

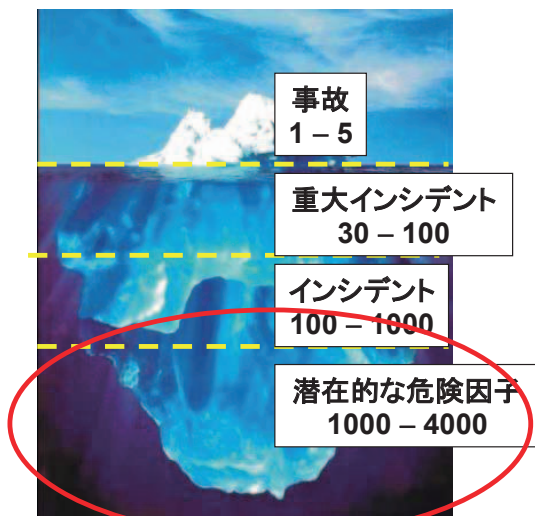
## 19. 定性的空域安全性評価手法について

航空交通管理領域 ※藤田 雅人、天井 治、森 亮太

### 1 安全管理システム

本邦では、事故・インシデントの発生の原因を個人の不注意・技量不足等に帰することが多いが、高いワークロード、マン・マシンインターフェースの不備、経済運航へのプレッシャー、安全を軽視した組織文化や規制の欠如等、個人に帰せられない要因も多い。また、それらの危険因子（ハザード・危険につながる可能性のある事象・条件）の中には、事故・インシデントに至らなかったために、表面化していないものも存在する可能性がある。

国際民間航空機関 (International Civil Aviation Organization, ICAO) のシカゴ条約付属書により、認定訓練組織、航空機の運航者、整備事業場、ヘリの整備、航空機の設計製造、航空交通業務、飛行場業務での安全管理システム (Safety Management System, SMS) の導入が義務付けられている。安全管理システムは潜在的な危険因子の発見・対策を目的としている。潜在的な危険因子を潰していくことにより、同一の原因に起因する事故・インシデントの発生を防止する。図1に概念図を示す。



安全管理システム

図1 ハイน์リッヒの法則

安全管理システムは安全方針と安全目標、安全リスク管理、安全保証、安全推進の4つの柱からなっている（図2）。安全方針の策定に際しては、管理部門の参画が必要となる。ガイドラインとしての安全方針が管理部門により定まったところで、「滑走路誤進入年間10件未満」等のより具体的な安全目標が設定される。

