［新たなモビリティ時代のサイバーセキュリティ―セキュリティによるジャパン・ブランドの向上に向けて―］

④ 航空分野のサイバーセキュリティと人材育成

応用

大久保隆夫　情報セキュリティ大学院大学

航空分野に潜在するリスク

2020 年オリンピック・パラリンピック東京大会を直前に控え，各インフラ分野におけるサイバーセキュリティ対策が叫ばれている．外国人観光客の主要な交通手段である航空も例外ではない．海外では，2017 年に米国国土安全保障省（DHS）がボーイング 757 型機のリモートでのハッキングに成功したと発表するなど，脅威となる事例はあるものの，自動車などの交通手段に比べ，あまり脅威が騒がれていないような印象を受ける．国内外の事例においても，インシデントの影響が大きいため，存在はしても明らかにされていないのかもしれない．ただ，それで終わってしまっても問題の解決にはならないので，どのようなサイバー攻撃（脅威）が想定されるかを，航空システムの構造から探ってみたい．

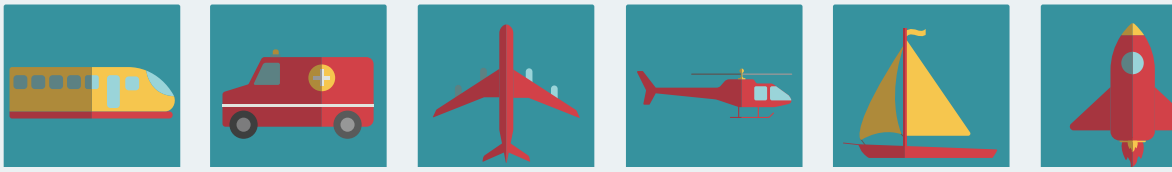
まず，どこからどこまでがサイバー攻撃なのかを明確にしておく．航空機に対する物理的攻撃，および，攻撃者が直接航空機等を操作したり，人間に働きかけての攻撃は対象としない．たとえば，ハイジャックや爆弾，ドローンを衝突させるなどの攻撃は対象外とする．また，対象とする航空分野は民間航空とし，軍用は対象外とする．そのため，自機の位置情報の漏えいは重大な脅威とはしない．本稿においては，下記に挙げるものを主たる脅威として扱う．

- 航空機の衝突，墜落
- 衝突や墜落を誘発する事態
- 運航に対する妨害

以上の前提の上で，航空システムのおおまかな構成と，それぞれの個所で想定される攻撃，脅威を図 -1 に示す．

図にはそれぞれの構成要素と，データの流れを示した．脅威は，データの流れに基づいて脅威識別する脅威分析手法「脅威モデリング手法」を用い，識別した結果を吹き出しで示している．なお，サービス妨害攻撃はほとんどの個所で想定されるため，表記を省いている．これらの脅威のリスクを評価するためには，攻撃の実際の可能性（likelihood）を判定しなければならないが，実際に内部仕様が明らかにされていない部分が多いため，リスクまでは提示していない．図から，航空機に対しては，多様な他システムからのデータ入力があり，それぞれの入力経路ごとに脅威の可能性があることが分かる．図の構成要素および脅威のそれぞれの詳細については紙数の都合上解説は割愛し，いくつかの例を挙げて解説したい．

たとえば，旅客管理システム，貨物管理システムでは，旅客および貨物の積載量，配置を計算し運航系システムを通してパイロットに送っている．パイロットはこの積載データを基に燃料計算を行い，フライトプラン（飛行計画）を立てる．このため，仮に旅客データや貨物データが改ざんされると，燃料不足やバランスなど運航に影響を及ぼす可能性が



ある．また，航空機内のシステムソフトウェアのアップデートは，整備システムを経由して行われる．そのデータはインターネットからHTTPでのダウンロードまたはUSB経由で入手する．そのため，2010年のStuxnetによるイラン核施設への攻撃と同様に，制御を狂わせるなどのマルウェアを混入する経路が存在することになる．

一般にサイバーセキュリティのリスクを評価する際には，被害の大きさ×攻撃可能性で計算する．しかし，航空システムの多くにおいて，これらの詳細仕様は公開されていないため，上記に挙げた脅威が実行可能かどうかは不明である．この中ではすでに対策済みのものもあるかもしれない．しかしながら，これだけのエントリポイント（攻撃者にとって入口になり得る点）が存在することは事実である．本稿ではそれを知ってもらうため，あえてエントリポイントを列挙している．

