航空システムにおける
情報セキュリティの研究課題

２０１４年５月２４日（土）

航空運航システム研究会（TFOS.SG)
航空システム部会　　松田　宏

本日の話題

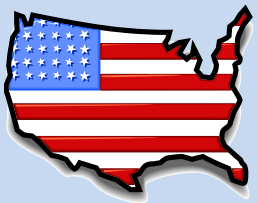
- 国家レベルのサイバー攻撃が現実に
  - やることが個人ハッカーとはけた違い！
- 「想定外とは不勉強と怠慢の言い訳である」
  - 何が起こり得るかの「想定」が第１歩
- 安全対策基準の矛盾と限界
  - 基準を守ればよい訳ではない
- 航空システムの情報セキュリティの脅威とリスク
- TFOS／システム部会の研究課題（提案）

米原発など標的に 中国サイバー攻撃

2014年5月19日、米司法省は中国人民解放軍の当局者5名を、米企業にシステムに侵入して原子力発電所などの情報を盗んだとして掲示訴追した。米政府が他国のサイバー攻撃を産業スパイとして訴追するのは初めて。

5人は上海の「61398部隊」と呼ばれる軍のハッカー組織に関与、米原発大手ウエスチングハウス（WH）、米鉄鋼大手USスチール、非鉄大手アルコアなど企業6社から原発の設計や太陽光パネルの製造コストなどに関する情報を盗み、中国の国営企業などのために使ったとされる。

中国外務省は「事実のねつ造だ」と全面否定する緊急声明を発表した。



（2014年5月20日　日本経済新聞から抜粋）

「事実は小説よりも奇なり」

- 2012年出版のトム・クランシーの軍事ミステリー”Threat Vector”（日本語版「中米開戦」。2014年に出版）は、虚実取り混ぜたエンターテイメント小説だが、内容は非常にリアル。
- この小説に、中国軍傘下の民間企業に偽装した巨大な秘密サイバー組織が出て来る。米国をサイバー攻撃し、無人偵察機を乗っ取り、社会インフラを混乱させ、米軍を無力化する。