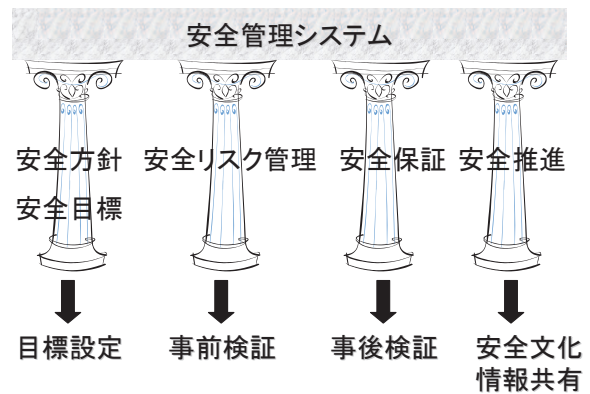


図2 安全管理4本の柱<sup>[1]</sup>

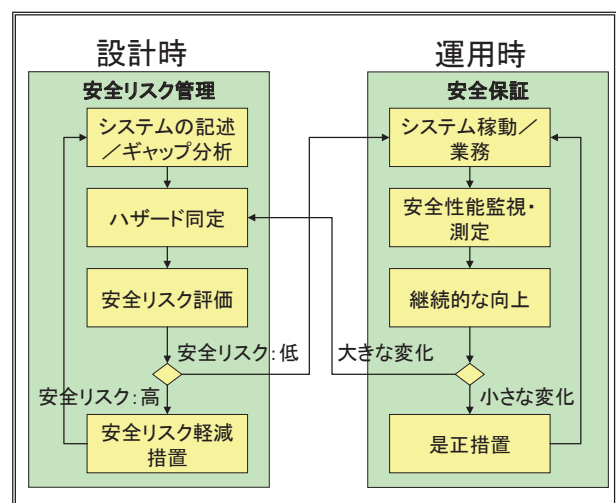


図3 安全リスク管理と安全保証<sup>[1]</sup>

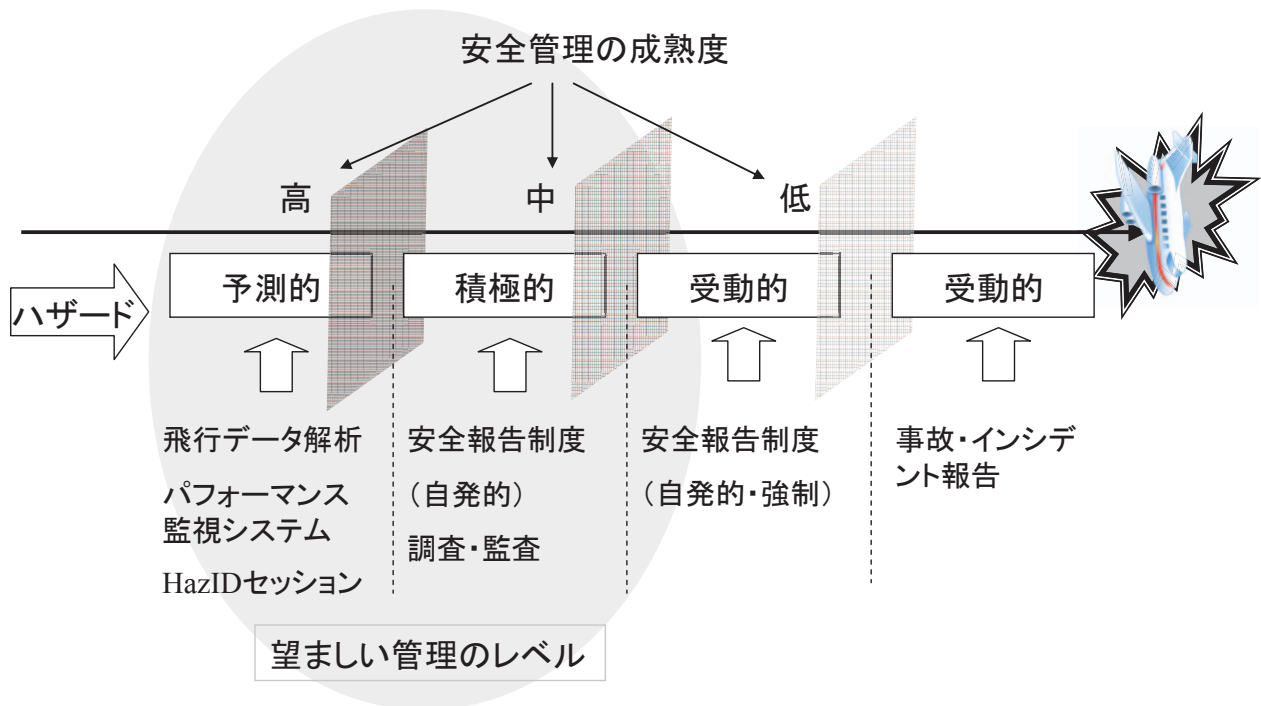


図 4 安全管理システムの成熟度とデータ源<sup>[1]</sup>

安全リスク管理は新規運航手順・システム導入前のハザード同定及びリスク評価から構成されている。一方で、安全保証では、運用状況・システムの性能等を安全の面から継続的に監視する。安全推進では、訓練や教育、対話を通じて安全文化を培うと共に安全情報の共有を図る。安全リスク管理と安全保証の関係を図 3 に示す。

安全管理システムの導入規模や成熟度は、組織やその取り組み方によって異なる。例えば、既に起こってしまったインシデントや事故からその原因を調査し、対処するという安全管理の手法がある。これは危険因子に関するデータが自ずと顕在化するまで待つ手法であり、受動的な安全管理手法である。

安全管理手法の一つとして、安全報告制度がある。事故・インシデントとして表面化はしていないものの、現場は既に潜在的な危険因子に気付いているかも知れない。安全報告制度では安全に悪影響を与える事象について現場から報告を求める。非懲罰・匿名性は、自発的安全報告制度推進のために非常に重要である。

