TALKSAFE2006　特別講演

リスクを見つけて制御する

筑波大学大学院　教授　**稲垣　敏之**

本日は「リスクを見つけて制御する」というタイトルでお話しさせていただきたいと思います。私はヒューマンエラーの講義をすることもありますが，ほとんどの事例は私自身の経験でまかなえるほど頻繁にヒューマンエラーをやっておりますので，今日は自戒も込めてお話しさせていただきます。

認知がすべての根源

「ベテランがエラーを犯すということは，あってはならない」という論調で報道されることがあります。特に事故が起こると，ヒューマンエラー糾弾の大合唱となりますが，その中でよく聞かれる言葉が，「信じられないミスである」，「決して起こしてはならないミスである」，「ベテランにあるまじき初歩的なミスである」といったものです。しかし，エラーを犯した当事者への非難や糾弾は全く不適切です。

エラーの背景にある様々な要因を理解し，本人をその場面に追い込んだものが何であるかをよく把握しておかなければいけない，これが非常に重要な視点であると考えます。このことは全日空・総安推発行の『ヒューマンファクターズへの実践的アプローチ』の中でも紹介されています。

航空事故の原因の7～8割をパイロットのエラーが占めると言われます。確かに一つの主原因を割り当てれば，表1のように，パイロットのエラーが約7割を占めます。しかし，多重要因で分析すれば，表の右欄にあるように，整備，設計・製造，マネジメントにかかわる要因も少なくなくありません。このことからも分かるように，事故の原因は一つではないという視点

表1　航空事故の原因分析例

原因	主原因で分析	多重要因で分析
パイロット	72%	70－75%
整備	3%	30－35%
設計・製造	13%	15－20%
マネジメント	－	60－80%
その他	12%	－
合計	100%	

（ヒューマンファクターズへの実践的アプローチ，1993）

が非常に重要となります。

さて，われわれの日常生活や業務は意思決定の連続です。「認知 → 判断 → 操作」が繰り返されているということです。分かりやすい例を挙げますと，「この部屋は寒い」と感じるのが「認知」，それから「エアコンの設定温度を上げよう」と思うのが「判断」あるいは「意思決定」，そして，リモコンを使って設定値を変更するのが「操作」あるいは「行動」です。設定値を変更した後，それでもまだ寒いと認知したら，もう少し温度を上げようと意思決定し，リモコンを押す行動を取る，というように繰り返すことになります。

ところが，「この部屋は寒い」と感じなかったら，設定温度を上げようと思うはずがありません。さらに，設定温度を上げようと思わなければ，当然リモコンを使って設定温度を変えることもありません。ですから，一番根源にあるのが実は認知なのです。

事故が起きた時，「オペレーターが状況を正しく認識しておれば，このような事態には至らなかったはずである」と言われることがありますが，これも認知が根源であることを表しています。身近な例でご説明しましょう。

（例）あるグループで緊急会合が招集され，重要事項を1時間で決定しなければいけない。会議室は非常によく冷房が利いているが，リーダーは暑がりなのか，プレッシャーがあるのか全く意に介していない。しかし，メンバーは寒くてたまらない。「何とかしてほしいな」「誰かがリーダーに言ってくれないかな」と，お互いに顔を見合わせている。さて，会議の結論は……。

このような状況では，誰も議論に身が入らず，意味のある結論は出てこないだろうと想像が付きます。つまり，この例では，リーダーが状況を正しく認識していなかったわけです。

ここで，研究の場においては，状況認識についてどのような議論がなされているかご紹介しておきたいと思います。

状況認識（situation awareness）は，3つのレベルがあると考えられています。

■状況認識（situation awareness）

レベル1：何かが起こっていることに気付く
レベル2：その原因を特定できる
レベル3：これからの事態の推移が予測できる

まず，何か変だということに気付き，次に原因を特定し，そして，これからどういう事態に移っていくか（ここで行動を取ればどうなるか，取らなければどうなるか）を予測できるということで，レベル3までいけば，状況認識は完了したことになるわけです。「まあ，レベル3は無理としても，レベル1の気付くことくらいは簡単であろう」と思いたいところですが，残念ながらそうでもありません。

例えば，1986～1992年までの航空のインシデントの研究報告では，次のようになっています。

●状況認識エラー169個の分類

レベル1	80.2％
レベル2	16.9％
レベル3	2.9％

（Jones & Endsley, 1995）

つまり，何か変だということにすら気付かなかったのが80％も占めるということですが，気が付かなかったら，その先の対処などできるわけがありませんので，これは非常にゆゆしき問題です。

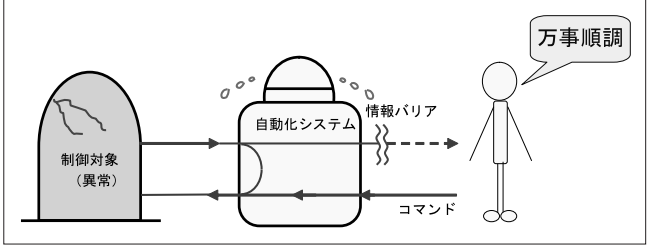
状況認識の失敗

それでは次に，それぞれのレベルの失敗例を挙げながら，問題点を探っていきたいと思います。

レベル1：「気付き」の失敗

まずは「レベル1　気付き」の失敗です。例えば，高度自動化が進んでいる現在，制御システムはかなり強力な制御能力を持っていますので，図1に示すように，制御対象に多少異常が生じたとしてもそれを隠蔽してしまうことがあります。自動化システムは自分が（汗をかいて）大変な仕事をしていることを積極的に人間に伝えようとはしませんし，長時間働いても文句も言いません。人間の方は情報が十分に提示されていなければ「何事もなく動いている，万事順調」と思ってしまいますから，変だということすら気付かないということが起こり得るのです。

