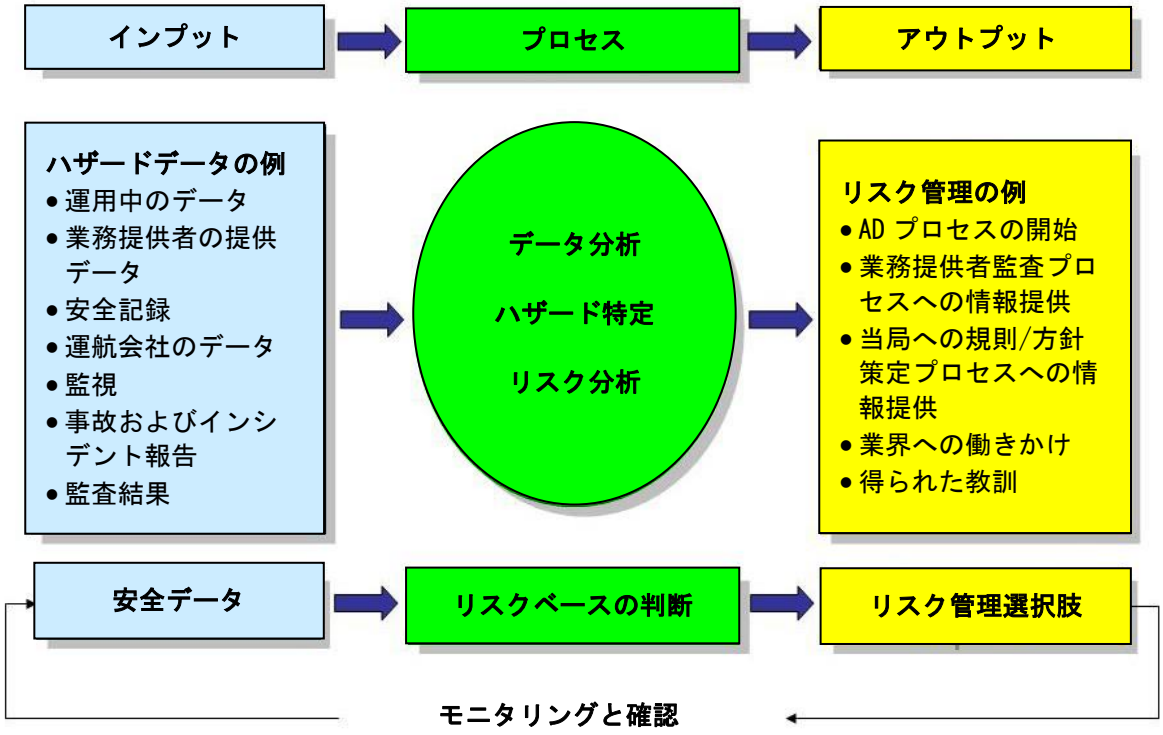


図 1: データ分析プロセスにおけるインプットとアウトプット

先にも述べたように、インプットは、新たなプロセスまたは製品のハザード分析、既存の航空システムの監視、運航中の事象、事故／インシデント調査、自発報告制度などを始めとする航空システムのあらゆる部分から得られる。必要に応じて、ハザードを排除するかリスクのレベルを下げるためにアウトプットやリスク管理が適用される。

効果的なハザードの特定は、データが有用であるかどうかに依存する。まだ稼動していない新たなプロセスや製品に対してハザード分析が実施される場合であっても、当該プロセスないし製品について示すデータが必要である。また、データを管理し必要なデータ特性を整理しなければならない。加えて、特定されたそれぞれのハザードについて包括的に理解するために、様々な航空のセクターのデータを結合し集約することも適切であろう。本書の第 4 章および 5 章でデータの特性およびデータ管理について詳しく説明する。

さらにまた、図 1 に示されているプロセスにおいては、受動的、積極的、ならびに予測的方法を活用してハザードを特定すべきである。インシデントまたは事故調査の結果として特定されたハザードの分析は受動的方法の例である。積極的なものとしては、監査、検査または義務報告後のリスク評価などがあり、一方で予測的方法とは日々のオペレーションにおけるシステムの脆弱性分析の結果を検討することなどがある。本書の第 6 章、7 章および 8 章でハザードの特定、リスク分析、リスク軽減に関して詳しく説明する。

4. データ特性

SMS や SSP いずれに基づくものであっても、安全管理プロセスをうまく機能させるにはデータを必要とする。本章では仕組みの設計、データ収集、分析および伝達プロセスにおいて考慮すべきデータの特性について簡単に考察する。

データの特性について考える前に、安全データは幾つかのカテゴリーに大まかに分類できることを考慮すべきである。すなわち、義務報告データ、自発報告データ、観察データ、そして監視データである。義務報告データは法令により提出を義務付けられる。これには事故や重大インシデントの調査ならびに一定の技術的事象から得られるデータが含まれる。自発報告データは、法令で義務付けられてはいないがハザードの特定に役立てるために報告されるものであり、インシデントやエラーに関する報告が含まれる。観察データとは、通常のオペレーションにおける異常値 [1] のことであり、これによりハザードを特定することができる。これには、Flight Data Monitoring や Flight Operational Quality Assurance などのプログラムが含まれる。監視データは、特定要件の順守を確認する監査、調査または検査から得られる。どのカテゴリーのデータも安全管理プロセスをうまく機能させるための重要な要素である。

データの種類に関係なく、分析のためにデータを統合して正しく使用できるようにする上で、質は最も重要な要素の 1 つである。データ品質に関する基本原則と実践をデータ収集・統合から分析までのプロセス全体を通じて適用することが重要である。最も重要なデータの特性として、有効性、網羅性、適時性、可用性、正確性というのがある。

データの有効性

データの有効性は他のデータ特性それ以上に重要であろう。分析結果の有効性は分析のために使用されるデータの有効性によって決まる。有効なデータがなければ、すべての分析結果、特定された傾向、そして出された結論は間違いで、誤解を招く可能性がある。データの有効性とは、データが正確かつ妥当であり、また収集されたデータが意図したものを測定しているということ言う。すなわち、データには必要な数字がすべて入っており、スペルも正しいということである。例えば日付には有効な日、月、年が入っており、32 日または 13 か月というのはない。

データの有効性エラーは通常、大量のデータをデータベースに入力するとき、あるいはデータ構造が異なる様々なデータベースを結合するときの間違ったデータ入力が原因となる。データの有効性エラーを減らすためには、単純なフィールド検証手法を採用すれば良い。例えばデータベースの日付フィールドで MM/DD/YYYY フォーマットを使用する場合、“MM” は “12” を超えてはならず、“DD” は “31” を超えてはならないという 2 つのデータ検証ルールのあるプログラムを使用することができる。この方法はデータ合理性検査と呼ばれる。

[1] 異常値とは、全体的な分布パターンから外れる観察結果である。懸念がもたれる、あるいはデータエラーのある箇所を示すものとなるが、いずれにしても詳細な調査を要する。

データの網羅性

網羅性とは、特定の分析において必要なデータと比較したときに、どの程度のデータを入手できるかということである。リスク・ベースの意思決定を支える新たな分析プロセスを開発する前に、最低限必要なデータを決めるべきである。必要なデータの量が多ければそれだけ、データを入手するために必要なリソース（例、時間、マンパワー）も増えるということに留意すべきである。データ収集の仕組みの設計時にはこのことを真剣に考慮しなければならない。網羅性のための要件は入手可能な情報に見合ったものにもすべきである。例えば、事故に関するデータの量は軽微なインシデントよりもはるかに多くなる可能性が高い。