また，図-1には記述していないが，空港システムも飛行機の運航と密接にかかわっているため，空港システムに対するサイバー攻撃も運航に対する脅威になり得る．たとえば，保安検査システムが攻撃を受けてダウンしたり，チェックを回避させることで，飛行機を出発できなくすることができる．これはセキュリティ事例ではないため次項には書かないが，2019年9月に大阪国際空港の保安検査係員が禁止品の刃物入り手荷物を通過させたため，保安検査場の封鎖，全旅客の検査のやり直しのほか，約30便が欠航になるという事例があった．

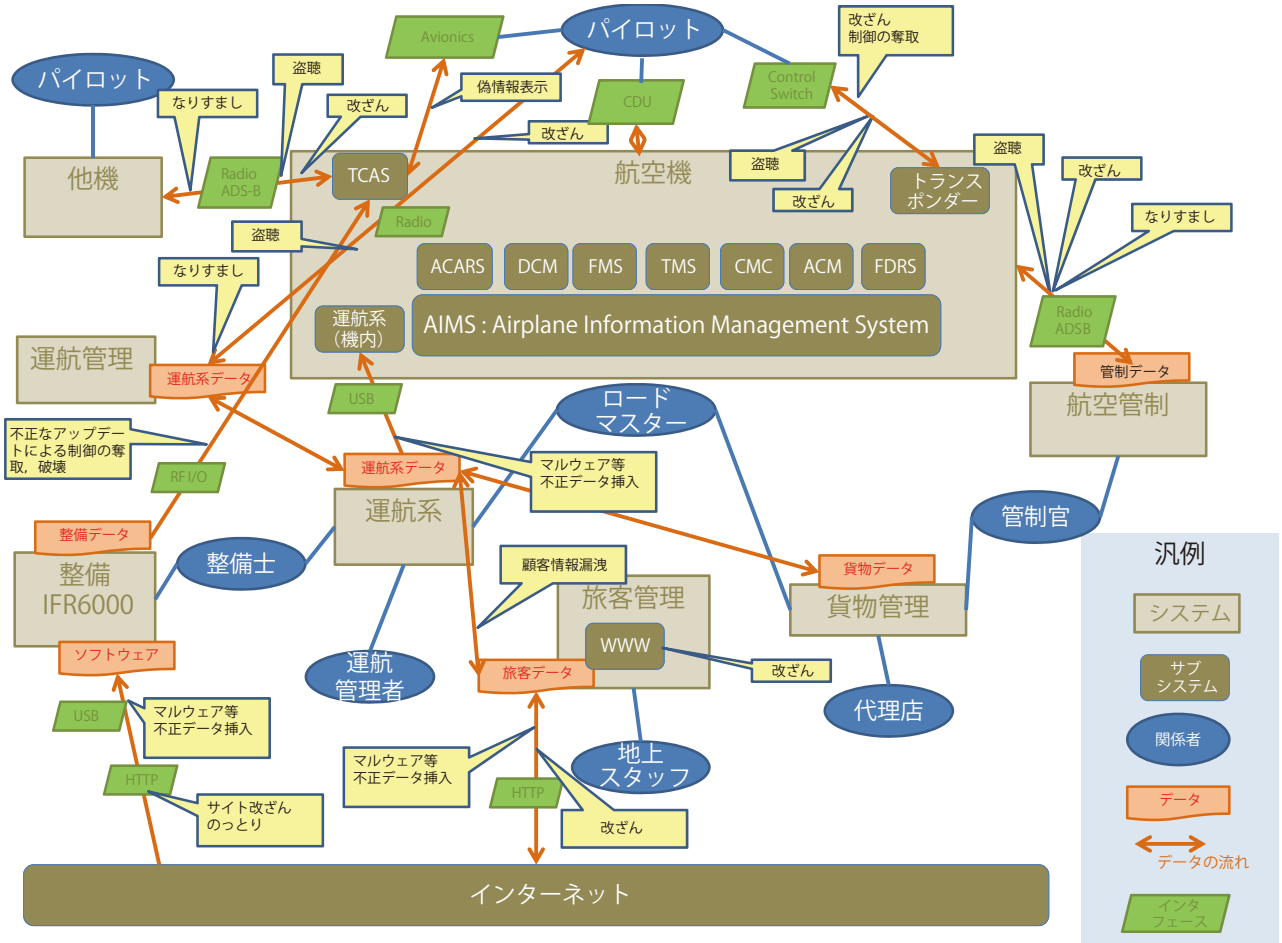


図-1　航空システムの構成と脅威

サイバーセキュリティ脅威事例

図 -1 の中で，実際に脅威の可能性が指摘された例もある．航空機と他機や管制との自機情報（位置，速度，高度，方向等）の情報交換に用いられる ADS-B（Automatic Dependent Surveillance -Broadcast）に脆弱性が存在することが 2011 年に指摘されている．ADS-B の通信はブロードキャストでかつオープン（平文）であるため，スマートフォンで現在飛行中の飛行機を表示できるアプリが存在するほどである．しかしそのため，改ざんや偽造による脅威の可能性が指摘されている．

また，ADS-B や GPS の情報は電波で行われるため，ジャミングや GPS スプーフィングなどの電波妨害による攻撃が想定される．実際に，韓国が 2013 年頃から断続的に GPS へのジャミングによる攻撃を受け，航空機等の航行に影響を与えていると言われている．

電波経由では，冒頭に述べた 2017 年，DHS がボーイング 757 型機のリモートでのハッキングに成功したと発表した．ハッキングの詳細な手口は明らかにされていないが，RF（電波）経由とのみ発表されている．ボーイングはこの脆弱性は既知であり，重大なものではないと主張している．

以上が，従来想定されていた脅威であるが，近年，想定外の事例が発生している．2015 年，航空機内のエンタテインメントシステムから，搭乗機の制御系をハッキングした人物が FBI に逮捕された．エンタテインメントシステムは本来，航空機の運航自体には関連がないことから，ネットワークとしては制御系と隔離されていると信じられてきた（このため，図 -1 にも記載していない）が，この事件により，エンタテインメントシステムから侵入される可能性が否定できなくなった．