図1　制御対象に生じた異常を隠蔽する強力な制御能力

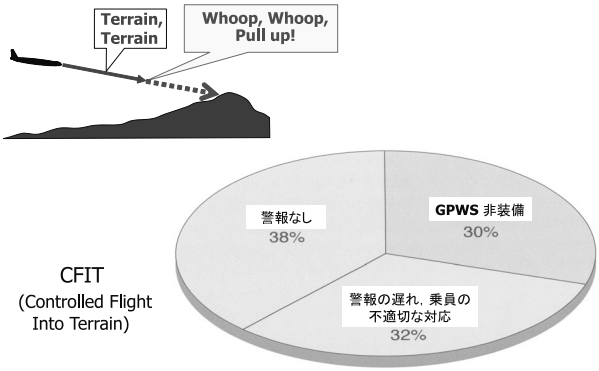


その例として，1985年，サンフランシスコ沖でボーイング747が10,000mほど落下した事故があります。第4エンジンが止まってしまって，機首が右に振れてきたのですが，自動化システムはラダーを使うタイプのオートパイロットではなかったので，バンクをとって機首を起こそうとしていました。しかし，パイロットは操縦桿を握っていなかったので，バンクがどんどん大きくなっていく様子に全く気が付きませんでした。そうして最後に，速度回復が十分できない，オートパイロットに任せておけないという段階になって，オートパイロットを切りました。その時まで自動化システムにはものすごく大きな力が掛かっていたのですが，パッと切られてしまったので，機体は裏返った形で10,000mも落ちてしまったのです。

「システムへの過度の信頼がもたらす警戒心の欠如」も気付きの失敗につながります。現在の自動化システムは非常に能力が高く，しかもめったに壊れることがありません。「万が一異常があっても，警報が知らせてくれるはずだ」と期待しても全然不思議ではありません。「有能な部下なので，任せておいて大丈夫だろう」というわけです。そうなると，その部下がどういう仕事をしているか細かく注意を向けようとはしなくなります。

異常があったら警報が鳴るであろうと思っていたのに，実際は鳴らなかったというケースとしてよく知られている中に，古典的なタイプのGPWSに関するものがあります。図2はCFIT事故の調査結果ですが，約3分の1が警報がなかったものです。パイロットは「もし前方に地表面が現れた場合，GPWSが必ず警報を出してくれるはずだ。それに即して自分が対応すればよい」と考えていたと思います。ところが，古典的なGPWSは地表面のすべての形状に対応できたわけではなく，不得意な形状もありました。従って，GPWSが不得意としている形状に対して向かっていた場合は，警報が出ずに，パイロットも気付かないままぶつかってしまうことも起こり得るわけで，調査結果ではこれが3分の1もあったということです。

図2　CFIT事故の調査結果



(Bresley & Egilsrud, 1997)

レベル2：「原因特定」の失敗

「レベル2　原因特定」の失敗のケースは，大体3つに分類することができます。

(1)「現象→原因」の形のルールのうち，その場面に該当しないものを適用する。
(2)「現象」が未知の現象であり，何がその現象を引き起こしているのか分からない。
(3)「現象」に対して「合理的」に見える説明を付けることができれば，それで納得する。

(1) はある現象が起こったとき，それを引き起こす原因についての知識が十分あるにもかかわらず，違う

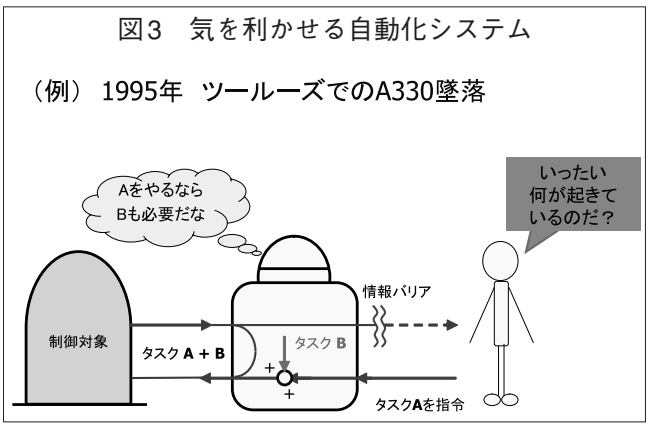
知識を適用してしまったために原因特定に失敗するというケースで，プロフェッショナルの方々にも起こり得ると思います。

特に今ここで取り上げたいのは（2）と（3）のケースです。事例を挙げて紹介したいと思います。

（2）は現象が未知の現象であり，何を意味しているのかよく分からないというケースです。「オートメーション・サプライズ」と言われる現象もその一つと言えます。

例えば，人間が自動化システムにAというタスクを指示した時，自動化システムは「Aをやるなら B もやっておいた方がいい」と判断し，事前に人間に知らせることなく，A を実行する時に自動的に B を始めることがあります（図3）。そうすると人間は，B を指示した覚えはないのに，A に重なって B も出てきてしまうため，何が起こっているのか分からなくなってしまうのです。

図3　気を利かせる自動化システム



1995年，ツールーズでテスト飛行中のエアバス330が墜落しました。エンジンを一つ切った状態でテイクオフの性能を調べているうちに起こった事故です。パイロットには十分な知識があったのですが，自動化システムが，自分が思っていたのと違うことを，違ったタイミングでやってしまったために，眼前の奇妙な現象の原因が分からなかったのです。

（3）は，現象に対して「合理的」に見える説明を付けることができれば納得してしまうという，人間の特性に大きくかかわるもので，プロフェッショナルの世界でも起こり得ます。

1995年，ニューヨーク発フランクフルト行きのDC-10が誤ってブリュッセルに着陸してしまいました。客室乗務員は，フライト中にPassenger Flight Information Systemのモニターに映し出された映像がフランクフルトではなくブリュッセルに変わっていることに気付いていましたが，「きっとモニターの設定が悪いだけだ」と考えて，コクピットには知らせませんでした。ところが，そのモニターはFMSに連動しており，パイロットが誤って目的地をブリュッセルと入力していたのです。客室乗務員は，変だと思った現象に対してある意味で合理的な説明を付けて納得してしまったので，そこから先，何の行動をとらなかったのです。