データの適時性

適時性はユーザーが期待するものであるが、一般的に最高のデータとは最新のものである。歴史的に、技術やプロセスの制約によってリアルタイムのデータ提供の可能性は排除される傾向にあった。しかしながらコンピューターやネットワーク技術の発達により、データのリアルタイム入手の障壁は崩れている。このため、その安全管理プロセスにおいて組織は最大限、航空安全データへのリアルタイムアクセスができるよう努力すべきである。例えばフライトデータモニタリング（FDM）データのワイヤレスダウンロードのための最新システムにより、オペレーターはほぼリアルタイムでデータにアクセスすることができる。

データの可用性

データはまた、絶えず必要なときに入手できるべきである。一般に、データの可用性はデータの保存場所やアクセス方法の冗長性によって実現される。データの可用性は、データを入手できる頻度（例、99.9%の可用性）や、一度に流すことのできるデータの量で測定することができる。

データの正確性

データの正確性とは、データが現実の対象物や説明される事象を正確に反映している程度のことを言う。データが不正確となる原因は幾つかある。最も一般的な原因は最初のデータ入力で、ユーザーが間違った値を入力するか、タイプミスが起きることによる。これはデータ入力者が必要なスキルを有し、適切に訓練を受けるようにすることで解決できる。データ入力に起因するデータの間違いは、アプリケーションの中にタイプミスを見つけるコンポーネントを組み込むか（例、スペルチェック）、可能な値のリスト表示など、データの正確性を確保するためのその他の方法によっても解決できる。

要するに、それぞれのデータ特性向上に取り組むべきなのである。それぞれにおいて取り組むのに相当な努力を要する場合もあるだろう。組織におけるデータの信頼度は 1 つの特性だけで達成されるようなものではない。データの信頼性というのはむしろ重層的な概念であり、一層ずつ達成されるのである。別の層が追加されるごとにデータの信頼度は上昇する。さらに、これらの特性はプロセスや仕組みの設計当初に考慮しておくべきである。プロセスや仕組みが実際に稼働しだしたら、経営陣がデータに基づいて決定を下せるようにするために必要なデータを入手するには遅すぎるかもしれないからだ。

5. データ管理

安全管理はデータに基づくシステムであり、よって効果的なデータ管理プロセスに依存する。データ管理とは、組織が必要とするデータを確保し、それらが整理され、信頼でき、かつ適切なものであることを保証するためのプロセスと手順の継続的な開発と維持である。データを管理する際には、その組織はどのような情報が必要であるのかを定義し、そのプロセスにおいてどのように活用するのか計画しなくてはならない。

効果的な安全データの管理のために、組織は以下のことを行うべきである。
- 目的を達成するために必要なデータを定義する。
- データの使用目的に基づいて、データアーキテクチャやデータベース構造を設計する。
- 必要なデータ収集頻度を含む、データの基準および形式を定義する。
- 収集データを規定の基準や形式に合致させるためのプロセスを開発する。
- 収集されるデータの必要性とその用途を考慮して、データ収集ツールを開発する。
- 複数のソースから収集するデータを決める。
- 安全データと、関連性があるかもしれないその他の相関データとを統合する。
- ユーザーのための適切なデータアクセスを保証する。
- データ保護の課題を考慮する。
- 組織内外の主体とのデータ共有を考慮する。
- 構成管理を始めとして、データのライフサイクル全体にわたってデータを管理する。

本章では、安全管理においてデータを効果的に利用するために考慮すべきデータ管理の主要なポイントについて説明する。

データ収集計画

データを収集する前に、組織（当局または業務提供者）は必要な情報を特定しなければならない。例えば、当局もしくは業務提供者は通常、事故や重大インシデントに関する詳細なデータをもっている。しかしながら、安全に関する出来事すべてについてシステムにデータが入っているというわけではない。したがって、この知識を得るためには、組織としてこのようなデータを収集するための計画を策定する必要がある。

収集するデータを特定した後、組織は情報源ならびに収集・保存プロセスについて決定する。例えば、システムは一般に公開するのか、乗務員か、それとも業務提供者に公開するのかなどということである。これに答えるには、第 4 章に記載されるデータ特性を検討して、情報源は当該水準の詳細データを提供できるものかどうか判定する必要がある。

データの標準化

内容の標準化はデータの活用に直接影響を及ぼす。よって、様々なソースからのデータを比較し、集約し、結合するためにはデータを標準化する必要がある。様々なソースのデータをリンクできるようにするには、共通の分類法のための基準を策定して維持するか、異なる分類法の間で変換できるようにする必要がある。分類法により、同じ名称を使用してデータを識別し、保存することができる。例えば、航空機の型式は「737-200」または「Boeing 737-200」または「732」として記録できるようになる。基準の例としては下記のものがある。
- 航空機モデル：運航を認められているすべてのモデルのデータベースを構築することができる。
- 空港：国際民間航空機関（ICAO）または国際航空運送協会（IATA）コードを使用して空港を識別することができる。
- 事象の種類：事故調査組織は ICAO およびその他の国際組織が開発した分類法を使用して事象を分類することができる。

レガシー問題やその他の要因により、各種データベースの間で共通の分類法が使用されていない場合もある。このような場合、同等性に基づくデータの標準化を可能にするためにデータマッピングを行うべきである。上記の航空機の型式を例にとると、データのマッピングにより、あるデータベースの「737-200」は別のデータベースの「732」と同等であることを示すことができる。場合によってはデータ収集時の詳細度が異なることもあるため、簡単なプロセスとはならないこともある。データが非常に不均一であるために共通の分類法の使用は実現不可能な場合、他の形でのデータ統合を検討すべきである。

新基準を作成する場合は、必要な基準策定のために内外両方のソースを検討しなければならないだろう。

データ構造および形式

データ収集のために利用するプロセスを決定したら、次なる段階は収集するデータの構造を定義することである。データを置く場所を考える必要もある。データを既存のデータベースに結合するのであれば、すでに収集されているデータと同じ構造を使用する必要がある。例えば、既存のデータベースに飛行時間、乗務員、航空機、空港およびその他に関する詳細情報が入っている場合、これを新たなデータベースと結合するには、この情報を効果的に統合するために既存データベースと同じ形式のデータフィールドが必要になる。システム間の共通フィールドはどれも同じ形式にすべきである。例えば「日付」フィールドは各システムで同じになる（例、「MM/DD/YYYY」）。構造や形式の異なるデータの結合を可能にするもう 1 つの施策として考えられるのはデータ変換の利用である。この方法は異なるソースのデータが同等である場合に適用できる。データが変換されるようになれば、データは互換的となり、様々なデータベースを使用する分析が可能となる。

データ収集ツール

ソース、内容、形式および基準が定義されたら、データを収集するための適切なツールを構築する必要がある。ここでは以下の特性を考慮することが非常に重要である。

- **アクセスしやすさ**：報告システムは見つけやすく、アクセスしやすい場所に用意すべきである（例、組織のウェブサイトのメインページの一番上にある大きなリンク）。許可されていない人間のアクセスは阻止するべきであるが、対象ユーザーにはアクセスしやすくすべきである。例えば乗務員（対象ユーザー）はパイロットのライセンス番号と、組織内の他のシステムにアクセスするときに使用されるものと同じパスワードによってアクセスできるようにすべきである。