積極的な安全管理からさらに進んだ安全管理への取り組みとして、予測的な安全管理をあげることが出来る。予測的な安全管理では、安全報告を待つまでもなく、日々のデータから潜在的な危険因子を発見・対処していく。飛行データや管制システムデータを収集・解析し、危険因子の発見や安全に係わるシステムの性能を継続的に監視していく。また、新システム・新方式の導入時には導入に先立って安全リスク評価を実施し、導入前に可能な限り危険の芽を摘んでおく。

図 4 に安全管理の成熟度とハザードに関するデータ源の関係についてまとめた。安全管理システムが成熟していくにしたがって、データ源が豊富になっていく様子が図示されている。

本稿では既存のハザード同定・リスク評価手法とその長所・短所および安全管理システムとの関係について述べていく。また、最後にこの分野での電子航法研究所の試みを紹介する。

## 2 安全報告制度・安全情報データベース

過去の事故・インシデント報告や安全報告制度により得られる安全情報を収集・整理することにより、現システムや方式に起因するハザードの情報（種別・頻度）を収集することが出来る。これらのデータは現場へのフィードバック情報として役立てることが出来る。また、他の分析手法により安全性解析を実施する際に基礎となる。コンピュータ技術の発達により、データベース化された膨大なデータから特定の情報を取り出すことは技術的には難しくない。また、登録されたメンバーに対して、インターネット経由で情報を提供することも可能である。

実際、アメリカ航空宇宙局(NASA)では、安全情報の水平展開を目的とした航空安全報告制度<sup>[3]</sup>の運用を行い、現在では操縦士・航空管制官・整備士等から3,000件/月の安全情報を入手している<sup>[2]</sup>。また、インターネットを通じたデータ提供も実施している。

当該手法により信頼できる成果を得るためには、蓄積されるデータの充実が不可欠であり、データの充実化のためには、安全報告制度の成熟化が不可欠であることは言うまでもない。

## 3 構造化ミーティング

構造化ミーティングは既存ないし新規の方式やシステムの潜在的な危険因子の同定・リスク評価手法の一つである。構造化ミーティング手法の専門家が議長となり、ミーティングを通して、評価対象となる方式やシステムの専門家(空域設計者や管制官・操縦士など)から考えうる危険因子を引き出す。専門家の経験に基づき、危険因子の発生頻度と危険因子発生時の被害の度合いを見積もり、リスク評価を行うこともある。したがって、構造化ミーティングは安全リスク管理におけるハザード同定作業において新しい設計に対する潜在的な危険因子の洗い出しに、今まで検討されなかった危険因子の引き出しに広く適用できる。図5に適用例を示す。

HAZOP (Hazard and Operability Study)<sup>[4]</sup>は構造化ミーティングの一つである。当該手法では評価対象を幾つかのノードに分割し、パラメータのズレを表すガイドワードを決定する。ノードごとにパラメータとガイドワードの組み合わせによって導き出されたズレに対して、現実的な発生原因を特定し、ズレの影響度や安全対策を検討する。

Hazard Ref:	Hazard Title	Hazard Description	Hazard Effect on ATM	Severity & Exposure Time (Ref SAM Severity Classification Scheme)	Mitigation Means
<b>OS 1 – Flight in Formation/Tail</b>					
H-[OS 1]-1	Partial Transponder failure (lost mode A)	Partial transponder failure (lost mode A) potentially leading to missed genuine alerts, when in conflict with no mode C and unassumed tracks	ATM safety not enhanced by STCA The Controller may become aware too late of a potential conflict to resolve it before a collision scenario develops. There may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Procedure for "manual correlation" to allow the track to be assumed again and STCA being fully active for the track (note that manual correlation is already normal ATCO practice at Semmerzake ATCC)
H-[OS 1]-2	Duplicate Mode A	Duplicate Mode A (due to wrong Mode A assignment by ATCO or to wrong input by pilot), leading to incorrect split track detection, with potential suppression of desirable alerts.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	- Implementation of a logic to check for termination of split track condition on each STCA cycle (proposed solution: indicate in the track format whether the track was updated by a plot or using the predicted position. The STCA alert will be suppressed when a track is not updated using the predicted position). -Use of a duplicate Mode A alert advising the controller when 2 tracks have the same mode A and allowing her/him to assess the situation (note that this feature is already present in the existing system).
H-[OS 1]-3	Lost Wingman	Lost Wingman after loss of visual contact (e.g. due to bad weather conditions) such that the wingman is no longer detected as part of a formation, potentially leading to un-alerted conflict with other un-assumed aircraft.	ATM safety not enhanced by STCA The Controller may become aware too late of a potential conflict to resolve it before a collision scenario develops. There may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Procedure for manually splitting the formation: the formation is split using a 20° angle difference between the elements. All aircraft are instructed to squawk according the manually split flight plan. Then a/c are automatically correlated.