レベル3：「予測」の失敗

「レベル3　予測」の失敗は，原因は特定できているのですが，「今，対応しなくても大丈夫だろう」と思ってしまうケースです。2005年6月，六本木ヒルズで回転ドアによる死亡事故が起こりました。そのドアに問題があることは，事故以前にすで分かっていたということです。しかし，今やらなくても大丈夫だろうと安全対策を先送りにした結果，事故に至ってしまったのです。こういうものが状況認識のレベル3の失敗と思われます。

状況認識の改善

個人として起こりうる状況認識の失敗についてお話ししてまいりました。それでは，一人では失敗することでも，チームを組めば改善されるのでしょうか。実はそれもそれほど簡単なことではありません。

図4は1992年1月20日，エアバス320がストラスブール空港手前の山中に墜落した事故の状況図です。この事故はヒューマン・インタフェースに絡む大事故として非常に有名になりましたが，その背後にもう一つ別の要因があることが分かっています。

パイロットはストラスブール空港に向かってフライトパス3.3度で降りようとしていました。しかし，実行されたのは3,300ft/mの降下だったのです。パイロットが頭に描いていたのは，図5の上の画面で，右端に「FPA（フライトパスアングル）-3.3」と書かれています。ところが実際には，コンピュータにデータ入

図4　チームを組めば状況認識は改善されるか

（例） 1992年1月20日，A320 がストラスブール空港
滑走路端から19.5kmの山中に墜落

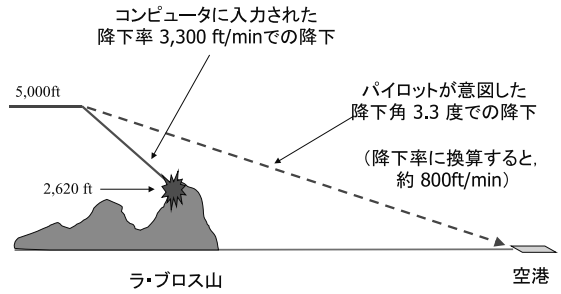


図5　降下角モードのつもりが降下率モード

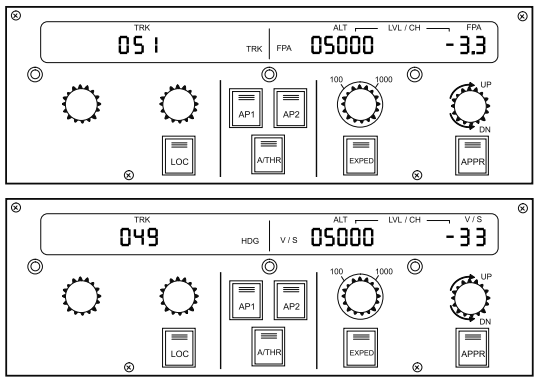
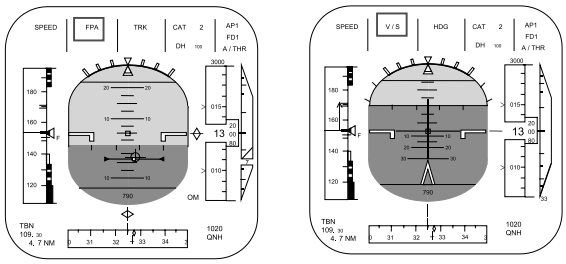


図6　PFD上には手掛かり情報があったのだが

Flight Path Angle (FPA)　3.3 °　　Vertical Speed (V/S)　3300 ft/min



（事故のモンタージュⅦ, 1997）

力する時，真ん中のプッシュボタンを押す回数が適切でなかったために，下の画面のようにバーティカルスピードモードになっており，「V/S -33」と表示されていました。

コンパクトなデザインをする時には，同じ入力装置をボタンの切り替えによって違った意味で使う「モード」が導入されるわけですが，これは「モードエラー」というヒューマンエラーを引き起こす大きな原因になっています。それから，バーティカルスピードの-33は3,300の意味なのですが，下二桁の00を省略されていたことも問題になりました。なお，現在は00が表示されていますので，こうした問題は起こらなくなっています。

この事故の詳細な調査結果が『事故のモンタージュ第7巻』に紹介されており，それを基に書いたのが図6です。これを見ても分かるように，プライマリーフライトディスプレイ上にはモードが違うことの手掛かりは十分あったはずです。つまり，フライトパスアングルを指定した時は「FPA」と表されますが，事故機ではバーティカルスピードの「V/S」が表示されていたはずで，これに気付くべきでした。さらに，空と地面の比率が違っていますから，パイロットは何か変だと気付いて当然だったのです。

それでは，なぜ気が付かなかったのでしょうか。『事故のモンタージュ』は人間関係のまずさを指摘しています。

副操縦士は技量に対して自信に満ちており，一方の機長は自信がなく，VOR-DMEアプローチは乗り気でなかったようです。副操縦士は，機長は気圧高度計の設定を誤っているとか，機長の操作では所定のコースに乗れないとかいろいろ気になり，コースに乗るには何をすべきかを機長に指示したりもしています。そして，実際は高度，降下率，速度などをコールアウトしなければいけない立場にあるのに，機長の操縦に気を取られているうちに，自分のなすべきことを怠ってしまったのです。

機長の方は，気象条件を尋ねても客室乗務員と話し込んでいて即座に返答しない副操縦士を，気に入らないと感じていました。

このように機長と副操縦士の人間関係がうまく成立していなかったわけですが，権威勾配がフラットになりすぎることがグラスコックピットの問題の一つとして指摘されています。とは言え，逆に権威勾配が大きすぎると，言いたいことも言えなくなり，やはり非常に困った問題が起こることは，皆さんもよくご存じだと思います。