- **報告のしやすさ**：報告書に記入するとき、ユーザーは可能な限り最低限の作業で情報を入力できるようにすべきである。例えば日付や時間のフィールドはカレンダーをクリックすれば自動入力できるようにすべきである。

- **重複情報のないこと**：すでに組織が入手している情報は再度収集されることのないようにする。例えば乗員に関する情報の入ったデータベースがすでにその組織内に存在している場合、パイロットのライセンス番号だけの照会で十分とすべきである。

- **入力内容の制御**：情報が所要の形式で得られるように形式制限を設けることができる。例えば時間が「0954」と入力された場合、システムが規定の構造に従って形式を整える。この場合は「09:54 am」となる。

以上はデータ収集ツール設計時に考慮すべき事項の一部に過ぎない。データ収集ツールは収集されるデータの種類や量に応じて紙ベースの場合もあれば、コンピューターベースの場合もある。

データ保存およびデータベース保守

データが収集されたら、一般に「安全なライブラリ（safety library）」と呼ばれることもある場所に保存すべきである。データ保存における留意事項として、収集されるデータに対して十分な保存容量を確保することがある。所定期間経過後に所定のデータを更新ないし処分することも必要だろう。さらにまた、このデータの入ったデータベースは、必要なときに有効かつ信頼できるデータが提供されるよう確保するために保守を行うべきである。保存計画ではデータ可用性を確保するための冗長性をもつ保存場所の確保も必要である。

データアクセスおよび可用性

データベースユーザーのデータに対するニーズをデータへのアクセスに必要なツールとともに特定すべきである。加えて、アクセス制限の必要性についても評価し、定期的に見直すべきである。データ管理計画では、保存されたデータへのアクセス制御、対象ユーザー数に対応できるだけの十分な帯域幅の決定、適切な冗長性の決定など、組織全体を通じてのデータ管理責任についても考慮すべきである。

データ保護に関するガイドライン

データ保護の原則はあらゆる種類の安全データに適用される。公表される事故報告データであっても、乗務員の名前や彼らを直接特定できるその他の情報など、一部のデータは保護される。任意データの場合、報告する個人が直接特定されないように保護するだけでなく、報告を奨励することも目的としているため、さらに高度の保護が必要であろう。それでも 、データの保護とこれがもたらす安全上の利益は現地／国内法や国家／業務提供者の安全文化と密接に連関しており、報告が奨励されることもあれば禁じられることもある。

安全管理の基礎となるのは、航空安全当局に提供されるほとんどの自発報告データは秘密が守られるべきであり、法律で認めるとおりに報告する個人の身元は匿名性が保たれるということに対する理解である。罰則を科されない自発報告データ報告協定が法律で認められておらず、証明／認可プロセスの一環として規定されていない場合、各国は法律または規則の変更を提案して、この立証済みのデータ共有のコンセプトを可能にすることを検討すべきである。

取り組むべきもう 1 つの重要な問題は、安全情報の使用に関する当局／業務提供者の方針である。安全データの過剰もしくは不相応な保護は安全管理を遂行するために必要なデータの可用性に悪影響を及ぼす可能性があり、当局／業務提供者が当該データを効果的に活用することを制限してしまう場合もある。このように、安全情報を確実に保護するためには、安全情報を保護する必要性と正義を行使する責任との非常に微妙な利害のバランスをとらなければならない。方針には安全情報の管理者の責任に関する指針と情報開示に関する規則を盛り込むべきである。収集されるデータならびにデータを伝達するときの手順および条件を決めるときには常に、非航空関係者による情報へのアクセスを扱う法令を考慮すべきである。

データ保護ならびに効果的な保護を行っているという信頼の獲得は様々な手段によって実現できる。可能性のある方法として、第三者にデータを収集させるというのがある。これは組織から独立している部門となる。成功しているもう 1 つの方法として、中立的な第三者を置いて業務提供者のデータを収集、非特定化、集約、処理させてから業界団体ないし航空安全当局に提供するというのがある。このように中立的な第三者は防護壁となり、データの機密性が保証される。だがこの方法には、第三者が航空安全を目的としてデータを検証および分析する専門知識に欠けるというデメリットが生じる場合もある。

要するに、データ保護プロセスは最低限、以下の内容に対応した正式な協定に基づいたもの

にすべきである。

- **匿名性：** 関連データ保護協定に従って、分析プロセスにおいて必要となる特定可能なデータはできる限り早い時点で永久に取り除かれるということを定める。

- **データアクセスおよび管理：**保護を要するデータを特定し、データ保護に関する包括的な責任を割り当てる。加えて、データアクセスおよび管理においては、データを保護するためのガイドラインと手順、データへの認可アクセス、データ処理および保存場所、レポートおよびその他のデータ出力への認可アクセスといったことについて規定し、保存期間経過後のデータ破棄を義務付ける。

- **データ分析施設：**すべてのシステム、オフィス、機器、ワークステーション、コンピューターおよびデータ分析プログラムに関係する周辺装置のための安全な、アクセスが管理される施設を用意する。用紙、媒体およびバックアップ装置を始めとするデータ分析関連のあらゆる資材の保管のための安全なシステムも用意すべきである。

安全データの共有

航空システムは、相互に作用し、航空製品のライフサイクル全体にわたって影響を及ぼす数多くのステークホルダーで成り立っているため、安全データの分析は一体となって行うべきである。安全管理のベストプラクティスでは業務提供者が非特定化された収集情報を当局と共有することが推奨され、それによって航空安全当局は航空システムにおける（セクター別または全体としての）トレンドを観察し、よりリスクの高いセクターに対処するために的を絞ってリソースを投入することができる。

共有すべきデータと、関連する安全上の問題について決定する前に、共通の分類法に取り組むことが重要である。データ共有においては、すべての情報源から同様のフィールドや分類法を使用するデータが提供されるか、これらの共通性に対応できるよう変換される必要がある。この問題についてはすでに本章の*データ標準化*のセクションで説明した。

データ統合／融合

今日のツールを使用すれば、データの統合や、既存データベースにある膨大なデータを有する新しいデータベースの合成が可能である。テクノロジーによってデータベースとシステムの統合が可能となり、保護情報（例、便名、航空会社、パイロットの身元）を明かすことなく航空データベース（例、空港気象データ、非特定化されて集められた飛行情報）間をリンクさせることが可能となっている。

また、航空安全当局もデータの集約・統合により、単一の航空セクターで収集できる容量を超えたデータ共有を進めるべきである。変則的な事象、異常、超過の状態がデータの統合により生成されるコンピューターグラフィクスで明白になるだろう。例えば、航空機データやレーダー航跡データから得られる飛行経路によって、分析者は他と大きく異なっているフライトパスに気付くことができる。次に当該領域の専門家がこの相違について調査し、その発生理由に関する理解を深めることができる。

図 2 はデータ統合の概念を図示している。この例では空港周辺の飛行の安全について、様々な数多くのソースから集められたデータを結合または統合することにより調べることができる。この図は空港周辺のデジタル地形データと空港発着航空機の飛行航路（青線）を統合したものである。