図5 STCAに対する構造化ミーティングの適用例<sup>[5]</sup>

HAZOP は 1970 年代に化学プラントの安全性評価に用いる目的で開発され、今では、原子力産業、プロセス産業、ソフトウェア開発等に適用されている。ATM 分野でも、ASAS への適用等適用事例がある<sup>[6]</sup>。

#### 4 リアルタイムシミュレーション

Human In The Loop(HITL)シミュレーションであり、リスクのない状態で、現実に近い環境を再現できる。実施方法としては、管制を行わず交通をフォローするのみの「シャドー・モード・トライアル」と実際に管制を行なう「生のトライアル」を実行することが出来る。リアルタイムシミュレーションは、安全リスク管理フェーズでの危険因子の洗い出し、洗い出された危険因子の発生頻度の解析に用いることが出来る。EUROCONTROL 実験センターでは安全を扱う上でよいと考えられるシミュレーションの実施例をまとめている<sup>[7]</sup>。

発生頻度が稀な危険因子や事象を考える場合、シミュレーションシナリオにおける危険因子の発生頻度が高く設定されていることが多く、管制官の反応が現実と異なることがあるという短所がある。

#### 5 事象木、故障木、蝶ネクタイ

事象木・故障木分析は原子力分野<sup>[8]</sup>で広く用いられ、現在、航空を含む多くの分野で用いられている。

事象木分析とは、危険因子から開始し、それに引き続いて起こる事象（対応策・防護システム）を考えることにより、重大な結果（事故等）に至るプロセスと（各分岐での発生確率が分かれば）重大な結果の発生確率を計算することが出来る。図 6 に事象木のイメージを示す。

また、故障木分析とは、事象木分析とは逆に、危険因子の原因となる下位の事象を考えることにより、危険因子の発生プロセスと（各分岐での発生確率が分かれば）発生確率を計算することが出来る。図 7 に故障木のイメージを示す。

これらの手法は、安全リスク管理における安全リスク評価作業で用いることが多い。

蝶ネクタイ分析は、リスクの定量化が不可能

か必須ではない安全リスク評価への構造的アプローチ手法である。蝶ネクタイ図は幾つかの種類が存在するが、多くの場合、蝶ネクタイの結び目は危険因子を、左側は危険因子を引起す可能性のある因子を、右側は危険因子の引起す結果を図示する。蝶ネクタイ図の主な役割は、重大な危険因子がどのように発生し、それに対してどのような安全防護が存在しているかを図示することにある。図 8 に蝶ネクタイ図のイメージを示す。図 8 の例の場合、蝶ネクタイの左側が故障木に、右側が事象木となっている。図 8 下のフロー図は管理システムや手順等を表している。

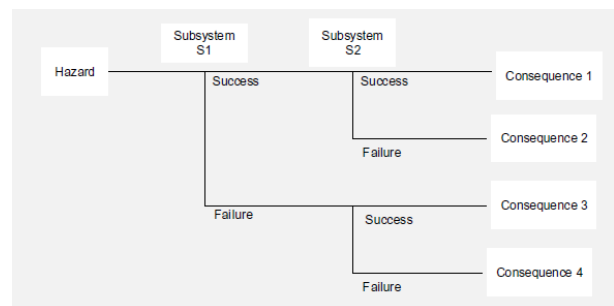


図 6 事象木 [2]