1977年3月27日，テネリフェ空港滑走路上で2機のボーイング747が衝突しました。副操縦士はクリアランスがまだ出ていないことに気付いていたのですが，滑走し始めようとしているキャプテンにそのことを伝えませんでした。なぜなら，キャプテンが非常に偉大な方だったために，自分の意見を言うことができなかった，つまり権威勾配が強すぎたのです。

リスクの認知

状況認識エラーについて説明してまいりましたが，その背後にあるものについても考えてみる必要があると思います。

まず，「何か変だ」ということに気付いたのに，そのまま放置してしまうという場合がありますが，なぜ放置したかについては，次のように考えてしまうことが原因かもしれません。

○私が間違っているのかもしれない。
○私が言わなくても，誰かが気付くだろう。
○面倒なことに巻き込まれたくない。
○そのうち，この現象は消えるかもしれない。

いずれにしても，「何が問題か」ということを知りつつも，対策を先送りする場合であり，どの場合も「リスクの認識の失敗」であると言うことができます。

ここで「リスク」という言葉を使いました。また，講演のタイトルにも使っています。われわれは「リスク」という言葉を日常的に使っていますが，実はいろいろな意味があり，どういう意味で使うかによって若干ニュアンスが違ってきます。そのことについて，少しご説明したいと思います。

「リスク」には，大きく3つくらいの違った意味があります。

(1) 事故・災害・危難など，個人の生命あるいは健康に対して危害を生じさせる事象

例えば，旅行保険を掛ける際に，「スカイダイビングなどのリスキーな行為の予定はありませんか？」と聞かれることがありますが，ここで言うリスキーな行為とは，自分の生命に対して危害を及ぼすような行為のことですから，リスキーを「危ない」と言い換えることもできます。

(2) 危険な事柄，あるいは損失を生じる確率

「この薬は効きますが，副作用が発生するリスクが20％ほどあります」と医者に言われた場合のリスクは「確率」という意味で，「この薬はよく効きますが，副作用発生の確率が20％ほどあります」と言い換えてしまえば分かりやすくなります。ただし，確率という意味でリスクを使うのは，副作用発生というような望ましくものに対してだけで，望ましいものに対して，例えば，「3億円の宝くじに当たるリスクは」という言い方はしません。

(3) 損失の大きさとその発生確率との積

エンジニアなどが「リスクを小さくしましょう」と言う時のリスクがこれであり，小さくするには2通りの方法があります。一つは好ましくない事象そのものを起こりにくくする，すなわち発生の確率を下げる方法，もう一つは，確率を下げることが無理な場合に，起こった時の損失を小さく方法です。2通りのやり方で対応しようとするのがエンジニア的発想です。

リスクの定義は終わりましたが，これで問題が解決するわけではなく，私がここで申し上げたいのは，リスクの認知は非常に難しいということです。

皆さんのようなプロフェッショナルではなく，一般人の場合としてお聞きいただきたいと思いますが，これに関しては有名な実験がいくつもあります。それをまとめると，大体次のようになります。

(1) ある病気にかかる確率は低くても，その病気にかかった時に死亡する確率が高ければ，その病気の死亡率を過大評価する。
(2) 確率の低い現象の生起確率は実際より高く感じ，確率の高い現象の生起確率は実際より低く感じる。
(3) 人の判断や意思決定は，質問の文脈や言い回しに影響を受ける。

まず，次の例について考えてみましょう。

(例) 1万人に1人の割合で感染する恐ろしいウイルスがまん延しています。T大学附属病院が99％の確率でこのウイルスへの感染の有無を正確に判定できる検査法を開発したというので，Yさんはその検査を受けてみました。結果は陽性で，Yさんはすっかりしょげてしまいました。

このような状況に置かれたら，誰もがかなりショックを受けると思います。しかし，実際にYさんが感染

している確率は1％しかありません。このトリックがどこにあるかと言えば，「1万人に1人の割合でしか感染しない」ことです。1万人全員が検査を受けたとすると，約100人は「陽性」と言われます。ところが，本当に陽性の人は1人しかいないはずですから，陽性と言われた100人のうちの99人は陰性です。ですから「陽性」と言われた人が感染している確率は1％しかないのです。これは検査法の精度にだまされてしまって，本来の罹患の確率とうまく統合することができないという有名な事例です。

次に，(2) ですが，自動車事故と航空機事故を比べると，発生率は自動車事故の方がはるかに高いわけです。さて，何の予備知識もない人に，これらの事故で年間どのくらいの方が亡くなると思いますかという質問をした場合，その人の答えを実際のデータを対応させると，航空機事故の死亡者数を高く見積もる傾向があります。これは，飛行機事故の発生率は低いのに，起こるとよく目立つために，実際より確率が高いと感じてしまうと考えられます。

それでは，(3) について，皆さんに問題です。

【質問1】　600人を死亡させる病気が突発的に発生する可能性がある。現在，次の2つの対応策が検討されているが，意見がまとまらず，最終的には委員長に判断をゆだねることになった。もし皆さんが委員長だったら，どちらを採用しますか。

対応策1：200人が助かる。

対応策2：600人全員助かる確率が3分の1。

【質問2】　600人を死亡させる病気が突発的に発生する可能性がある。現在，次の2つの対応策が検討されているが，意見がまとまらず，最終的には委員長に判断をゆだねることになった。もし皆さんが委員長だったら，どちらを採用しますか。

対応策3：400人が死亡する。

対応策4：600人全員死亡する確率が3分の2。

すでにお気付きの方もおられると思いますが，対応策1と対応策3，対応策2と対応策4は全く同じものです。さすがに全日空の皆さんは冷静な方が多いようですが，一般の実験では，質問1の場合は対応策1を選ぶ人が多いという結果が出ています。200人が助かるというポジティブな意味合いで表現されると，誰も助からない確率がある方法を採るより，200人を確実に助ける方が良いとはずだと考えてしまうのです。