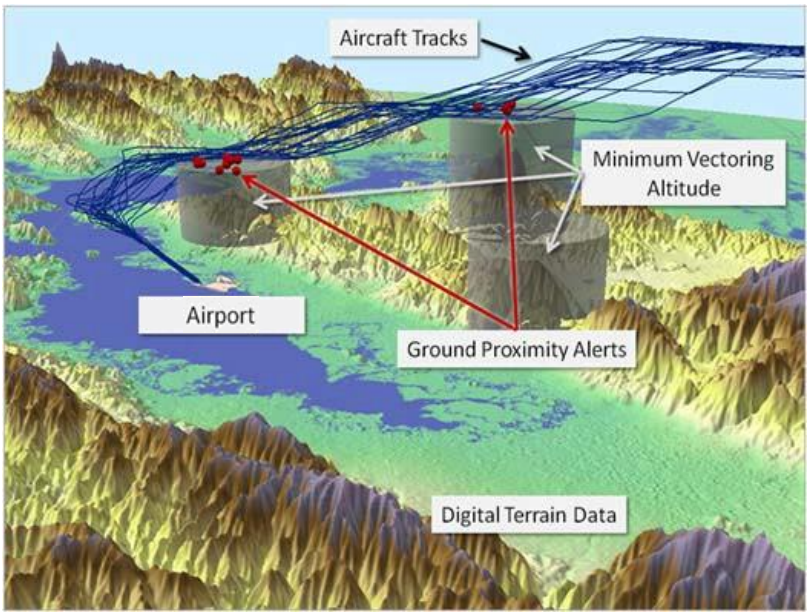


図 2: データ統合例

データに関するその他の留意事項

適切に機能するリスク管理プロセスを構築するときに安全データに関して考慮すべきさらなる事項として次のものがある。データセキュリティ、データの完全性、そしてデータの陳腐化である。データセキュリティとは、データの安全が確保され、あらゆる損失から保護されるようにすることを意味する。これは重要なテーマではあるが本書で扱う領域外である。

航空システムにおいて安全データをどのように扱い、処理し、伝達するのか検討すべきであり、データの完全性を維持するための手段を組み込むべきである。ヒューマンエラー、ハードウェア障害、およびソフトウェア処理エラーによって起こるデータの破損はデータの完全性を損ない、無効なデータや分析結果の原因となる可能性がある。理想を言えば、データ取扱い／処理経路で発生する可能性のあるデータ破損を特定するために、エンドツーエンドの完全性チェック—繰り返し冗長性検査（CRC）やその他同等の保証技術の使用など— を行うべきである。

さらにまた、データの陳腐化も不正確なデータの原因になる。正確なデータ値の多くは時を経て不正確になる（すなわちデータの陳腐化）。例えば、航空機登録および航空機型式証明保有者情報や航空会社が運航する航空機の数は時とともに変わってくる。更新しなければデータは陳腐化して不正確となる。最後に、1 つの要件を完全に満たそうとすると別の要件を満たすことができなくなるという場合もある。例えばデータ保護はデータの信頼性を低下させ、保護が行き過ぎればデータ品質チェックをほぼ不可能にすることもある。

以上、本書の第 4 章と 5 章ではデータ特性の重要性とデータの管理について説明した。次章ではこのデータを使用してハザードを特定する方法とリスク管理プロセスにおけるデータの使用法について説明する。

6. ハザードの特定

SM ICG ではハザードを、*航空機インシデントまたは事故の原因となるかこれに寄与する可能性のある状態*として定義している。ハザード特定段階では、当局または業務提供者の安全アナリスト[2]がデータを分析して、潜在的ハザードならびに付随する影響ないし結果を特定し、文書化する。ハザード特定プロセスにおいて必要とされる詳細度は検討にかける航空プロセスの複雑度に依存する。

[2] 本書で使用される安全アナリストとは必ずしもデータ分析の専門家を意味するわけではない。アナリストは特定の航空セクターの専門家、あるいは安全アナリストないし専門家の集団で構成される安全委員会でも良い。一般に、技術的に多様な集団による徹底的な検討を経て、単一主体が安全に関する重要な意思決定を下すのが優れたやり方である。

ハザードの特定における留意事項

効果的なハザードの特定を確実に実施するためには幾つかの要素を考慮しなければならない。第一に、システムにおけるハザードを特定する体系的なプロセスを開発することである。利用できる方法は多数あるが、いずれにおいても以下の 3 要素に留意する。

a) 安全アナリストは技術および／または管理面での専門知識を有しているべきである。
b) 安全アナリストは各種のハザード分析技術に関して訓練を受けているか経験を積んでいるべきである。
c) 規定されたハザード分析ツールが存在しているか、開発されるべきである。

第二に、安全アナリストはハザードを特定するために必要なデータソースを特定することである。そして最後に、安全アナリストは入手可能なデータや評価対象となる航空システムの種類に最も適した技術ないしツールを選択すべきだということである。

潜在的なハザード源

ハザード特定時には考えられるすべてのハザード源について検討すべきである。検討にかけるシステムの性質や規模に応じて以下のものが含まれる。

a) 機上ないし地上設備（ハードウェアおよびソフトウェア）
b) 運用環境（環境条件、空港インフラの不備、空域、空港設計および航空路設計を含む）
c) ヒューマンパフォーマンス
d) マン／マシンインターフェース
e) 運用手順
f) 整備手順
g) 外部インターフェース（例、外部委託）
h) 組織の業務手順
i) 組織の変更

ハザード特定のきっかけとなるもの

ハザード特定プロセスを用いる実例は様々あるが、主なものとして以下の事例がある。

- **システムの設計：**ハザードの特定は、運用開始前の、特定の航空システムとその環境についての詳細説明から始まる。次に安全アナリストはそのシステムに関係する様々な潜在的ハザードとともにインターフェースで接続する他のシステムへの影響について特定する。

- **システムの変更：**ハザードの特定はシステム（運用面または組織面）に変更を加える前に始まり、航空システムへの特定の変更についての詳細説明が含まれる。次に安全アナリストは計画される変更に関係する様々な潜在的ハザードとともにインターフェースで接続する他のシステムへの影響について特定する。

- **オンデマンドおよび継続的モニタリング：**ハザードの特定は運用中の既存システムに対して適用される。図 3 はオンデマンド分析と継続的モニタリングの両方を含むプロセスの例を示している。データモニタリングは以下の検出にも役立つことに注目すべきである。すなわち、予想よりも頻繁に発生するか、より深刻なハザードであるか、そして採用した軽減策が想定よりも効果的でない、などである。加えて重大な懸念アイテムについては通知限界値を設定して継続的分析を実施する。