(新潮文庫）

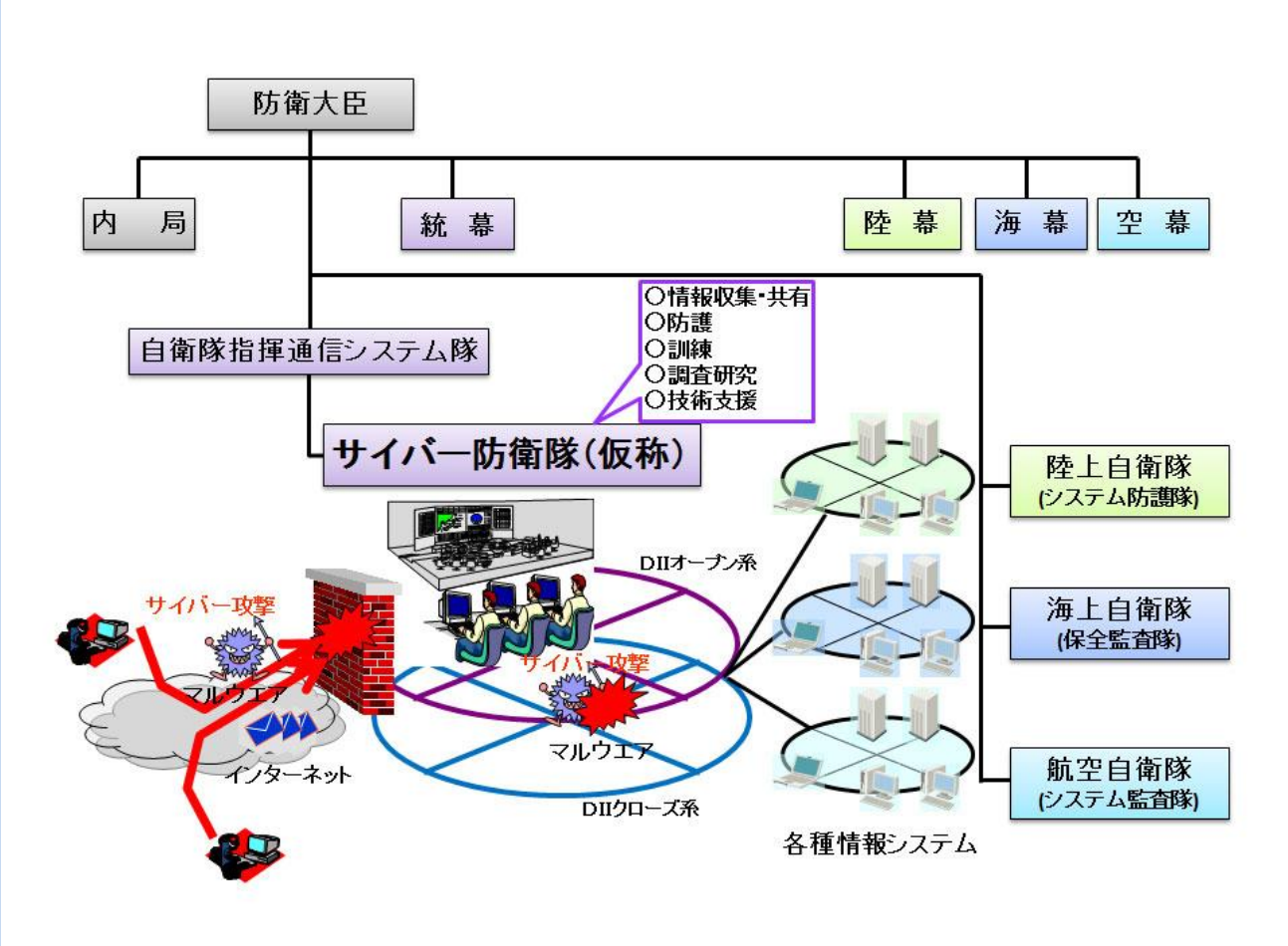
各国がサイバー部隊を増強中

- 中國人民解放軍61398部隊は上海市にあるサイバー戦部隊で、専門要員2000人。傘下に約40万人のサイバー部隊。
- 米国サイバー軍（United States Cyber Command; USCYBERCOM）は、メリーランド州にあるサーバー戦統合部隊。専門要員1800人（2016年までに6000人に増員予定）。
- ロシアは、2017年までにサーバー攻撃からの防衛を目的とするサイバー安全保障部隊を創設する(2014年2月公表）。
- 北朝鮮は1990年代に500人規模のサイバー部隊を創設。現在では3000人の要員がおり、世界最高レベルとの評価。
- 韓国は、サイバー司令部の要員を500人から1000人に増員。2013年に銀行や放送局がサイバー攻撃を受けたため。
- 英国、フランス、イスラエルなどもサイバー部隊を増強中。

（資料：Wikipediaによる）

わが国自衛隊もサイバー防衛隊を創設

- わが国の自衛隊でも、2013年に指揮通信システム隊内に100人規模のサイバー防衛隊を創設。



韓国への大規模サイバー攻撃

- 2013年3月20日に韓国で、少なくても3銀行と2放送局のコンピュータシステムが大規模サイバー攻撃を受けた。
- 銀行ではATMや決済処理が一時的に停止し、放送局では手作業で放送を継続する事態となった。
- 2009年7月には大量アクセスにより韓国全土のインターネットがまひし、企業や社会サービスが混乱する攻撃があった。
- 2011年3月に同様の妨害攻撃があり、同4月には農協銀行が侵入を受け、データが破壊され業務が停止した。
- 某国によるサイバー戦争遂行能力アピール作戦だろうとの推測もある。

（資料：日本経済新聞　2013.4.5より抜粋）

古典的なテロ攻撃／妨害等の事例

（物理的な攻撃）

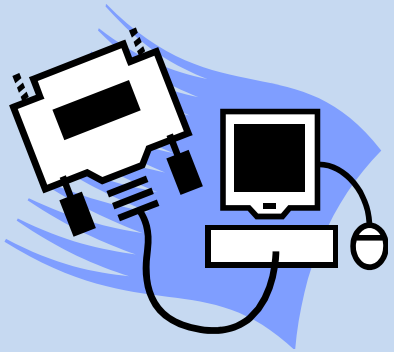
- 航空交通管制部庁舎に手製のロケット弾が撃ち込まれた
- 無人の航行援助施設の玄関に火炎瓶が投げつけられた
- 航空路監視レーダ・データを伝送するケーブルが切断された
- 空港機器室の無線機器のヒューズが抜き取られた