質問2の場合は逆に対応策4を選ぶ人が多くなります。200人助かるというのと，400人死亡するというのは全く同じ意味なのですが，確実に400人が死亡してしまうという望ましくない表現をされると，確率に掛けてみる方がいいだろうと思ってしまうのです。

このように，実際には同じものであるにもかかわらず，文脈によって結論が変わってしまうことがあります。こういう現象を知っていると，実は悪用することもできます。結論をどちらかに誘導したい場合には，聞き方を調整すると可能になるかもしれません。

信頼と過信

さて，「今の事例は一般の場合であり，プロにはあり得ない」と思いたいところですが，実際には対象について豊富な専門知識を持っている人，つまりプロフェッショナルな方でも的確にリスクを認知できるとは限りません。その大きな落とし穴の一つが「過信」と言われるもので，ベテランの「豊富な経験」や「長年の安全実績」が，かえって安全を損なうこともあるのです。

そこで，「過信」についてお話ししたいと思いますが，その前に，「信頼」とはどういうことか，ご理解いただく必要があると思います。

信頼は4つの次元からなっていると考えていただいてよいと思います。

■信頼（trust）

基礎：自然界の法則や社会の秩序に合致している。

能力：常に安定的かつ望ましい行動や性能が期待できる。

方法：行動を実現するための方法，アルゴリズム，ルールが理解できる。

目的：上記の背後にある意図・動機が納得できる。

（Lee & Moray, 1992）

まず基礎的な部分ですが，例えば今私が，「私の足

は床から2cm，常に浮いています」と言えば，皆さん，「何をばかなことを」と思われるでしょう。それでも，「いや，絶対そうなんです」と言ったら，それから先の私の話は信用しなくなると思います。それは自然界の法則に合致していないことを主張する者を信頼できないからです。社会の秩序に合致していないものも信頼することはできません。

次に能力についてですが，例えば私が，AさんかBさんのどちらかに仕事を頼もうと思ったとします。Aさんは非常に能力が高いが，気まぐれで，気が乗らなければちゃんとやってくれない。BさんはAさんほど仕事の能率は良くないけれど，確実にこなしてくれる。私としては当然Bさんに頼みたいと思うわけです。それは，頼んだことに対して常に安定的に結果を返してくれるからです。

方法，アルゴリズム，ルールが理解できることも信頼の一つの要素です。例えば，Cさんは非常にいい仕事をしてくれるけれど，私にはどんなやり方で，どんな考え方で行動しているか分からないという場合は，一抹の不安を覚えるでしょう。

そして，これらの背後にある意図，動機が納得できることも信頼を獲得する大きな要素になります。例えば，Dさんはいつも非常に親切にしてくれる。だけど，なぜ私に親切にしてくれるのか分からない，何か魂胆があるのかもしれないと思う場合は，背後にある意図や動機が納得できないので安心感を覚えないのです。

人が人を信頼するかどうか，あるいは人が機械を信頼するかどうかは，これらの点に大きくかかわってくるのであり，全部満たされれば大きな信頼感を覚えますし，どれか一つでも欠けていれば十分な信頼はおけないことになります。

不適切な信頼としての過信

今申し上げたのはある意味で「不信」の形ですが，私がこれから説明したいのは，反対の「過信」がどういうケースで起こり得るのかということです。

まず能力。いつも安定的に仕事を返してくれる人や機械に対して信頼感を覚えると申し上げました。そういう相手に対しては，「今までいつもきちんとやってくれていた。今のケースでも当然上手に対応してくれるだろうし，これからもずっとそうだろう」と思ってしまいがちです。しかし，過去の実績と現在の状態で，これから先も完璧であろうと期待してしまうのはいきすぎで，これは一つの過信のケースとなります。

次に方法。高度の機能を持っている人や自動化システムとのやりとりでも起こってくるものですが，例えば，「この機能がどのように実現されているか詳しくは知らないが，よく設計考えて設計されているであろう。どのようにタスクを実行するつもりか知っているわけではないが，詳細まで把握しておかなくても大丈夫だろう」と考えてしまうのは，過信の一つの形態ということになります。

目的に関しても，自動化システムと人間とのやりとりで起こってくるケースがあります。「なぜこのようなことをしているのか分からないが，良かれと思ってやっているのだろうし，別に悪いようにはしないだろう」と思ってしまう事例などで，オートパイロットに対して，時々このように感じることがあるというパイロットの例も報告されています。

SOPとヒューマンエラー

イラストは『CFIT Education and Training Aid』に「ベテランの落とし穴」として掲載されているもので，注釈に，「特にベテランの方は，SOP（Standard operating Procedure）を大事にしてください」とあります。

ベテランの落とし穴

（CFIT Education and Training Aid）

それでは，SOPは万能なのでしょうか。ここからはそのことについてお話ししたいと思いますが，その前に，われわれがどのような認識のもとに，「SOPは万能か？」という議論をしているか，少し説明しておきたいと思います。

ヒューマンエラーの分類

ヒューマンエラーにはいろいろな分類の仕方がありますが，認知心理学的な分類で「スリップ」（行為のエラー）と「ミステイク」（思考のエラー）の2つに分けることがあります。

●スリップ（行為のエラー）

ほとんど定型化された動作を意識せずに行ううちに，当初の意図と異なったことをしてしまうエラーを「スリップ」と言います。

私は12階建てビルの8階の部屋で仕事をしているので，エレベーターに乗るといつも“8”のボタンを押しています。ある時，9階に行く用事があってエレベーターに乗り，ボタンを押しました。止まったので降りると，何とそこは8階でした。つまり，私は無意識のうちに“8”のボタンを押してしまっていたのです。9階に行くという意図が，8階のボタンを押すという行為に乗っ取られてしまったという意味で，こうしたエラーを「乗っ取り型エラー」と言います。