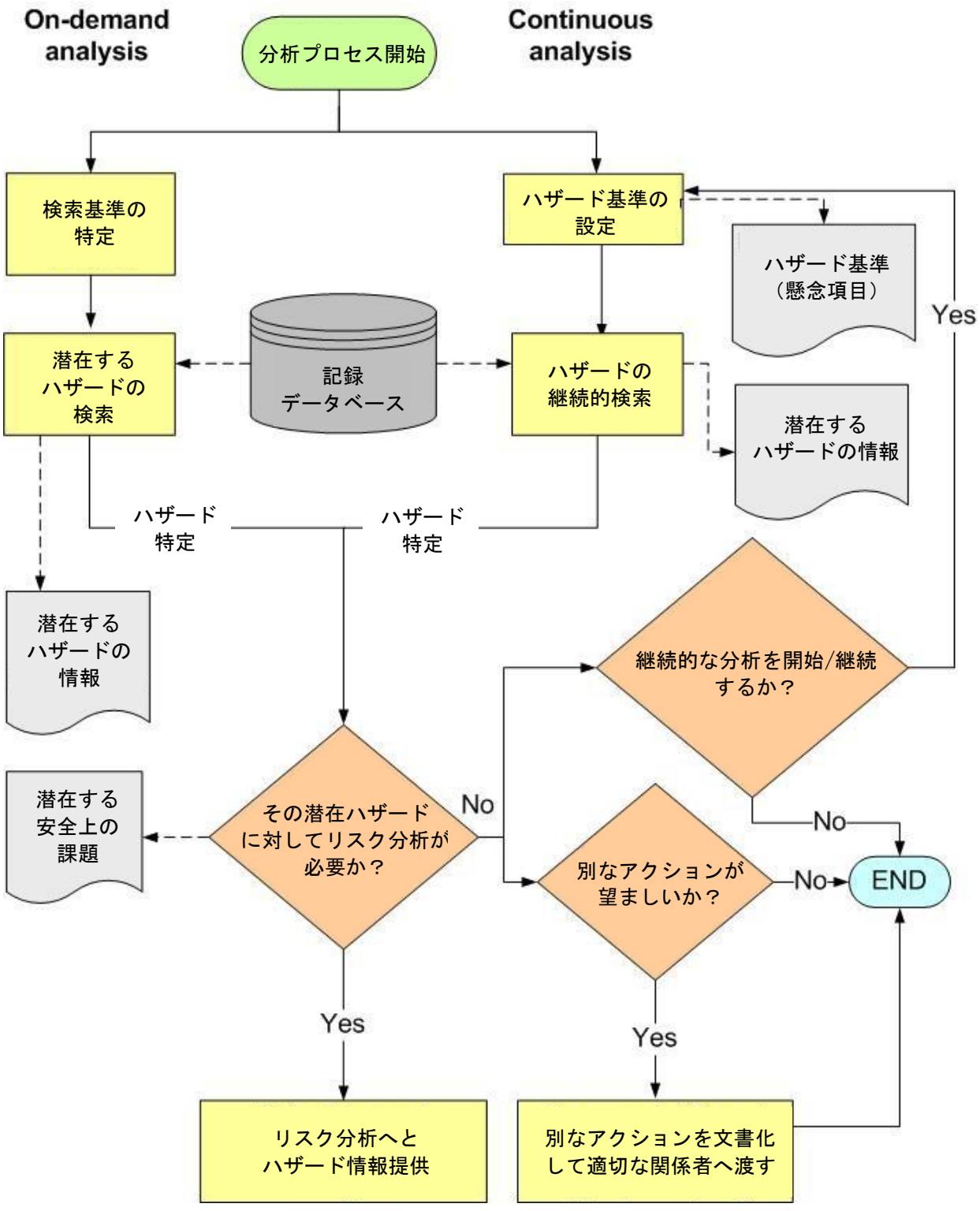


図 3: オンデマンドおよび継続的分析におけるハザードの特定

ハザードの特定方法および手段

ハザードを特定するための方法や手段は数多くある。以下に 3 つの例を示す[3]。

ブレインストーミング

ブレインストーミングとは専門家の集団内で行われる制限のない活発な討論である。進行役はグループセッションに先立って議論を促すテーマや論点を用意し、セッションでは各人に想像的思考やメンバー間での議論を促す。進行役が口火を切り、枠にとらわれるようなルールを設けることなく議論が続けられる。すべての意見が受け入れられて記録され、異議を申し立てられたり批判されたりすることはない。これにより、専門家たちが水平的思考を心地よく感じる環境が生まれる。

メリット：

- 新規の、または複雑でないシステムの新たなハザードを特定するのに効果的である。
- 主要ステークホルダー全員が関与する。
- 比較的迅速かつ簡単に行える。
- 広範囲の種類のシステムに適用できる。

デメリット：

- 比較的まとまりがないために必ずしも包括的ではない。
- 参加者の専門知識やプロフィールに左右される。
- 集団心理または経営トップの目標の影響を受けやすいこともある。
- 成否は進行役の能力に大きく依存する。

Hazard and Operability（HAZOP）法

HAZOP とはパラメーターや逸脱の指針用語（guideword）を使用する体系的かつ構造的な手法である。この手法はシステムに関する非常に詳細な説明が得られるかどうかに依存し、通常はシステムを明確に定義されたサブシステムと、サブシステム間の機能の流れまたはプロセスフローにまで分解する。次にシステムの各要素が多セクターにわたる専門家集団の間で、指針用語と逸脱の様々な組合せに照らして議論にかけられる。グループディスカッションは議長によって進められ、特定の指針用語と逸脱の組合せについて話し合われたときに特定されたハザードを含む討議結果が書記によって記録される。特定の指針用語と逸脱の組合せがハザードとならない場合、あるいは信憑性がないと考えられた場合でも、網羅性を証明するためにこのことも記録すべきである。指針用語と逸脱内容は HAZOP 議長によって事前に用意しておくべきであり、分析対象のシステムないし運用に合わせたものにする必要があるだろう。

航空関係の代表的な指針用語として以下のものがある。

- Detection（検出）
- Co-ordination（調整）
- Notification（通知）
- Transmission（伝達）
- Clearance（クリアランス）
- Authorization（許可）
- Selection（選定）
- Transcription（転写）
- Turn（旋回）

[3] 欧州民間航空安全チーム（European Commercial Aviation Safety Team：ECAST）安全管理システム・安全文化ワーキンググループのハザード特定ガイダンスより

- Climb（上昇）
- Descend（下降）
- Speed（速度）
- Read-back（復唱）
- Monitoring（モニタリング）
- Signage（標識）
- Handover（ハンドオーバー）
- Supervision（監督）

代表的な逸脱として以下のものがある。
- Too soon / early（早すぎる）
- Too late（遅すぎる）
- Too much（多すぎる）
- Too little（少なすぎる）
- Too high（高すぎる）
- Too low（低すぎる）
- Missing（不明）
- Twice / repeated（2 回／繰り返し）
- Out of sequence（順序誤り）
- Ambiguous（曖昧）
- Reverse / inverted（逆転／反転）

HAZOP 法のメリット：
- 体系的かつ厳密。
- 多セクターにわたる専門家が意見を交わす。
- 広範囲の種類のシステムに適用できる。
- ハザード特定プロセスについて詳細かつ監査可能な記録を作成する。

HAZOP 法のデメリット：
- 相当な準備を要する。
- 複雑でないシステムにおいては利用し難い。
- HAZOP 議長の能力に大きく依存する。
- 時間がかかり、それゆえに費用がかかる。
- 想像的な思考は禁じられるため、ハザードは所定の種類のものとなる。

<u>チェックリスト</u>

チェックリストとは、過去の経験から導き出された既知のハザードないしハザードの原因のリストである。過去の経験とは、同様のシステムや運用に関する前回のリスク評価、あるいは過去に発生した実際のインシデントのことである。この手法においては体系的に適切なチェックリストが利用され、特定のシステムへ適用できるかどうかについてチェックリストの各項目が検討される。チェックリストは利用する前に適用できるかどうかを常に確認しなければならない。

