*<<White Paper>>*

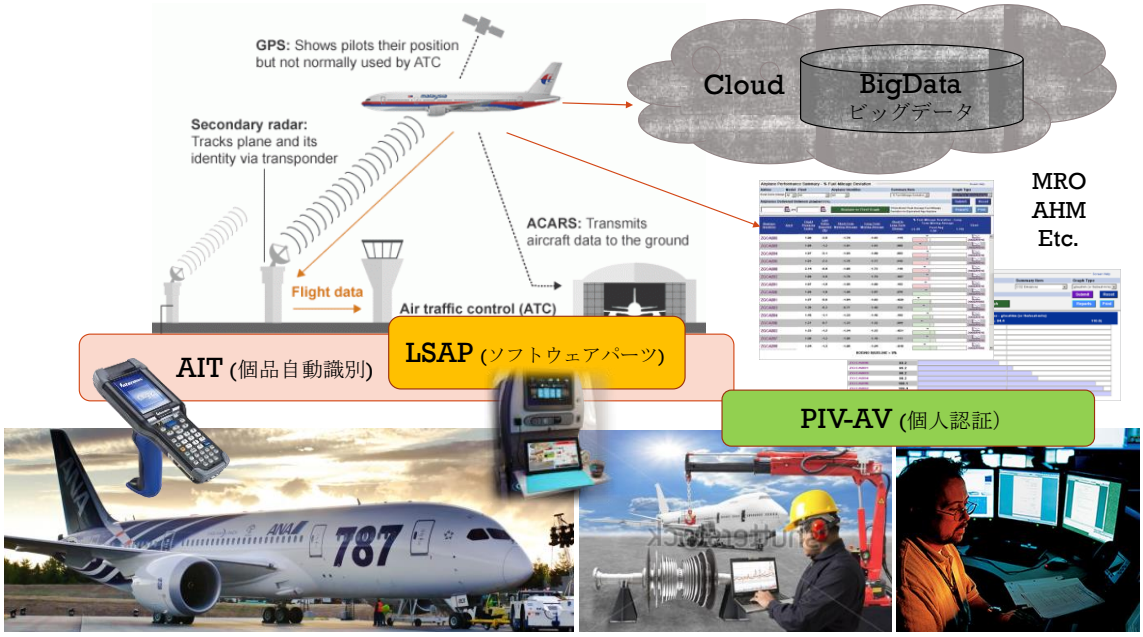
# 航空機の IoT LSAP について

## ～ Loadable Software Aircraft Parts とそのセキュリティ対策 ～

IoT、Industry4.0、Industrial Internet など、製造業における情報産業化が進み、様々な時流を生み出すキーワードが溢れていますが、航空業界ではすでに 20 年近くにわたりこの分野への取り組みがなされてきました。それは、機器の不具合が乗客の命取りにつながる可能性の高い航空業界ならでは、安全・安心への高い意識による賜物と考えます。

### (1) 航空機部品の管理

航空機は数百万点ともいわれる多くの部品で構成されています。それらのうち重要な部品については、実績飛行時間に応じて点検や交換を行うことにより、高い水準での安全を確保しています。それら重要部品はひとつひとつが高価であり、個々の使用状態に応じた管理を行う必要から、シリアル番号に基づく個品管理の概念が早くから実践されてきました。




個品のシリアル番号を間違いなく自動識別するため AIT（Automated Identification Technology）が検討され、バーコードや RFID の標準化・適用がいち早く行われたのもそのためです。輸送など大量の物流を捌くための活用とは異なり、部品毎に使用状態を管理し、使用履歴が重要な情報となる部品整備管理の世界は、ID を識別するための RFID タグ自体に履歴情報も持たせるメモリを期待したユースケースも作り上げてきました。

加えて、昨今の部品機能の高度化・複合化により、ソフトウェアを持つ部品が増加しています。そのソフトウェアを、出荷後でもダウンロード・更新可能な形態で提供される航空機部品を LSAP（Loadable Software Aircraft Parts）と呼んでいます。これこそが、いわゆる航空機 IoT の要であり、航空業界が保全性や信頼性の確保に苦心してきたところです。ボーイング社の B-787 や B-777 などの新しい航空機ではすでに LSAP の管理態勢が確立され、AHM（Airplane Health Management）などのアプリケーションとして航空安全に大きく寄与しています。