（妨害電波／情報操作）

- 航空機に管制用周波数で偽の管制指示が出された
- GPSに対する妨害電波により航空機に深刻な影響

（偶発事故による妨害）

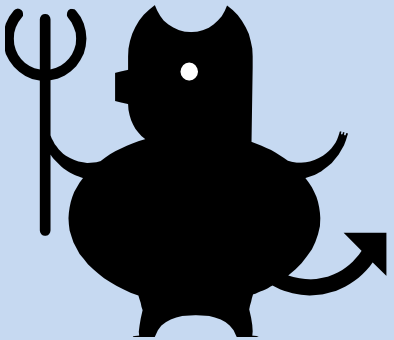
- 米軍艦艇がILSと同じ周波数を誤発信
- 工事現場のワイヤレスカメラがDMEに影響



サーバー時代のテロ攻撃／妨害

（活動の主体）

- 国家機関または民間企業に偽装した大規模組織
- 最高の技術と豊富な資金を持つプロ集団



（攻撃の目的）

- 航空機の遅延や欠航による社会的混乱
- サーバー攻撃能力の誇示による威嚇
- 事故の誘発／破壊活動（墜落、衝突、爆発など）

（攻撃の対象）

- 航空機搭載システム、運航管理システム、管制システム
- 対空通信、通信衛星／地球局、航空通信ネットワーク

サーバー攻撃で起こりうること（例）

（航空機搭載システム）

- FMS飛行計画データの改ざん／消去で飛行不能に
- ACARS，CPDLC，ADS通信途絶／データ改ざんで飛行不能に

（運航管理システム）

- システム停止で機材繰りや飛行計画作成ができず欠航
- データの改ざんで間違った飛行計画が作成されれば事故に

（航空管制システム）

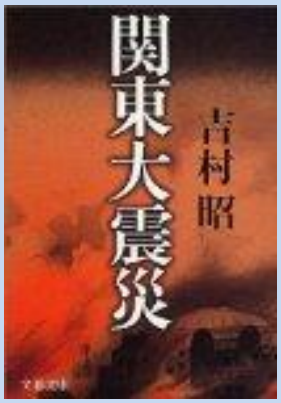
- システム停止で管制指示等が出せず飛行不能に
- データ改ざん／消去等で間違った指示をすれば空中衝突も

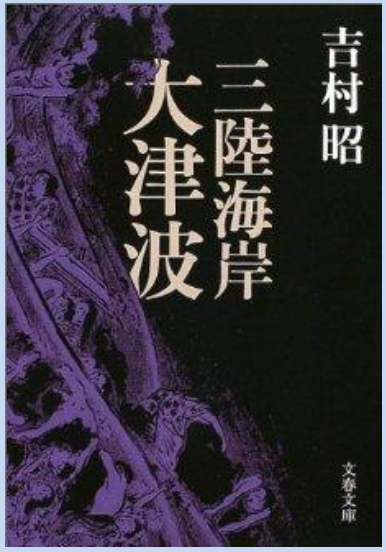
（通信ネットワーク）

- 障害で停止し、代替手段がなければ飛行不能に
- なりすましにより偽情報が伝達されれば事故に（CFITなど）

想定外とは不勉強と怠惰の言い訳

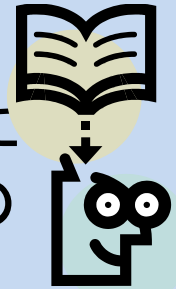
- 三陸海岸はたびたび地震・大津波に襲われている。「三陸海岸大津波」は歴史小説家・吉村　昭が明治29年の大津波、昭和8年の大津波、昭和35年のチリ大地震大津波の3部構成で、三陸各地の被害状況を克明に紹介している。
- その中に「想定外というのは不勉強と怠惰の言い訳だ」という言葉がある。起り得ることを想定しないのは過去の事例を勉強せず、リスクを十分に検討しなかった怠惰によるという。
- 過去に起きたこと、運よく最悪の事態は回避したがそうでなければ大変なことになった事態、構造上起こり得ることを十分に考えたい。