メリット：
- システムの専門家でなくても利用できる。
- 広範囲にわたる過去の知識や経験が記録される。
- 一般的で明白な問題が見過ごされることがない。

デメリット：
- 新規のシステムまたは複雑でないシステムを扱うときには利用が限定される。
- ハザード特定プロセスにおいて想像的な思考ができない。
- 過去に見られなかったハザードを見逃す可能性が高い。

7. リスク分析

安全管理プロセスにおける次なる段階は、特定のハザードそれぞれに対して見込まれる結果に付随するリスクの評価や分析であり、それぞれのリスクは重大性と可能性の積で決まるものである。よって、ハザードに順位を付け設定されたリスクガイドラインと比較できるように、重大性および可能性は、特定されたハザードによって想定される結果に基づいて測定可能な単位で表現するべきである。そしてこれらはリスク軽減の適切な範囲と時期を決定するのに役立つ。

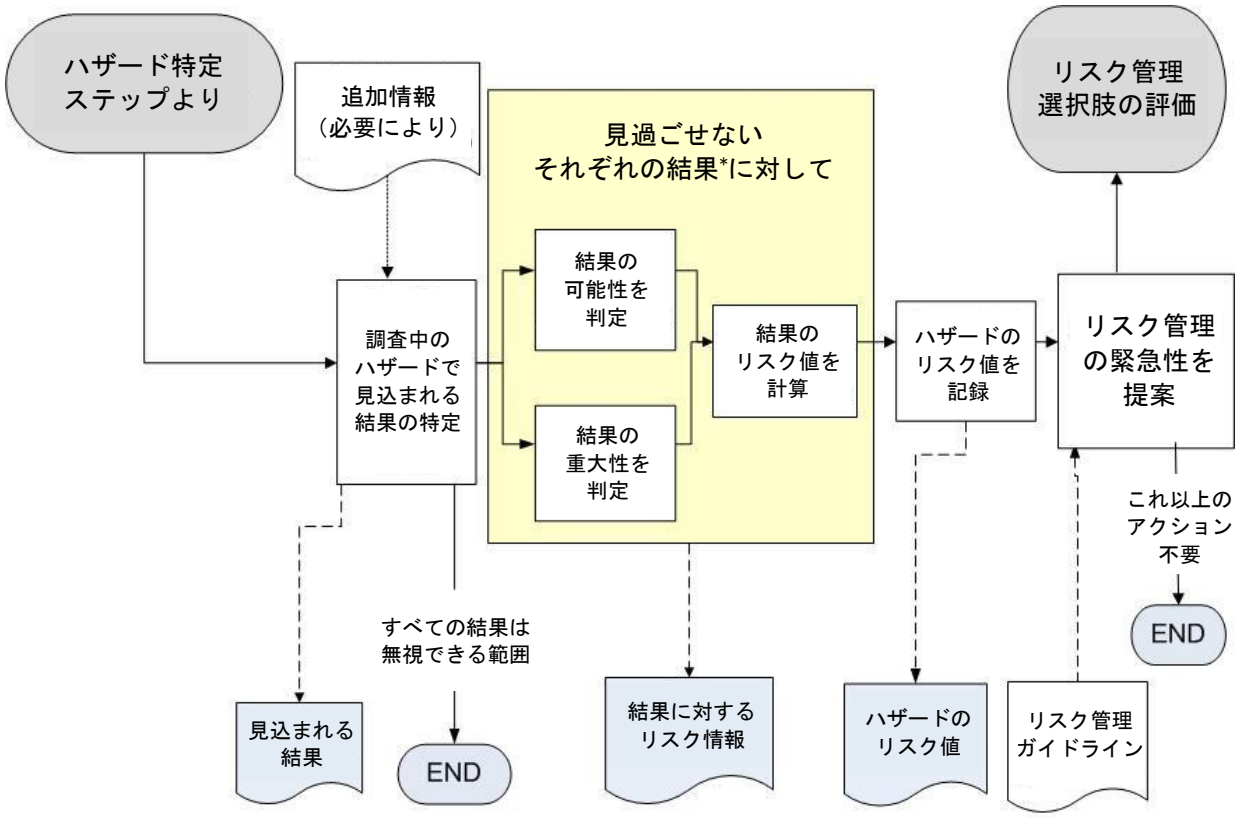
リスクを評価する際には定量的方法および定性的方法のどちらでも使用できる。定量的データを使用する方が、より客観的となる傾向があるため望ましい。ただし、定量的データを入手できない場合には、定性的データと専門家の判断に頼っても構わない。定性的判断は人によって異なるため、1 人だけで分析を行うのであれば結果は意見とみなすべきである。専門家のチームが分析に関与する場合、結果は定性的データおよび専門家の判断とみなすことができる。したがって、分析の質は選ばれたチームの専門家たちの経歴に依存することになる。

定量的データの利点：
a) データは量、数字または量で表される。
b) データはより客観的となる傾向がある。
c) より合理的な分析と結果の具体化が可能になる。
d) データはモデリングのために使用できる。

定性的データの利点：
a) データは質の基準として表される。
b) データは主観的である。
c) 判断は、数字によってではなく専門家によって示される場合が多い。

モデリングが必要でデータを入手できる場合、リスク評価は統計もしくは観測データ（例、レーダー航跡、ハードウェア故障率）に基づくべきであることに留意すべきである。リスクについて純粋な統計的評価を行うほどには十分なデータがない場合、判断に基づくデータを使用しても良いが、それらは定量的に表現すべきである。例えば特定種類の運用について真の割合は分からないが、判断に基づくデータを使用して推定できるという場合などである。いずれの場合も定量的な測定値で、過去のデータでは表現できないような—もしくは誤った内容に至ってしまう恐れがある—事実を説明しなければならない。このような場合においては、入力データについての調整が必要になるかもしれない。

図 4 は修正のためのリスク管理の種類と優先順位を決定するときに用いられるリスク分析プロセスの例を示す。



*単一のハザードが複数の望まれない結果を引き起こすこともある。

図 4: リスク分析プロセス例

リスクは様々なリスクプロフィールに照らして観察し、コントロールできることに注意すべきである。単一の飛行、航空機の機種、単一ないし複数の業界などにわたってリスクを観察することができる。リスクプロフィールは特定の航空セクター（当局または業務提供者）の全体的な安全目標に依存する。

また、どのようなリスク分析であれ重要なのは、特定のリスク分類に至る様々な前提事項の文書化である。将来見直すことができ、必要に応じて、特に運用環境が変化した場合には更新することができる。

8. リスク軽減策

リスク軽減の目標は、特定されたハザードのそれぞれの結果に付随するリスクについて、許容できる安全水準に達するまで軽減する適切な計画を実行することである。安全アナリストは適切なリスク軽減ないしリスク管理方法を策定し、文書化し、提言する。リスク管理とはハザードの影響／結果であるリスクを軽減することである。リスク管理方法にはリスクを低下させるかハザードを排除する選択肢や代替策が含まれる。例として次のものがある。追加的方針ないし手順の実施、冗長システムおよび／またはコンポーネントの開発、訓練の細目の見直しや結果のレビュー、代替となる製造元の利用などである。

リスクのレベルが受容できるものでないと判定された場合、アナリストは、経営陣が許容できるとして組織（当局または業務提供者）の方針に明示されているレベルまでリスクを減らすような、可能性のあるリスク軽減策を特定し、評価する。次にアナリストは提案された軽減策が全体的なリスクにどのように作用するか評価する。必要に応じて、アナリストはこれらの施策によって、リスクが経営陣が受容できるレベルへ低減するまで、このプロセスを繰り返す。リスク評価の結果、リスクが受容できないレベルであることが判明した場合、何らかの緩和処置によって許容可能レベルに至るまで、直ちにオペレーションやプロセスを停止すべきである。