AIT、LSAP に並ぶ３つめのキーワードとしては、現在体系化の検討が進められている「運用者個人の認証」です。米国の ATA（Air Transport Association of America）では Spec42 として、ソフトウェアを持つ「もの」を取り扱う「人」が、資格や本人性も含め信頼できるかどうか十分な認証を必要とする世界標準規格を制定しようとしています。欧米の航空業界では認証・認可された人が持つ身分証明 IC カードとして PIV-AV（Personal Identification Verification - Aviation）が標準化されつつあります。

本書では、この３つのキーワードを中心に航空機の IoT に関する取組みについて整理し、今後の進んでゆく方向を見極めるとともに、その他の業種に対してもリファレンスモデルとなることを期待します。

## ①. AIT とは

AIT は訳すと「自動 ID 認識技術」ということになりますが、いわゆる ID コードを機械的に読み取る技術やデバイスによるソリューション全般のことを指します。

ID とは、人の場合は社員番号や運転免許証などの個人に付与された番号で、紙やカードの券面に記載されているのが普通です。それらの ID は桁数の大きい数字や、時には文字が入り混じった並びのことが多く、記憶違いや入力など伝達時のミスによって間違って処理されてしまうこともあります。そこで、機械的な読み取りができれば間違いも少なく、スピードも速いということで AIT が注目されたのです。

航空業界では昔からシリアル番号として、前述の様々な使用状態を把握しておきたい部品に対して、固有のコードを付けて管理してきました。ちなみに同形の部品が多くあり、一品一品を識別しなくても良い場合は、製造時期など毎にまとめてロット番号といったコードでグループを管理しています。

このシリアル番号（厳密には、製造者コード＋部品番号＋シリアル番号等で一意になるコード）を名札のように各部品に付けて管理しているわけですが、これが読みにくい位置に貼られていたり、劣化して読めない状態になってしまい困るというところからも、AIT の検討が始まりました。

当初はバーコード化が検討・採用されました。航空機部品の場合は世界中を巡りますのでグローバルな標準化が必要です。その部品に付けるバーコード銘板規格の標準化を先導し

たのが、アメリカの民間航空機業界である ATA でした。ATA の発行する SPEC2000 というドキュメントの第９章がそれにあたります。

そして１０数年前から、目視できない位置にあるタグでも離れて瞬時に読めるという RFID を使おうと、同じ ATA で検討が開始されました。特に UHF 帯の電波を使う EPC C1G2 規格の RFID は、大型の旅客機の羽についたタグを数メートル離れた地上からでも読めるという期待で盛り上がりました。


そして、当時 RFID の検討を牽引していたウォルマート、国防総省、ボーイングという３つのグループの中で、ボーイング率いる航空業界だけは RFID に ID 識別だけでなく電子メモとしてのメモリ搭載を要求しました。部品に貼付したタグ自体のメモリに、シリアル毎の部品修理履歴を記録しようとしたのです。部品修理履歴は、当時も現在も紙に記録することが義務付けられています。部品は航空機に搭載した状態で、記録の紙は地上の倉庫や事務所に置いてあるのが普通なので、それではいざ故障探求をしたい時に手元に必要な情報がすぐ揃えられない、という事態を改善しようとしたわけです。

それはそれで画期的なアイデアではありましたが、RFID の技術もまだ追いつかず、処理時間の問題や読み書きの距離性能、コストなど様々な課題をクリアしてゆく必要がありました。その過程で、離れて読めることを必須とはせず、ID 識別と整備記録メモリが使えれば良いということで CMB（Contact Memory Button）というボタン型の接触読み書きタイプのメモリデバイスも適材適所で取り入れられてきました。

航空業界では、これらバーコード、RFID、CMB および目視可能な券面表示を総称して AIT と呼ぶようになりました。それぞれのメモリフォーマットやコード規格は ATA（現 A４A）で定め、RFID の通信インタフェースは GS1（元 EPC Global）や ISO/IEC に任せるという分担で世界規格を作っています。また、過酷な使用環境に耐える物理媒体としての規格は RTCA (Radio Technical Commission for Aeronautics) や SAE (Society of Automotive Engineers) など米国の規定として検討されるようになっています。

いまやコンビニで売っている全ての商品にバーコードがついて、レジの計算もほとんど機械的に行われていますが、航空業界でも、まずは対象の部品に AIT が付いた状態にすることが必要でした。そこで、ボーイングとエアバスが業界をリードすべく大号令を出し、自ら率先して RFID タグを貼付し、搭載部品サプライヤーに対しても同様に貼付するように指示を出しています。これから出荷される新しい機種、機体には RFID の AIT が銘板として貼付されてくることでしょう。