また，運航系システムが直接攻撃された例としては，2015 年のポーランド航空（LOT）の事例がある．同航空会社の運航システムが分散型サービス妨害（DDoS）攻撃を受けた結果，ワルシャワ・ショパン空港出発便のフライトプラン作成が困難になり，搭乗客 1,400 人がシステム復旧まで約 5 時間空港に足止めされた．攻撃を受けた経路は明らかにされていないが，運航システムは外部に公開されていないため，内部システムに侵入した上で攻撃を受けたと推測される．

重要インフラおよび航空分野に対する人材育成

2019 年 10 月現在，オリンピック・パラリンピック東京大会の 2020 年を 1 つのマイルストーンとして，重要インフラを対象とした人材育成プロジェクトが進められている．

戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保

2015 ～ 2019 年度の内閣府が進める重要インフラのサイバーセキュリティ確保を目的とした研究開発プロジェクト（管理法人：国立研究開発法人 NEDO）の中で，サイバーセキュリティ人材育成の研究開発が進められている．研究開発は，インフラ 14 分野のうち電力，交通（航空分野を含む），通信，放送の 4 分野における，システムの運用技術（Operation Technology：OT）にかかわるもので，対象も運用従事者としている．また，SIP の目標が 1,000 人以上の受講であること，プロジェクト終了後も成果が継続することが必要であることから，担当する慶應義塾大学と情報セキュリティ大学院大学では，以下の 3 つの柱によるカリキュラム，教材開発を行った．

- 従来の IT 中心にはない OT 寄りの内容とする
- 事業者が組織に導入し自力で教育を行うことができるようにする
- 各分野の実例を盛り込む

上記の方針に基づき，カリキュラムおよび教材を作成し，これまでに 30 組織程度（電気，ガス，交通，放送分野）に配布を行った．また，インシデントに対し 1 次対応を行う従事者には，それがサイバーインシデントなのかどうかを判断できる基礎知識が必要になるため，サイバー攻撃が起きた際にどのような現象が表れるかを，仮想的に体験できる体験型教材の開発を行った．体験型教材はブラウザ上で実行すると，PC のデスクトップの画面が表示され，画面の指示に従いあたかも PC の画面をマウスでクリックしているかのように，操作を行い，また起きることを仮想的に体験することができる．体験型教材の画面例を図 -2 に示す．