次なる段階として、提案されたそれぞれのリスク管理方法の評価を行うべきである。理想的なリスク管理とは、費用がかからず、実行しやすく、迅速に実施され、完全に効果のあるもので、別のリスク（意図せぬ結果というリスク）をもたらすことのないものである。ほとんどはこのような理想どおりにはいかないため、リスク管理方法の候補について、効果、コスト、実施の適時性および複雑度という特性を秤にかけて評価し、選定すべきである。リスク管理の方法が選定され、実施されたら、意図された目標を達成できているかを確認するために監視して検証すべきである。

選択されたリスク軽減手法は以下のカテゴリーの 1 つ以上に該当すると思われる。

- **リスク回避戦略：**リスク回避戦略では、別のアプローチを選択するか、オペレーションや、手順や仕組み（ハードウェアおよびソフトウェア）の開発に加わらないことによって発生の可能性および／または影響を避ける。この手法は複数の代替策ないし選択肢が用意されているときにとるべきである。リスク回避戦略はオペレーションまたはプログラムの開始時点で「決行（go）」か「中止（no-go）」の決定の根拠として用いられることが多い。

- **リスク低減戦略：**リスク低減戦略とは、オペレーションまたは活動の頻度低減、または受容したリスクの影響度を軽減するための対策を実施することを意味する。リスクを低減するための対策が別の当事者により実施されるのであれば、この戦略はリスク移転処置となる可能性がある。

- **リスク移転戦略：**リスク移転戦略ではリスクの所在を別の当事者に移す。
組織は、主として最もそれを管理することができる組織または業務部門にリスクの所在を移転する。移転を受けた当事者はリスクを受け入れ、文書化しておくべきである（例、協定書、合意書、覚書）。リスク移転の例としては、取得組織から整備を提供する組織への航空システムの移転がある。

- **表面化リスク分離戦略：**この戦略においては、リスクの影響を分離するか、これを防ぐため冗長性を組み込む処置が講じられる。分離の例として、複雑な地形に囲まれた飛行場への運航は、特定の飛行性能をもつ航空機に限定するというものがある。

- **リスク前提戦略：**リスク前提戦略とは、リスクの発生に伴う影響の可能性や見込み、その深刻度をただ受け入れることである。通常、ハザードに付随する高いリスクに対して前提戦略を用いることはない。それでも安全上のリスクを受け入れる前に、これを軽減してレベルを下げておかなければならない。この手法を選択する場合は、事前に想定されるリスクに対する実施可能な対策を準備しておく必要がある。

以上、第 6 章、7 章、8 章で説明した指針は、ハザードを特定し、ハザードの結果に伴うリスクを評価し、リスクを許容可能なレベルに軽減するときに使用できる一般的な方法を示している。次章では各当局で用いられているハザードの特定および分析方法を例示する。

9. 各当局の現在のリスク管理方法

SM ICG は加盟当局の実践状況について、現時点での状況（ベースライン）を明らかにするために、既存のデータ収集、ハザード特定、および分析プロセスについて調査を行った。この調査の目的は、安全管理プロセスを策定しようとしている各国に対して、既存の方法や手段に関する情報を提供するとともに、それらの詳細を確認するための参照用 URL を紹介することである。各当局はすでに完成しているプロセスとこれから展開を図るもの両方の情報を提供してくれた。下表に調査結果を幾つか例として紹介する。表に続き、最初の例—*Decolagem Certa*（DCERTA）システム—について既存のリスク管理プロセスに関するケーススタディとして詳しく取り上げる。

表 1: 当局のリスク管理方法例

航空安全当局	プロセス／システムの名称	プロセス／システムの説明および目的	詳細情報の参照先
ブラジル国内民間航空局（ANAC）	Decolagem Certa (DCERTA) システム	ブラジルは *Decolagem Certa*（DCERTA）システムと呼ばれる自動化システムを開発した。これは小型民間航空（General-Aviation）について、乗務員（ライセンス、資格、診断書）、航空機、および運用飛行場に関して空港 AIS でパイロットが提示する飛行計画に記載される情報に基づいて規則への順守状況を確認するものである。このシステムは安全分析のためのデータを提供し、これがリスク・ベースの監査プログラム構築を可能にする傾向指標を出すのに使用されることになった。	http://www2.anac.gov.br/decolagemcerta/
欧州航空安全局（EASA）	欧州事故・インシデント報告システム調整センター（ECCAIRS）	欧州事故・インシデント報告システム調整センター（European Coordination Centre for Accident and Incident Reporting Systems：ECCAIRS）の使命は、各国および欧州の運輸当局や事故調査機関が公共交通機関の安全性を高めるために安全に関する情報を収集、共有、分析するのを支援することである。	http://eccairsportal.jrc.ec.europa.eu/index.php?id=1
スイス民間航空局（FOCA）	SRM（安全リスク管理）	FOCA は ICAO フレームワーク（Doc. 9859）に準拠した機関内 SMS を実施している。ハザードの特定は、発生報告書、監視結果、航空事故調査局（AAIB）の調査およびその他の情報源から得られるデータが誘因となってこれに基づいて実施される。分析は普通、定性的に行われる（Hazard Identification Studies (HAZID)、HAZOP 法）。その後のリスク分析は定性的または定量的、あるいは両方で行われる。結果はハザード一覧／リスクポートフォリオに記録される。ステークホルダーの SMS からのデータも統合される。	http://www.bazl.admin.ch/

米連邦航空局（FAA）／航空機認証サービス（AIR）	安全性モニタリング／データ分析（MSAD）	安全性モニタリング／データ分析（Monitor Safety/ Analyze Data：MSAD）は、航空機製品の運用中のハザードを特定し、評価し、軽減するためのデータに基づく方法で、製品によって規定されるハザード基準を用いて航空安全データから潜在的なハザードが浮かび上がるようにする。MSAD では継続的運航安全（continued operational safety：COS）データを整理するために標準的分類法を使用して、従属変数の分析を通じて安全に関する最新動向の迅速な特定を進めている。安全問題はリスクを判定するために分析され、これにより修正処置の範囲と時期が決定される。MSAD では因果分析手法を用いる。この手法で潜在的要因、例えばプロセスの障害などを特定することができ、これが適切な航空安全機構（AVS）の監視業務プロセスオーナーに伝えられる。	http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/215154
カナダ民間航空局（TCCA）	TP 13905「リスク管理タイプ 2A（ショートプロセス）」	文書 TP 13905 "Risk Management, Type 2A (Short Process)" で従うべきプロセスについて詳しく定めている。アドバイザリー・サーキュラー（AC）107-001 "Guidance on SMS Development" でもリスク管理について詳しく規定している。	http://www.tc.gc.ca/eng/civilaviation/publications/tp13905-menu-1906.htm
ニュージーランド CAA	リスクプロフィール格付け	運航会社はそれぞれの評価セクターにおいて 1 から 5 の範囲で格付けされる。1 は模範的格付けである。定性的な評定であり、その時点での CAA スタッフと顧客とのやりとり、または CAA データベースに記録されている組織の変更にのみ関係する。 2 から 5 は、レベルの高いリスクを記録するために使用される。リスク項目には、運航会社の全体的なリスクに及びそうな影響についての CAA の評価に基づいて重みが付けられる。評価セクターそれぞれにおける評点を組み合わせると相対的なリスクプロフィールが得られ、個別の運航会社のリスクプロフィール格付け（可能性のパーセントとして表示）を図で表示することができ、同じ証明書を有する他の全運航会社の格付けと比較される。格付けは各運航会社と CAA 間の守秘事項である。	http://www.caa.govt.nz/Surveillance_System/The_Risk_Profile_Ratings.htm
国土交通省航空局（JCAB）	航空安全情報管理・提供システム（ASIMS）	運航会社は事故、インシデント、および安全運航に影響を及ぼす可能性のある出来事を ASIMS システムに報告することが義務付けられている。JCAB は報告された事象について原因を分析し、安全上のリスクを評価する。これの結果は効果的な監督を行い、必要な安全措置を講じるために利用される。	