冒頭でご紹介したストラスブール空港のクラッシュの事例は，スリップの中の「モードエラー」と言われるものです。パイロットの意思決定は正しかったのに，コンピュータにデータを与えるときにボタンを押す回数を間違ってしまった，つまり，意図は正しいのですが，とった行動が間違っていたのです。

●ミステイク（思考のエラー）

意図した通りに行為が実行されたのですが，意図そのものが誤っていたといたというエラーで，明らかに思考のエラーであるものを「ミステイク」と呼んでいます。

それから，われわれは行為を認知的な階層というとらえ方で，「スキルに基づく行為」，「ルールに基づく行為」，「知識に基づく行為」の3階層に分類していますが，これも議論を整理するに当たって便利であると考えられています。

(1) スキルに基づく行為

感覚系からの情報に基づいて，無意識的・円滑に行われる日常的あるいは熟練の域に達した行為です。

例えば，車を運転していてカーブを曲がろうとする時に，「今，どのくらいのスピードで走っている，従って，レーンを逸脱しないで曲がるためには何度の角度でステアリングを切らなければいけない」といちいち考えることをせずに，ほとんどの人が無意識的にステアリングを切っていると思います。そのように意識しないで，体が勝手に動いてしまうのが，スキルに基づく行為の典型的なものです。

(2) ルールに基づく行為

「AならばBである」という条件・動作ルールに基づく行為です。

「今，この場面では私はこれをしなければいけない」ということを念頭に置きながら，行動するのがルールに基づく行為と言えます。

(3) 知識に基づく行為

過去の経験やノウハウが無い場合は，条件・動作ルールがないため，どういうふうに対応すればよいのか分かりません。しかし，対応しなければならない，ということになりますと自分自身の持っている知識を総動員して，事態を理解して，その中で何をすべきか考えようとします。これが知識に基づく行為です。

3つの階層を紹介しましたが，思考が関係するのは(2)と(3)であり，(1)は思考にはあまり関係しないことをご理解いただくと，次のヒューマンエラーの分類がお分かりいただけるかと思います。

●スキルベース・スリップ（行為のエラー）

スリップは，思考は正しかったけれど，意識せずに行った行為が間違っていたエラーですから，スリップはスキルに基づく行為でしか起こり得ないことになります。そういう意味で「スキルベース・スリップ」という言い方をします。例えば，必要操作をほとんど無意識的にできる人が，ステップを確認しないまま熟知

した操作系列を実行するうち，やったつもりでやり忘れていた，というのがスキルベース・スリップです。

●ルールベース・ミステイク（思考のエラー）

「AならばB」の形で表される条件・動作ルールに基づいて行為をすべき場面において，AではなくA＊という状況にあるにもかかわらず，Aであると考え違いをしてしまうエラーは，ルールベースの思考のエラーということになります。

●知識ベース・ミステイク（思考のエラー）

これまで経験したことがないので，どのように対応すればよいか分からないような時のエラーが，知識ベース・ミステイクです。

さて，何のためにこのようなことを申し上げてきたかと言いますと，このヒューマンエラーの分類とSOPを照らし合わせてみると，SOPが対応できるのはルールベース・ミステイクだけであることがご理解いただけると思うからです。

SOPは「この場面ではこれをする」というようにルールに基づいて書かれていますから，ルールベース・ミステイクを防止するのに役立ちます。しかし，知識ベース・ミステイクに対しては，ほとんど効力がありません。ルールで書けないものへの対応が知識に基づく行為で要求されるのですから，それに対するルールをSOPの形で書けるわけがないからです。また，無意識的に体で対応してしまうスキルベース・スリップにも効果はあまり期待できません。

そうしますと，日常的な業務の中で，「SOPさえ守っていればよい」，あるいは「SOPに書かれていないことは気にしなくてもよい」と考えることは明らかに間違いです。

それでは，SOPでカバーできないものはどうすればよいか，それをカバーするのが教育と訓練です。教育がどの部分に対応するか，訓練がどの部分に対応するかということが，その次のテーマとなってきます。

日常に潜むリスクを見つける

リスクを正しく認識するのは非常に難しいと申し上げましたが，そのような中で日常に潜むリスクを見つけるにはどうしたらよいのでしょうか。

第一は，昔から行われてきたように，「事故やインシデントから学ぶ」ことが大切です。

例えば，最近，シンドラー社製エレベーターによる死亡事故が起こりました。その後に，それ以前にも同種のトラブルが国内外で続発し，しかも全く同じような死亡事故もあったことが判明しました。判明したのが事故後であったのが非常に残念であり，事故やインシデントの情報を共有することの重要性を指し示しています。

航空分野でも同じようなことが言われています。前述のストラスブールでのA320墜落事故（1992年）以前，88年以来，同種のインシデントが発生していました。モードの取り違えをGPWS作動によって気付いたガトウィック空港とデュッセルドルフ空港のケース，クルーが気付いたサンディエゴ空港とナンテ空港のケースでは，いずれも生還しています。

ところが，ストラスブール空港の事例ではGPWSは積んでおらず，クルーも気が付かなかったために，4つの生還例のいずれにも該当しないものになってしまいました。もしこれらのインシデントの情報が共有されていれば，ストラスブールの事故は防げたかもしれないと思います。

いずれにしましても，事故やインシデントなど，形になったものから学ぶべきものを見つけ出す必要があります。

ヒヤリハット事例の共有

さらに，まだ形には表れていないが，何か気になる点，しっくりしない点があるという時点で，何らかの対応がとれるのではないかと思います。犠牲や損害が生じたものから学ぶのは当然のことなのですが，それからしか学べないというのはあまりに悲しいので，それらが出ない前に見つけたいというのがわれわれの望みなのです。

その対応策の一つとして，「ヒヤリハット事例の共有」が非常に重要です。例えば，自分のヒヤリハット経験を誰かに話すと，「実は私にも同じような経験がある」と問題を提示くれる人がいるかもしれません。そのような問題意識の共有から，問題解決に向かって