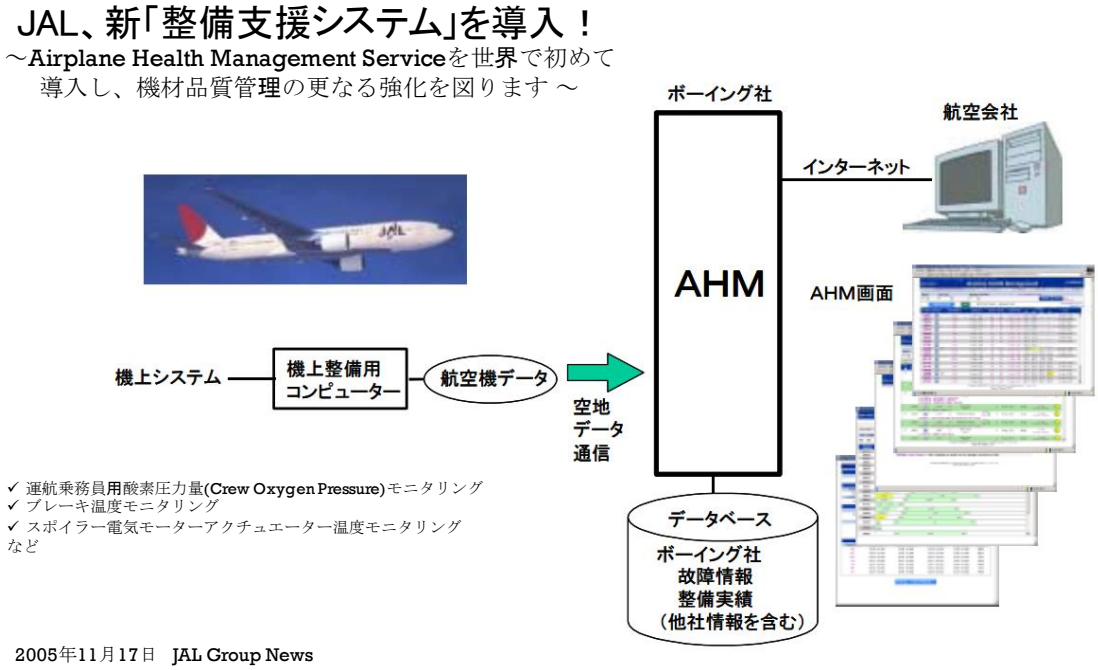
この状態を作ることこそが､航空機 IoT 時代のインフラとして初めの一歩になるのです。多くの多様な企業の集まりである航空業界全体に、統一的な動きとして AIT の活用が開始されたことは関係者の大変な苦労の賜物でしょうし、業界にとって画期的な変化のブレークスルーポイントであると考えています。

## ②. LSAP とは

AIT（RFID 銘板）は大型旅客機で 1000～5000 点の部品（部品といってもモジュールのイメージです）に貼付されており、中型クラスでも 500～1000 点程度に貼付されていますが、様々なアプリケーションが提供され、普及が進み、コストも下がれば、もっと対象部品数は増えることと思います。

そういった航空機部品の中でも、前述の通り近年はソフトウェアを持ったものが増えています。これまでのようないわゆるコンピュータ（フライトコンピュータや○○制御装置など）ではなく、従来は機械的に操作していた装置が機内ネットワークを介してコックピットと装置が通信でつながり、お互いの組み込みソフトウェアが会話しながら動作するといった構造に置き換わってきているのです。そして、これらのソフトウェアが組み込まれた部品は、運用開始後もソフトウェア部分のアップデート操作を可能とする LSAP が増加しています。大型機種では 1000 点ほど、小型機種でも 50～100 点ほどは存在しているようです。

これら LSAP には、単純な ID を返すだけの RFID とは異なり、様々な応答情報を求めることもできます。機器にセンサーを搭載していれば、その場の様子をデジタル通信でリアルタイムに地上の管理者に伝えて、異状の発見や早期対策の準備ができるようになります。