現在，コンテンツとしてランサムウェア，フィッシング，バックドア，SQL インジェクションの 4 つが開発済みである．図 -2 はランサムウェアの教材の画面である．受講者は，実際にランサムウェアに感染しなくても，PC でどのような操作を行うと，マルウェアに感染してしまうのかを追体験することで，脅威の仕組みや防衛策について学ぶことができる．また，Web アプリケーションのため，事前の環境の準備等は必要なく URL にアクセスすることで一度に多数の受講者が受講可能となっている．

運輸総合研究所の人材育成プロジェクト

運輸総合研究所では，日本財団助成事業として，2018 年度，2019 年度にサイバー攻撃に対する人材育成に関する調査研究を行った．この調査研究においても，2020 年東京大会を視野において，航空分野，鉄道分野それぞれを対象としたカリキュラム，教材を開発し，航空，鉄道事業者を対象としてトライアルを行った．カリキュラムの開発は下記の手順で行った．

1. 対策項目の抽出

   2016 年度に運輸総合研究所が発行した航空の安全・安定輸送に資するサイバーセキュリティ

図 -2　体験型教材の画面例

対策の手引き」に記載されている対策カテゴリから，システムの維持管理およびインシデント対応に必要と考えられる対策項目を抽出する．

2. タスクの抽出
iコンピテンシディクショナリ（情報処理推進機構発行）の「タスクディクショナリ」を参照し，抽出した対策項目を実践するためのタスクを抽出する．

3. 学習内容の検討
iコンピテンシディクショナリの「スキルディクショナリ」を参照し，抽出したタスクからスキルを抽出し，学習内容を整理する．

4. 机上演習の実施
学習内容の整理に必要な知見を得るため，机上演習を実施する．

5. 学習内容の決定
1．(2) および (3) で得られた知見をもとに，対象となる人材の役割を考慮した上で学習内容を決定する．

6. カリキュラムの作成
上記検討結果をもとに，カリキュラム作成を行う．

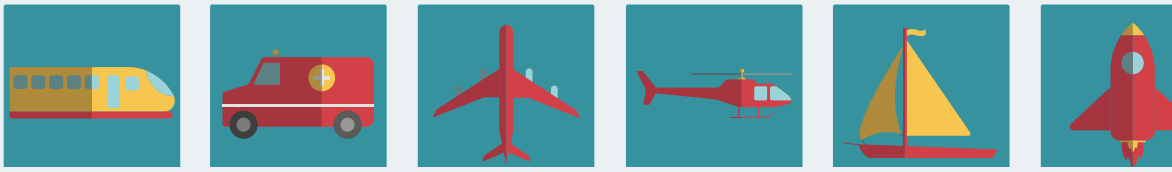
次に，カリキュラムをもとにした人材育成を実施するための教材を情報セキュリティ大学院大学監修のもとに開発し，検討委員会によるレビューを経て完成した．教材は各回 120 分で表 -1 に示す最大全 9 回の講義を想定したものになっている．

表の項目は，航空，鉄道で共通だが，内容については航空，鉄道それぞれで異なっている部分がある．たとえば，第 1 回の「サイバー攻撃の現状」では，紹介する事例が鉄道と航空では異なっている．また，サイバー攻撃対策などでも，鉄道と航空ではその構造の相違により，紹介する内容が微妙に異なる．

この教材を，鉄道，航空分野それぞれに対し，3 日間で教育の試行を行った．航空分野の受講者は 3 名で，対象は講師予定者または教育にかかわる担当者であった．受講者に対し，受講後にアンケートを実施した．以下，航空分野についてその結果を紹介する．理解度については，全員が「大体は理解できた」「少しは理解できた」という自己評価だった．第 4 回（ネットワーク基礎）第 6 回（サイバー攻撃対策）が難易度が高いという評価だったが，第 4 回は用語が難しいという評価だった．サイバー攻撃対策には，ネットワークの知識が必須という考えから，第 4 回の講義が導入されているが，その前提となるネットワーク基礎の知識が必要との認識が浸透していないためと考えられる．一方，第 6 回では，用語以外にも考え方や理論に難しさを感じたという意見があった．これについては，対策の相関関係の把握が困難であっ