の取り組みが行われていくと思います。

ただ残念ながら，ヒヤリハット事例を集めるというのはそれほど簡単なことではありません。報告が自分の評価に使われるのではないかと心配する方もいるでしょう。あるところで，事例収集を促進するために，報告者を表彰してはどうかという案が出されたという話を聞いたことがありますが，ヒューマンファクターの観点から言えば，とんでもないことだと思っています。インシデントやヒヤリハット事例の収集は，匿名性の確保・保証が重要です。報告者の評価には使わないことを宣言した上で実行に移されるべきです。表彰するとなれば報告者を管理する情報が必要になりますから，匿名性は失われるはずです。

日常に潜むリスク

日常に潜むリスクの例として，「SOPからの逸脱」について考えてみたいと思います。

SOPからの逸脱としては，「意図した逸脱」と「意図しない逸脱」があります。

(1) 意図しない逸脱

「何かに注意が集中してしまって，うっかり見落とす」，「現在の状況を類似の（別の）状況と混同してしまい，誤ったルールを適用してしまう」，「起こってほしくない状況から目を背ける」，「緊急度の高い状況の中で，手順が欠落してしまう」などのケースが考えられます。最後のケースは，人間をサポートする自動化システムの構築という議論につながっていく問題であると思います。

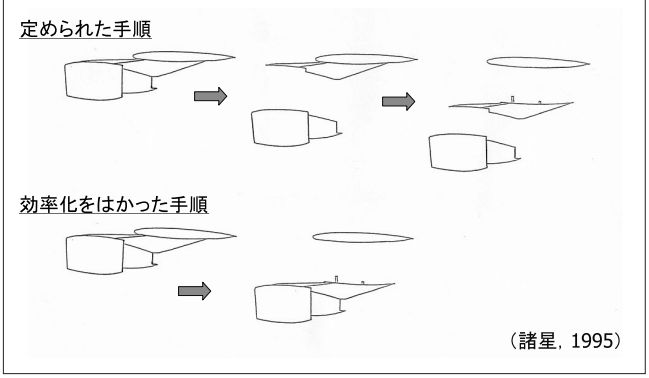
(2) 意図的逸脱

意図的な逸脱を行っているにもかかわらず，この状態にリスクが潜んでいるということが感じられないとすると，これは非常に深刻な問題です。その例として4つ挙げたいと思います。

(1)「なぜこのような面倒な手順になっているのだ，もっと良い方法があるのではないか。」

図7はベアリング交換の例です。定められた手順では，エンジンを外して，その次にパイロンを外して，ベアリングを交換するようになっていたのです

図7　SOPからの意図的な逸脱

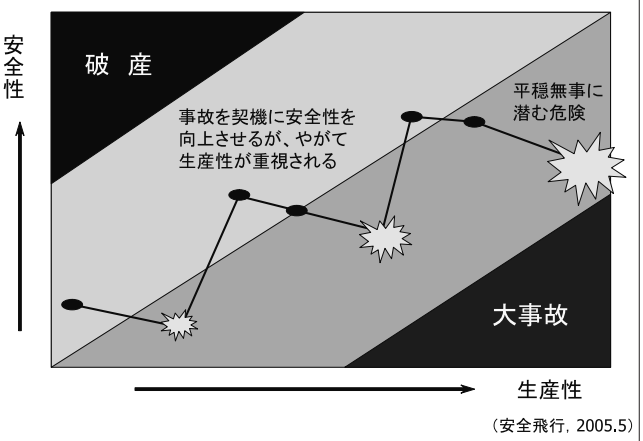


が，効率化を図って，エンジンとパイロンを切り離さずに一挙に翼から外してしまう手順を作ってしまい，その結果，非常にまずいことが起こってしまいました。なぜ2段階で取り外す手順を作ったかという，もともとのアイデアが伝承されていないということが重要な点です。

図8は「生産性対安全性空間における仮想的組織の変遷」を示すものです（『安全飛行』2005年5月号）。

事故を契機に安全性を向上させようといろいろな工夫が行われます。その結果，安全が続いていくと，生産性や効率を重視する方向へシフトしていってしまいます。そしてまた何かトラブルが起こると，安全性を向上させる手が打たれるのですが，しばらくすると風化していくという現象があるということです。もともとの安全性を確保するためには，SOPがなぜそうなっていたのかという認識を共有することが非常に重要であることを示しています。

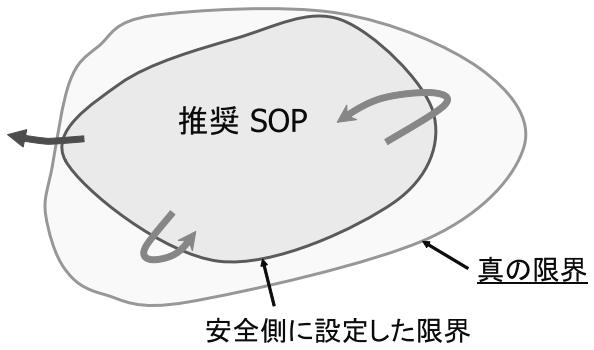
図8　生産性対安全性空間における仮想的組織の変遷



(2)「以前，逸脱しても大丈夫だった。今回も大丈夫に違いない。」

これは特にエンジニアに対する問題提起になると思います。エンジニアの世界では，安全を確保するためにかなり厳しく限界を設定している場合があります。ある時，ふとした拍子に限界を越えてしまったけれど，何も起こらなかった，大丈夫だったという経験を何度かすると，真の限界はもっと外にあるので少々逸脱しても構わないと考えてしまう可能性があります。こうなると，せっかく安全のために厳しく設定した限界が，結局は妥当ではないことになってしまいます。(図9)

図9　SOPからの意図的な逸脱



(3)「他の人たちも守っていない」

他の人も守っていないので私も守らなくていいと考えて，意図的にSOPを逸脱するケースです。

昨年起きたJR福知山線の脱線事故の後，運転士の多くが日常的に規程を越えた120km走行をしていたことが明らかになりました。新聞記事には「『遅れ』におびえる運転士」という見出しが付いていましたが，この事例のように，守るべきことを皆が守らないという状況が起きた場合，なぜそうなったのか，その背景を考えることも非常に大切です。