上図の AHM なども、そういったアプリケーションの一例です。このような活用が今後ますます増えてくると考えています。

そして LSAP は、ソフトウェア製造時の信頼性・品質規格として DO-178C を規定し、運用後の配布システムとして PKI を使った厳密なソフトウェア認証の仕組みを構築しています。ソフトウェアのアップデート時には、送付されたプログラムオブジェクトが確かに信頼できるものかコードサイニング技術などを使って検証し、間違いのないインストールが出来るような運用体系を構築しています。また、エンジン始動にあたって、重要な LSAP 群のソフトウェアバージョンが正しく合っていることを逐一確認したのちに、初めてスイッチが入るというしくみの航空機もあるようです。

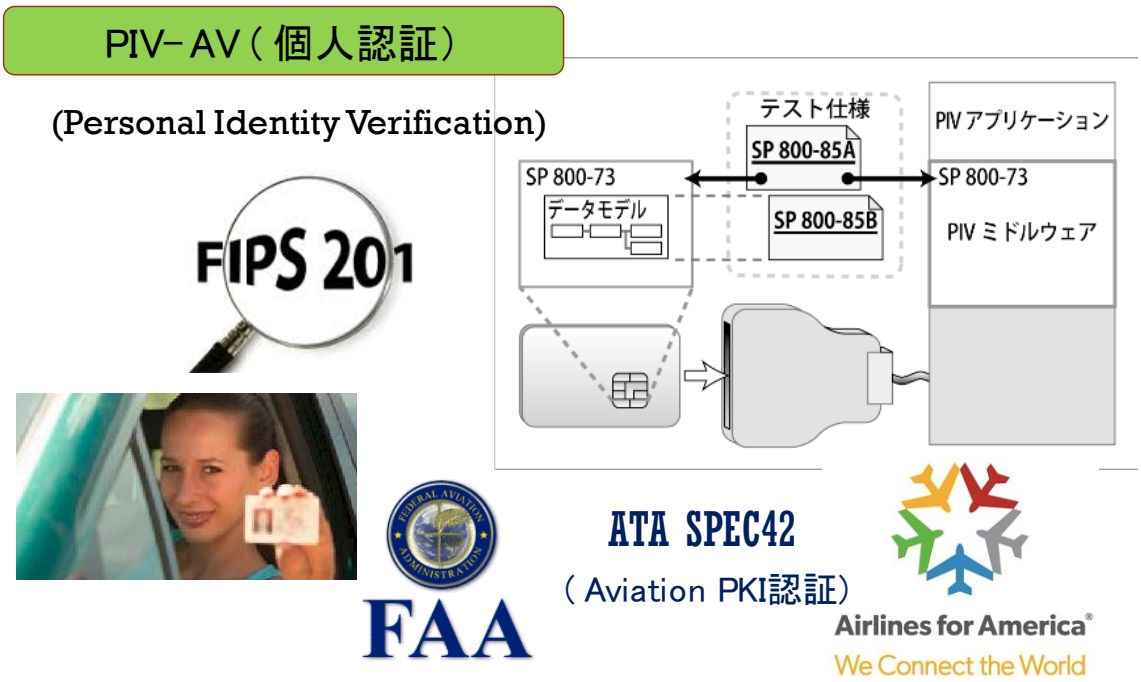
今後の LSAP は、単なる間違い防止の段階から、積極的な妨害や攻撃からどう防御するかという観点も入れ込む段階に来ており、以下に示す PIV-AV を利用した操作者の認証と、部品そのものの認証を信頼性の高い PKI に基づく電子証明書の活用により実現するしくみの検討・標準化の取組みが始まっています。

## ③. PIV-AV と認証基盤について

３つめの取り組みが、個人認証である PIV-AV です。PIV は米国連邦政府の職員身分証用の電子証明書付き IC カードで、AV は Aviation の略です。航空業界では、PIV と同等の保証レベルのポリシーによって個人の身元確認を行い、厳格にシステム利用者を認証しよう

としています。どんなに強固に外部侵入に備えたシステムでも、内部に入り込まれた時点でどの対策も意味がなくなるほど脆弱になる可能性があります。PIV-AV はシステム利用者を信頼できる人だけに絞り、容易になりすましが出来ない仕組みを作った上で、それでも内部に入り込まれた場合には、誰がやったことなのか後から確実に追跡できる記録を残すという考え方です。

この米国流身分証明 IC カードは、我が国のマイナンバーカードなどと異なり、自然人としての個人を証明するとともに、会社や官公庁などいずれの組織に所属しているのか証明するものとなっていることです。PIV-AV では全世界の民間航空関係者に共通に発行するため、グローバルな標準規格とすべく ATA（A4A）において Spec42 として検討が重ねられています。