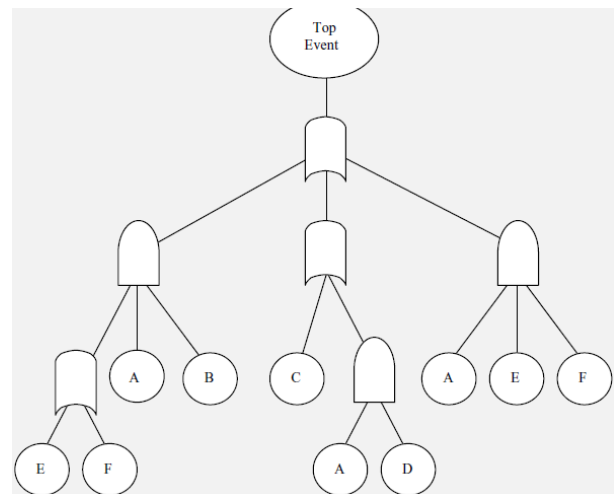


図 7 故障木 [2]

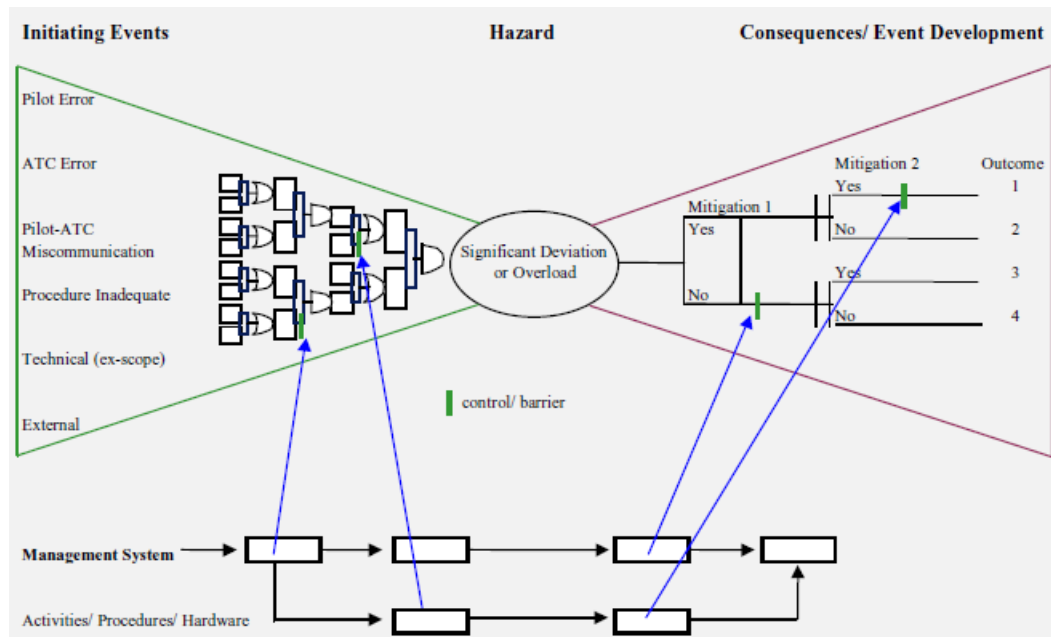


図 8 蝶ネクタイ分析 [2]

## 6 ヒューマンファクター

管制官や操縦士等の人間は航空交通管理システムの中でシステム要素の一つとして、重要な位置を占めている。それ故、上記の手法を人間に適用するだけでなく、認知的アプローチ等人間を対象とした特別な手法も多い。ただし、本稿では割愛する。

## 7 ハザード追跡，長期自動監視

第 3 章から第 6 章までは、主に新システム・新手順導入前の安全リスク管理フェーズにおいて適用される手法を紹介した。しかし、安全管理マニュアル<sup>[1]</sup>でも述べられているように、安全リスク管理だけでは十分ではない。運用中も変わらず安全であることを保証し続ける安全保証業務も重要となる。そのためには、以下を実施する必要がある。

1. 安全リスク管理フェーズで見逃した危険因子の同定
2. 安全リスク管理における解析で仮定された仮定の継続的な妥当性検証
3. 特定された危険因子の発生頻度の確認