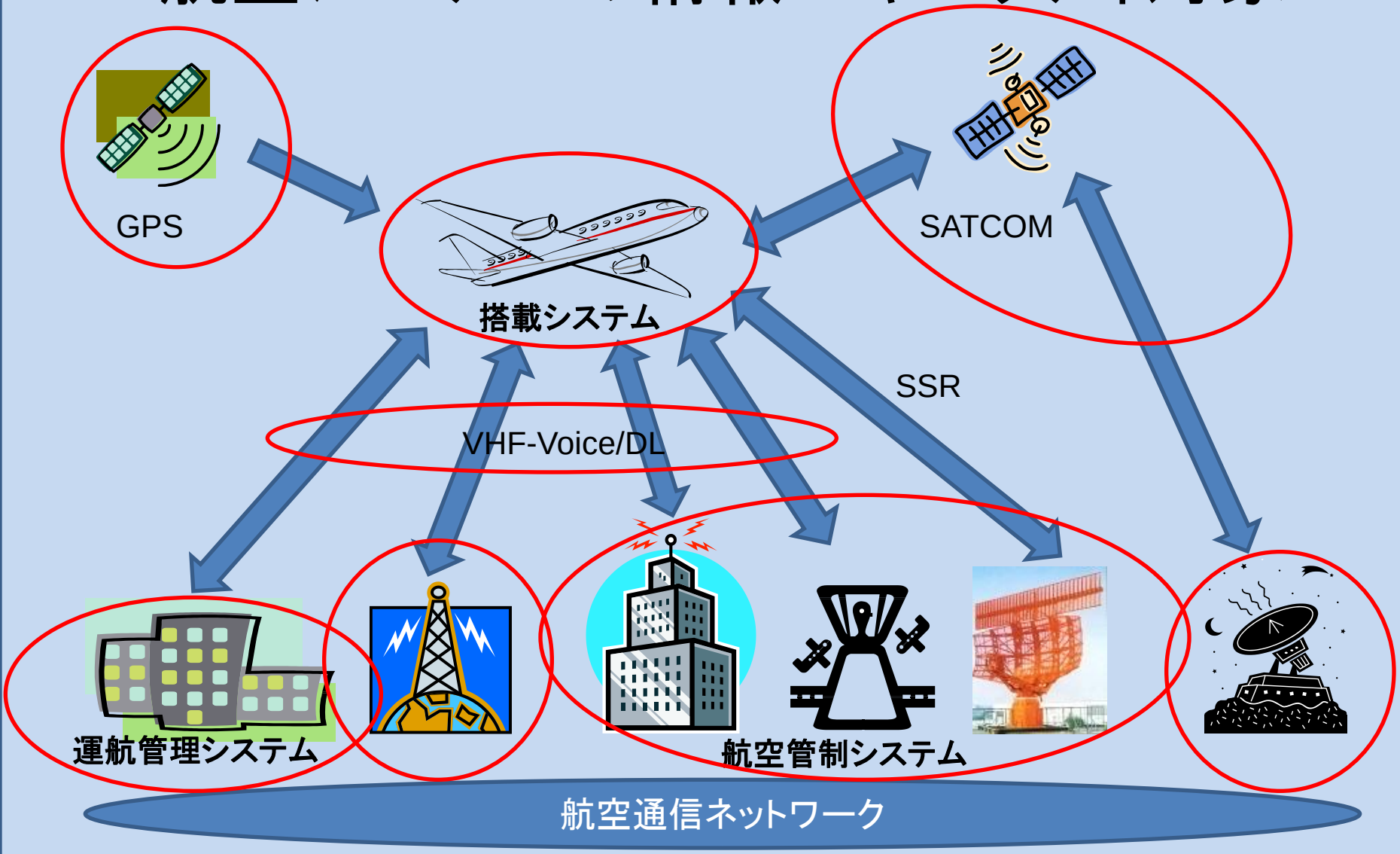


起こり得ることを想定する方法

- 航空関係で過去に起きた事件・事故等の事例を収集し、分析する（少ないし、公表されていないものが多いはず！）
- 他の業界で起きた過去の事件・事故等の事例を収集し、同様のことが航空業界で起きるとすればどうなるかを想像したシナリオを作成する（シナリオ分析）。
- 過去の事例で「運よく」最悪の事態にはならなかったものについて、「運が悪ければ」起こったであろう最悪の事態への筋道を想像したシナリオを作成する。
- 対象システムの弱点を探し、そこに攻撃を加えたらどのような結果になるかを体系的に推定する（Fault Tree Analysis)。
- 対象システムに関与している内部の「人」に着目し、彼（彼女）なら何ができるかを想像する。



航空システムの情報セキュリティ対象



安全対策基準の制約と矛盾

- 対象業界が異なるたくさんの安全対策基準がある
- 設備や運用管理体制などに関する型式的な項目が多い
- 情報セキュリティ対策も含まれているが、万全ではない
- 最新の技術や新しい攻撃手口に対応していないことがある
- 最低限の安全性は確保できるが完璧ではない
  - 基準適合認定を受ければ安全だと錯覚（安心）しがち
  - 「善意の管理者の義務」は果たしていると言い訳は可能

安全対策が公開されており、専門家なら脆弱性がわかる！
（本来、セキュリティ対策の内容は秘密にすべき）

情報システムの安全対策基準（その１）

- 情報システム安全対策基準（経済産業省）
- コンピュータ不正アクセス対策基準（経済産業省）
- コンピュータウィルス対策基準（経済産業省）
- システム監査基準（経済産業省）
- ソフトウェア管理ガイドライン（経済産業省）
- 情報通信ネットワーク安全・信頼性基準（総務省）
- 情報システム安全対策指針（警察庁）
- 医療情報システムの安全管理に関するガイドライン（厚生労働省）
- 行政情報システムの安全対策指針（行政情報システム各省庁連絡会議）

情報システムの安全対策基準（その2）