(4)「危ないとは分かっているが……」

ちょっとSOPを逸脱しても，私が気を付けて頑張れば，ユーザーにもう少し利便性を提供できると思って行う行為は，ある意味の善意です。けれども，人間の宿命で，いつまでも注意を完璧に保つことができるとは限りません。2005年5月に起きた竹ノ塚踏切事故は，善意の行動ではあったかもしれませんが，それが裏目に出て，犠牲者を出してしまったのです。

今，述べましたように，SOPを守ることができない，あるいは意図的に逸脱しても仕方がないという状況があるとすれば，SOPそのものに問題があるのかもしれません。従って，SOPは必要に応じた見直しとチューニングが必要なのです。

SOPは「ルールに基づく行為」を実行者の練度，知識，精神力に依存しないようにする上で非常に有効ですが，限界もあります。その理由としては，

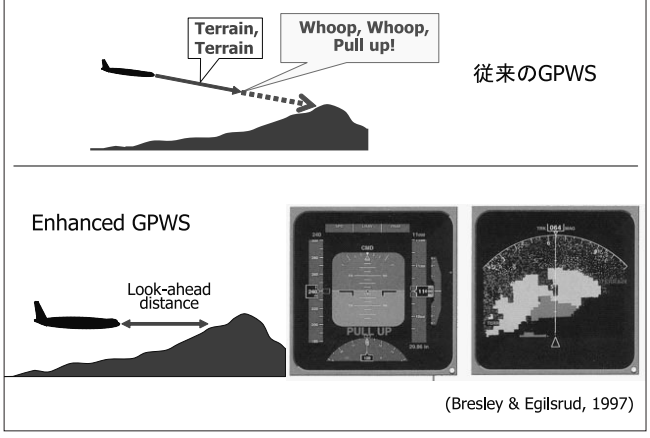
○現状に即したものであること
○明らかな有効性を持っていること
○簡単に実行できること
○合理性を持っていること

のいずれか一つでも満たされないものがあると，「守らなければならない」という意識が希薄化してしまうからです。

例を2つ挙げてみます。

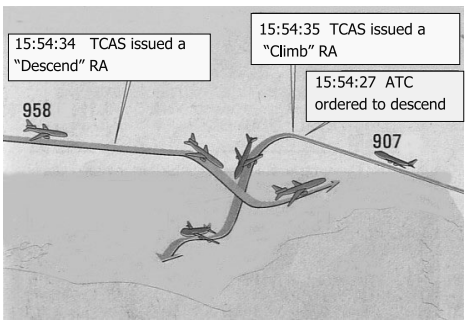
一つ目はGPWSの例です（図10）。従来のGPWSでプルアップというメッセージが出た場合，明らかに不適切であると断言できない限り，警報に従っていました。しかし，現在のEnhanced GPWSは，機械が現状をどう認識しているかを表示していますから，パイロットは警報が出る前から，すでに機械の判断を認識しています。従って，EGPWSのもとでのSOPは，旧来のGPWSのもとでのSOPと少し形が違うという気がします。

図10　SOPの見直しとチューニング（GPWSの例）



もう一つはTCASの例です（図11）。この場面で，パイロットはもちろん，TCASも管制官も意思決定ができるということです。三者の意思決定があって，最終的に誰が意思決定するかという権限の問題がまだ十分には解析されていませんが，近々，管制官にもTCASが何を言ったかが見えるようになると思います。そうなると，このような状況でのSOPは，今までのSOPとは変わってくるのかもしれないと思います。

図11　SOPの見直しとチューニング（TCASの例）



原図面（朝日新聞，2001.1.31）

むすび

いろいろ申し上げてきましたが，最後にまとめたいと思います。

まず，リスクは本来潜在的にしか感じることができない性質があり，今対処しなくても，すぐに顕在化するとは限りません。ここに問題のやっかいさがあります。つまり問題を先送りしてもいいのかということが出てくるのです。

次に，リスクは見つけること自体はなかなか難しいのですが，見つけることができれば，制御する方法は自ずと決まってきます。従って，今日は「リスクを見つけて制御する」というタイトルを付けましたが，「リスクをいかに見つけるか」が最も大事ですので，日常に潜むリスクをいかに見つけるかということを主体にお話しさせていただきました。

個人レベルで「何か変だ」という問題に気が付いたとします。自分で考えてみることは当然ですが，そこにとどまらず，他の人に報告や問い掛けをすると，その問題をグループで共有でき，グループで考えることができます。さらに，それを組織に報告・問い掛けをすると，組織全体で問題を共有することができて，組織としての問題解決につながっていくでしょう。

また，その過程や結果は構成員すべてにフィードバックされるべきです。さらに，必要に応じて社会に対しても情報のフィードバックした方がよいと思います。これが社会に対する組織の信頼を形成していく上での非常に大切なプロセスになると思います。

最後に，抽象的な話になりますが，一番大切なのは次のようなものであると考えます。

●問題意識を持つ文化
●常に本質に立ち返って考える文化
●議論ができる自由な文化
●人の問題を自分の問題としてとらえる文化
●状況認識の共有を可能にする文化
●情報伝達の確実性を尊ぶ文化

精神論のように思えるかもしれませんが，われわれ研究者が過去のいろいろな事例を研究し，いろいろな問題を考えてきた中で到達した，最終的な結論の一つであると考えています。

このような文化を持つ組織は，ダイナミックな対応能力を持つ組織であると思います。まさに全日空の皆さんはこのような文化を持っておられると実感しております。そして，ダイナミックな対応能力を持った組織として，これからも発展されると思っております。これは私の全日空に対する過信ではなくて，信頼です。

ご清聴ありがとうございました。