項目 1 は第 2 章で述べた安全報告制度・安全情報データベースの運用を通して実現していく。

項目 2 及び項目 3 は既知の事象の監視であり、可能な限り、系統的・網羅的かつ継続的に実施される必要がある。

項目 2 及び項目 3 のための手法の例として米国でのレーダデータによる自動的安全性能監視システム PDARS (Performance Data Analysis & Reporting System)<sup>[9]</sup>がある。PDARS はアメリカ航空宇宙局とアメリカ連邦航空局が共同開発したレーダデータのネットワーク化と分析用ツールである。PDARS により、各施設の意思決定者は、安全性だけでなく、ATC 運用の健全性、遂行能力等を監視することが出来る。PDARS は安全管理システムにおける安全性能監視活動の一部を担う。

PDARS の主要機能は以下の 4 つである。

1. 航跡データと飛行データの自動収集・解析
2. 日報の自動生成
3. GRADE (Graphic Airspace Design Environment) による可視化
4. PDARS WAN によるデータと報告書の配布

## 8 電子航法研究所の試み

電子航法研究所の空域安全性研究チームは、長らく ICAO で開発された衝突危険度モデルの研究を行なってきたり、現在も継続している。しかし、当該手法は航空機管制間隔の安全リスク評価や安全性能監視・測定（図 3 参照）のための手法であって、危険因子同定の手法ではなかった。成熟した安全管理システムの構築のためには、危険因子同定のための手法の開発も必要であると考え。したがって、電子航法研究所の空域安全性研究チームは現在 WebHIRAS の開発に着手している。WebHIRAS とは Web2.0 技術<sup>[10]</sup>を用いた危険因子同定・定性的リスク評価支援ツールである。第 3 章で述べたように、多くの場合、危険因子の同定は構造化ミーティングにより行なう。ミーティングには、以下のような問題点がある。

- 参加者のスケジュール調整の困難さ
- 遠隔地からの参加コスト
- 限られたミーティング時間
- 記録の手間

一方で、一方的な情報提供ツールであった Web 技術が電子掲示板・チャット・twitter<sup>[11]</sup>といった双方向コミュニケーション手段として成熟している。これらは、参加者がいつでも好きなときに参加でき、遠隔地でも簡便安価に接続でき、長時間にわたる意見収集が可能で、別途発言内容を記録せずとも、書き込まれた内容がそのまま記録となる。

WebHIRAS では 3 種類のユーザが想定されている。構造化ミーティングの議長や事務局の役割を担う「管理者」、構造化ミーティングの参加者に対応する「評価者」、Web 技術の問題に対応する「Web 技術者」である。管理者は、問題の設定、必要な資料の収集・提供、スケジュールの策定、評価者からのリスク評価対象に対する質問への回答、評価者の誘導、報告書の作成を行なう。

評価者は、評価対象となる資料を熟読のうえ、WebHIRAS を用いて思いついた危険因子の書き込み、経験に基づくリスク評価、コメントの書き込みを行う。表 1 と表 2 に危険因子の発生頻度・被害の深刻さの分類例を示す。評価者は自らの経験や専門的な知見に基づいて、発生

頻度・被害の深刻さの分類から評価対象の危険因子に当てはまるものを選択する。意見が大きく割れる場合には電子掲示板等で議論し、決定する。（決定には「情報不足により不明」も含まれる。）

Web 技術者は WebHIRAS の使い方等、管理者・評価者からの技術的な質問に対応する。

WebHIRAS にも問題点はある。WebHIRAS はパソコンの使用を前提としているため、パソコン等に不慣れな参加者にとっては使い辛いものとなるということである。この問題に関しては、高齢者向け携帯電話の成功が教訓となる。携帯電話はメール・カメラ等電話本来の機能を満載し、操作の習得に非常な困難を伴っていた。現在では、携帯電話各社は「大きなボタン」「読みやすいディスプレイ」「シンプルな機能」の高齢者向け携帯電話サービスを提供している。

WebHIRAS においても、「シンプル」をコンセプトとしたデザインを採用し、可能な限りユーザフレンドリーな環境を提供する予定である。

WebHIRAS が抱えるもう一つの問題点は、他の参加者の発言内容が Web にアクセスしない限り確認できないということである。常に発言があったか否か確認のために Web にアクセスすることは煩わしい。これに対処するために、WebHIRAS では、他の参加者の発言があったときに自動でその内容を参加者にメールで通知する機能をつけている。