- 物流分野における情報セキュリティ確保に係るガイドライン(国土交通省）
- 航空運送事業者における情報セキュリティ確保に係る安全ガイドライン（国土交通省）
- 重要インフラにおける「安全基準等の継続的改善状況等の把握及び検証」（NISC:内閣官房情報セキュリティセンター）
- 金融機関等コンピュータシステムの安全対策基準（FISC:金融情報システムセンター）
- 情報システムの設備環境基準（電子情報技術産業協会）
- 情報システム及び関連設備の運用基準（日本品質保証機構）
- 情報セキュリティ管理基準（日本セキュリティ監査協会）
- データセンターファシリティスタンダード（日本データセンター協会）

漏洩情報が航空機攻撃を支援？

- わが国では騒音対策の目的で、空港周辺を飛行する航空機の型式、高度、飛行経路を、地上で測定した騒音値と一緒に１日遅れでインターネットで公表している。
- 米国では、VIPが搭乗している航空機がテロリストに携帯型小型ミサイル攻撃を受けることを避けるため、１０分間遅らせた空港周辺の飛行情報をインターネット公開している。
- わが国では、米国大統領来日した際の搭乗機の飛行計画をツイッターで公表した管制官が日米地位協定違反を根拠に処罰された事例がある。

スティンガーミサイル

情報改ざんが航空事故の原因に？

- 管制機関に提出された飛行計画の経路が悪意の部外者に改ざんされ、管制官が”Flight Plan Route”という管制承認を出したら、管制官が認識していない経路を飛行する航空機は他機との間隔が保障されない（レーダー監視により最悪の事態は避けられるが）。
- なりすましによる偽管制指示がCPDLCで航空機に送られ、それに従って高度を変更したら、空中衝突の恐れがある。
- ACARSでアップロードされた新しい飛行計画データが改ざんされたものであれば、本来の飛行経路を外れる可能性がある（パイロットが確認し、異変に気がつくはずだが）。
- ATIS/AEISの情報が改ざんされQBH値が大幅に違っていれば、他空域との境界で高度差がなくなり衝突する恐れがある。