表 -1　航空分野向けカリキュラム

回	種類	種類
第 1 回	サイバー攻撃の現状	サイバー攻撃により，業務にかかわるシステムの停止や誤作動が生じると，社会的混乱や人的被害をもたらす可能性があり，その対策が急務であることを認識する．
第 2 回	サイバー攻撃の手法と脆弱性	航空分野において発生する可能性のあるサイバー攻撃の手法と脆弱性を理解する．
第 3 回	サイバーセキュリティ基礎	サイバーセキュリティ対応の基礎となる考え方や手法の概要とその重要性を理解する．
第 4 回	ネットワーク基礎	サイバー攻撃の概要を把握するため，また，サイバー攻撃に対処（原因究明，復旧など）する専門機関と連携し，対応（支援）するために必要となるネットワークの知識を学習する．
第 5 回	セキュリティ技術	サイバー攻撃に対処（原因究明，復旧など）する専門機関と連携し，対応（支援）するために必要となるセキュリティ技術の用語と概要を学習する．
第 6 回	サイバー攻撃対策	手引きをもとに，主なセキュリティ対策の概要を学習する．
第 7 回	サプライチェーンのセキュリティ対策	サプライチェーンのセキュリティ対策の重要性とインシデント対応に備えるための重要なポイントを学習する．
第 8 回	インシデント対応	インシデント発生の際，その原因がサイバー攻撃である疑いを考慮し，迅速かつ適切に対応（支援）するためのポイントを学習する．
第 9 回	学習の振り返り	学習の振り返りを通して本カリキュラムを総括する．



たためと考えられる．教材の量，講義時間については，カリキュラム作成後の検討委員会において委員から「セキュリティを教えるのに少なすぎるのでは？」という意見があった．確かに，セキュリティは広範囲な分野を扱う上，たとえば本学が提供している社会人向け「短期」集中コースにおいても，CSIRT（Computer Security Incident Response Team．組織内においてインシデント対応の中核を担うチーム）やフォレンジックなど1つのテーマについてだけで3日～1週間の講義を要する．そのため，教育として十分ではないことは想定されたが，受講側の業務との関係上，3日程度の拘束が限界という意見があり，最終的にこの量となった．アンケートでは，「量が多すぎて消化しきれない」「第5, 6回は3倍程度の時間が必要」という意見があった．この点は今後改善の余地があると考えられる．

試行の最終回では前述のLOTの事例をインシデントのシナリオに挙げて，実際に起きるか，対策などについてグループディスカッションを実施した．結果，積極的な議論が行われたが，結論としては，「自社では構成が異なるためインシデントは起きないだろう」という意見にまとまった．インシデントのシナリオについては，システムや組織が各事業者によって異なるため，カスタマイズが必要になることが分かった．

鉄道，航空双方の教育を試行して得られた知見は，鉄道分野のOT系が独立しているのに対し，航空分野の業務システムはIT系の汎用技術を採用しているものが多いため，ある程度のIT技術やサイバー攻撃についての認識も高いようである．そのため，航空分野に対しては今回の教材よりもより高度なセキュリティ技術，対応方法を盛り込むのが適切と考えられる．ただし，今回参加したのは大手の航空会社であり，格安航空会社（LCC）などの中小企業では大手ほどセキュリティ教育は十分でないことが想定される．

今後に向けて

2020年に向けて，という目標に対しては，述べてきたように航空分野におけるセキュリティ対策および人材育成は最大限の努力がなされてきた．その成果が十分であったかは，大会の成否を待たなければならないかもしれない．が，長期的観点に立ったとき，東京大会で終わりとするのではなく，今後はその後も見据えた長期的観点による人材育成が必要になる．他分野にならい，事業者間でサイバーセキュリティの情報共有を行う交通ISACの取り組みも始まっていると聞く．今後はこのような組織も活用し，運用だけでなく安全なシステム構築も含めた対策・人材育成が求められると考える．

（2019年10月30日受付）

大久保隆夫（正会員） okubo@iisec.ac.jp
1991年東京工業大学物理情報工学専攻修了．同年（株）富士通研究所入社．2006年情報セキュリティ大学院大学博士後期課程修了．博士（情報学）．2014年より同学教授．専門はシステムセキュリティ，セキュリティバイデザイン．