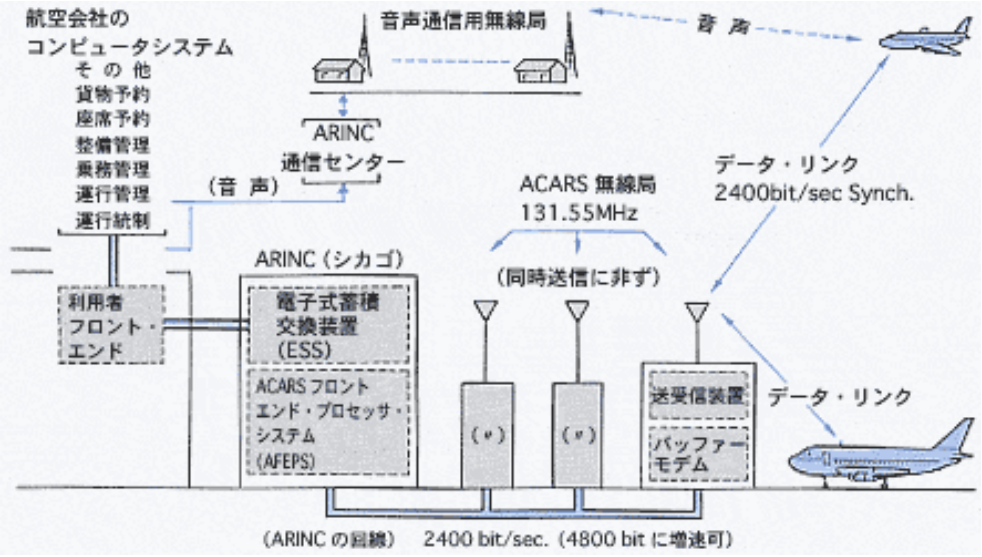



### (2) 航空機のデジタルネットワーク通信網

人＝個人認証、もの＝部品の AIT として電子的に識別できるようになり、そういった認証基盤の上でアプリケーションを動かすために、ネットワークが必要になります。民間航空業界では、フライト中の航空機とのデジタルデータリンクとして ACARS というシステムが古くから利用されてきました。その解説を「JAL 航空実用事典」から引用すると、

- エーカーズ（ACARS:automatic communications addressing and reporting system）空地デジタルデータリンク・システムとして，必要な運航情報を ARINC（ARINC:aeronautical radio incorporation エアリンク：北米，欧州の主要航空会社および米国の自動車産業メーカなどが株主になって設立され，軍事を含む航空通信のサービスを

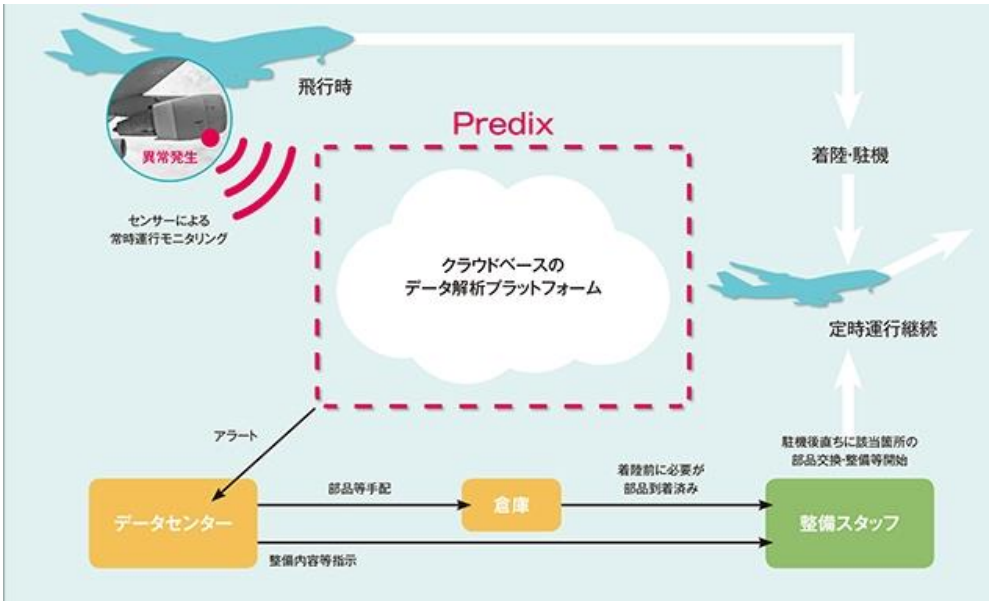
提供する非営利会社）の通信網を介して航空機側から地上へ，または地上から航空機側へ自動的に提供するシステム。出発・到着時刻や出発地・目的地，便名，搭載燃料などのデータはデータリンクの無線通信系を介して地上の ACARS 無線局に送信される。このデータは無線局から中央の処理装置に伝送され，電文型式にフォーマット変換された通報は，ARINC の電子式蓄積交換装置を介して各航空会社のコンピューター・システムへ直接伝送される。データ通信の内容としては，上述のほか最新の気象情報やフライトプランデータの送付，航空機の故障情報などの送付が可能であり，航空機側にも機上プリンターなどが設置されている。現在，欧米の航空会社では VHF-ACARS が実用に供されており，衛星を利用した空地データ通信もすでに実用化されている。