サイバー攻撃による被害の想定（例）

- 予約発券システムのトラブル　⇒　遅延／欠航
- 乗客搭乗や貨物積載の混乱　⇒　遅延／欠航、誤積載
- 出発機／到着機情報の混乱　⇒　ゲート混雑、誘導路飽和
- 航空機搭載システムトラブル　⇒　飛行継続困難、最寄空港への緊急着陸、墜落（CFITを含む）
- 通信ネットワークのトラブル　⇒　遅延／欠航、空港閉鎖、ニアミス、衝突
- 飛行計画の改ざん　⇒　燃料不足、ニアミス、衝突、墜落(CFITを含む）
- なりすましによる偽管制指示　⇒　ニアミス、衝突、墜落

内部の人間によるサボタージュ

- 国産ジェット戦闘機の整備が終了し、テストフライトをしたら操縦系統が正常に動作しなかった。調査したら、重要なケーブルが切断されていた。内部犯行の可能性が大きい。
- 豪華客船の建造中に火災が発生し、船体の約4割を焼損した。大幅な工期遅延と莫大な復旧費が発生したが、溶接作業のミスと、内部による破壊工作の両方の可能性があったが、真相は不明。
- 国賓として来日していた某国大統領の搭乗機の出発直前に空港監視レーダーがダウンした。管制塔で出発に立ちあっていた大使館員の承認を得て予定通りに離陸させたが、原因は不明で、当時の政治情勢から内部犯行の可能性もあったとのこと。

情報セキュリティ対策の弱点は「人間」

- マレーシア航空370便の行方不明事件で運航乗務員によるハイジャックの可能性が疑われ、機長の自宅が捜査された。
- 家族を人質にとられたり本人を殺すと脅迫されれば、責任ある立場の内部の人間も破壊活動を行うことがある。
- 内部の人間が自分の政治信条などにより外部に情報を漏らし、指示により破壊活動をすることは少なくない。
- 個人的に親しい人のため、内部の人間が情報漏洩や金銭横領などを行った事例は少なくない。
  - 国防大臣の女性秘書が敵国のスパイだった
  - 女性銀行員がフィアンセのために大金を横領した
  - 女性外務事務官が親しい新聞記者に秘密情報を渡した

情報セキュリティの「人間」対策（例）

- 米国では、秘密情報を扱う政府職員に定期的に「うそ発見機」による検査を受けることを義務付けている。
- わが国の金融機関では、職員の日頃の言動や個人的な事情、家族の状況などを細かく把握している。個人口座の入出金も監視し、不審な点常があれば理由を確かめている。
- 金融機関の電算センターでは私物持込みを厳しく制限しており、必要最小限の身の回り品を透明なプラスチックケースに入れ、警備員の確認を受けなければならない。
- USBメモリの記憶容量が大きくなり、ネット経由のように証拠を残さず大量のデータを持ち出せるようになった。

（近年、雇用の永続性が失われ、派遣社員や下請／孫請けが増えているため、情報漏洩のリスクが高まっている）

TFOSシステム部会の研究課題

- 航空における様々な分野の間で情報交換し、全体的な視点を持つことができるのは大きなメリット。しかし、入門編や概論、最新動向の紹介を中心にした「勉強会」になりがち。
- できれば具体的な事例を収集し、従来にない切り口で分析して新しい体系やモデルを提案するなど、「独自性のある新しい研究」はできないものだろうか。
- 航空以外の分野で起きた類似事例の分析を通し、航空安全にも効果のある解決方法として再構築するなど、「新しい提案」ができることが望ましい。

（提　言）

⇒　航空システムにおける情報セキュリティについて、潜在的な脅威を洗い出し、何が起こり得るかを研究しませんか。

次回予告

- 航空システムで起こりうる情報セキュリティ関連の脅威の仮の体系（案）
- 情報セキュリティ関係の事件／事故の事例
- 航空における情報セキュリティ向上の難しさ