頻度分類	頻度
ありうる	1 日に 1 回起こる
起こりそうにない	1 年に 1 回起こる
全く起こりそうにない	100 年に 1 回起こる
ありえない	100 年に 1 回も起こらない

表 1 発生頻度の分類例<sup>[12]</sup>

深刻さ分類	1	2	3	4	5
影響	安全マージンの完全な喪失	安全マージンの大幅な喪失	安全マージンの喪失	安全マージンの軽微な喪失	安全に対する影響なし
影響の例	以下に例示される事故 ・単独／複数の壊滅的な事故 ・単独／複数の空中衝突 ・単独／複数の地上での航空機同士の衝突 ・単独／複数の管制下・操縦可能状況下での進入禁止区域への侵入 ・完全に操縦不可能 監視や交通管制・操作手順等の事故を防止するような（考察対象となっている危険源とは）独立な回復手段がない	以下に例示される重大なインシデント ・操縦士・管制がコントロールしていない状況ないしそのような状況から回復できない状況での大きな管制間隔（例：管制間隔基準の半分以上）の喪失 ・単独／複数の航空機のクリアランスからの逸脱で、事故の回避（やその他回避行動が求められる）のため急激な衝突回避行動や進入禁止区域進入回避行動が必要	以下に例示されるインシデント ・操縦士・管制がコントロールしている状況ないしそのような状況から回復できる状況での大きな管制間隔（例：管制間隔基準の半分以上）の喪失 ・操縦士・管制がコントロールしていない状況ないしそのような状況から回復できない状況での小さな管制間隔（例：管制間隔基準の半分以下）の喪失。（衝突回避行動や進入禁止区域進入回避行動なしでは）そのような状況から回復することが出来ない。	以下に例示されるインシデント ・安全に直接の影響はないが、管制官や操縦士のワークロードの増加やCNSシステムの機能低下等により、間接的に安全に影響のある状況 ・操縦士・管制がコントロールしている状況ないしそのような状況から回復できる状況での小さな管制間隔（例：管制間隔基準の半分以下）の喪失	運航に直接・間接の影響がない状態

表 2 被害の深刻さの分類例<sup>[12]</sup>

## 9 まとめ

本稿では ICAO が導入を進める安全管理システムを概説し、それを支える危険因子同定・リスク評価技術等を紹介した。最後に、電子航法研究所の試みとして、Web2.0 技術を用いた危険因子同定・定性的リスク評価支援ツール WebHIRAS を紹介した。WebHIRAS は現在開発中であり、本年度中のプロトタイプ完成を目指している。

## 参考文献

- [1] Safety Management Manual, ICAO Doc 9859, 2<sup>nd</sup> ed., 2009
- [2] FAA/EUROCONTROL ATM Safety Techniques and Toolbox  
[http://www.eurocontrol.int/eec/gallery/content/public/document/eec/report/2007/023\\_Safety\\_techniques\\_and\\_toolbox.pdf](http://www.eurocontrol.int/eec/gallery/content/public/document/eec/report/2007/023_Safety_techniques_and_toolbox.pdf), 2<sup>nd</sup> ed. (2007)
- [3] Aviation Safety Reporting System  
<http://asrs.arc.nasa.gov/>
- [4] Kletz, T. Hazop and Hazan, 4<sup>th</sup> eds., Taylor & Francis, 1999.
- [5] EUROCONTROL Guidance Material for Short Term Conflict Alert Appendix D-2: Functional Hazard

- Assessment of STCA for ATCC Semmerzake, EUROCONTROL, 2006.
- [6] COSPACE HAZOP REPORT, available from internet, EUROCONTROL 実験センター, 2005
- [7] Antonini, A., Karmarque, Y., HITL Safety Experiments Guide, EUROCONTROL 実験センター, 2004
- [8] （社）日本原子力学会標準，原子力発電所の停止状態を対象とした確率論的安全評価手順，AESJ-SC-P001:2002, 2002
- [9] den Braven, W; Schade, J., Concept and Operation of the Performance Data Analysis and Reporting System (PDARS), ATAC Corporation, 2003
- [10] <http://oreilly.com/web2/archive/what-is-web-20.html>
- [11] <http://twitter.com/>
- [12] EUR RVSM PROGRAMME FUNCTIONAL HAZARD ASSESSMENT, EUROCONTROL, Working Draft, 2001