民間航空当局のデータ活用例

事例：ANAC – ブラジル国内民間航空局 – *Decolagem Certa*（DCERTA）システム。

ブラジル国内民間航空局（ANAC）では小型民間航空のセクターにおける事故およびインシデントデータを分析することにより、事故に至った多くの運航において何らかの規則不順守のあったことが分かった。小型民間航空セクターの運航会社は数多く、ANAC は財源および人的リソースが限られていたために検査活動を通じてこうした状況を管理することは困難であった。この問題を解決するために、ANAC はデータに基づく方法によってリスクの集中箇所を特定し、検査を最適化する体系的な手法を開発することにした。

ANAC は *Sistema Decolagem Certa*（DCERTA）、翻訳すると「安全な離陸システム」と呼ばれるシステムを開発した。このシステムは飛行計画が作成されると瞬時にそのデータを収集して航空局のデータベースと交信し、パイロットのライセンス、資格および診断書、航空機証明書、ならびに各フライトの運航手順について不順守がないか探す。DCERTA システムによって収集されるこのデータは主として規則順守データであるが、社会のために安全な航空サービスを保証するための規則が整備されれば、安全関連のデータにもなる。

データは、最も頻度の高い不順守、それについて頻度の高い地域、さらには不順守率の高い業務提供者を特定するために使用される。軽減策は 2 種類の手法で講じられる。

1. 先ずは、違反と確認された不順守が規則に従って処理される。これは*受動的なリスク管理*であり、業務提供者が違法な、つまり危険な運航を続けることを禁じるために、違反を罰する。

2. 2 番目の手法は*積極的リスク管理*である。データを統計的に分析することにより、最も「順守していない」運航会社と、いっそうの注意を要するセクター（例、社員のライセンスをしっかりと管理していない運航会社）を特定することが可能になる。これにより ANAC はリスクが高いとして特定された運航会社を重点的に検査する計画を立て、大事に至る前に修正することができる。

さらに*積極的リスク管理*では、航空機の運航会社を遠隔的に監視し、指標や達成すべき将来の目標を定めることが可能である。例えば ANAC は 3 つの主な指標を通じて複数の航空セクター（商用航空、訓練、小型民間航空など）を監督している。これらの指標とは不順守全体、個人に関する不順守、そして航空機に関する不順守である。不順守と危険な運航との関係が図 4 と 5 で分かる。

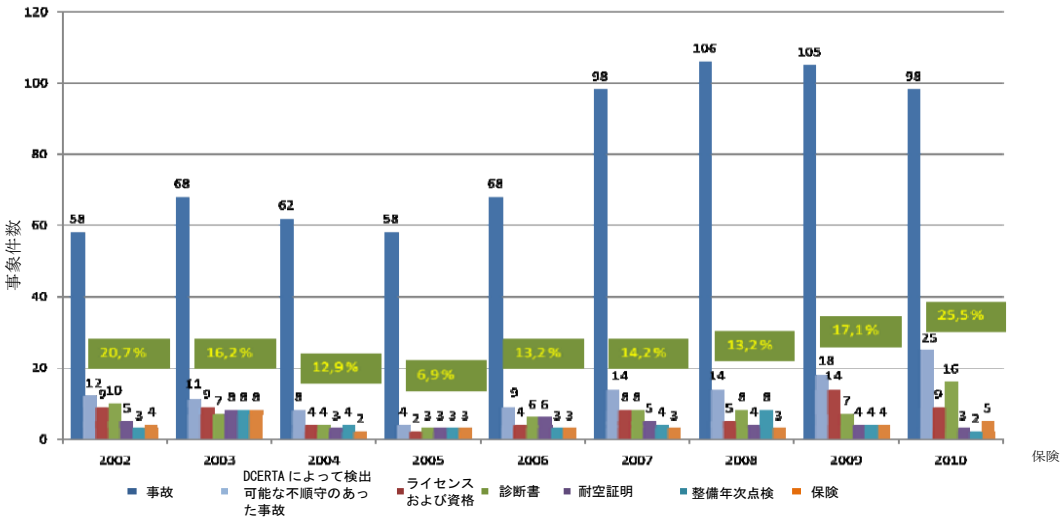


図 5: 不順守と関連事象

図 5 において、青色の棒はブラジルの民間航空（一般航空を含む）における事故件数を表しており、その他の棒は DCERTA システムによって検出された様々な不順守を表している。

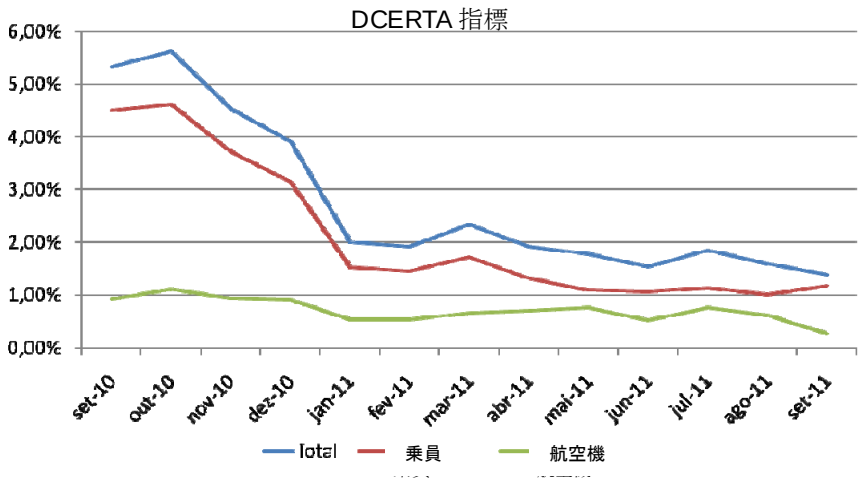


図 6: DCERTA 指標

図 6 において、青線は DCERTA システムで何らかの不順守が見つかったフライトの割合を表す。赤は乗員に関する不順守状況を表し、緑は航空機の状況を示す。図で示されているように、2011 年 9 月に不順守のあったフライトの合計数はフライト総数の 1.5%未満である。一方、図 5 において、事故に至った運航で不順守のあったフライトの合計数は 2010 年には全体の 25.5%を占めていた。

この分析は、不順守と運航に関係するリスクのレベルとの関係を非常に明確に示しており、DCERTA システムはブラジル民間航空局の安全リスク管理にとって非常に有用な手段となっている。