こういった航空機と地上を結ぶネットワークは、今後、より高速化し、どこでも使える環境が開発されてゆくものと考えます。

### (3) その他航空機の状況

その他、GE の「インダストリアル・インターネット」の取り組みなども有名です。GE は世界的な航空機エンジンのメーカであり、航空機本体と同様のリモートメンテナンスのための IoT 的なサービスを構築しています。




（GE 社のホームページより）

防衛航空機でも、世界規模の共同開発で製造されているロッキードマーチン社の F-35 では、ALIS(Autonomic Logistics Information System)というシステムで運航中の F-35 のセンサー情報をリアルタイムに地上に送信し、整備準備時間を短縮するなど、可動率の向上にデータを活用するようになっています。

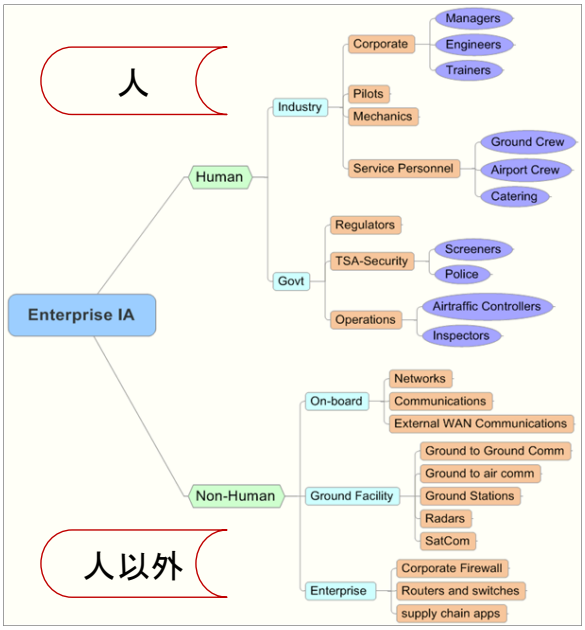
（ロッキードマーチン社のホームページより）

### (4) まとめ

このように航空機部品が AIT で自動識別できるようになり、LSAP としてインテリジェンスを持ち、それを扱う人を PIV-AV カードで認証するという環境が整うと、様々なセキュアなアプリケーション活用が出来るようになります。

これらの活用シーンを影で支えるのが PKI 認証の技術であると考えます。認証される対象は人に限らず、LSAP 部品などの「もの」を含めて航空業界の IoT が構成されています。これらはアメリカ国内規格を中心に標準化が検討され、次々にグローバルに適用され、すでにデファクトスタンダード化されつつあると言えましょう。

以下の図は、Exostar 社の Identity Assurance in Commercial Aviation 白書に掲載されている認証の対象とするものの一覧（一例）です。「人」の他に、ネットワーク機器や設備・部品、ソフトウェアなども対象ととらえています。




**航空業界者**
- 従業員
- パイロット
- 整備士
- クルースタッフ

**政府関係者**
- 航空当局
- セキュリティ 関係
- 管制官・ 検査官

**機上設備**
- ネット ワーク
- 通信機器

**地上設備**
- 地上通信機材
- レーダー
- 衛星通信機材

**その他**
- ファイアウォール
- アプリケーション

### (5) Carillon 社のソリューション

カナダの Carillon 社は、対象物のアイデンティティを保証し、紙ベースの認証から電子的な認証への移行を促進し、また、知的財産を保護すべく設計された様々なアイデンティティ管理ソリューションを提供している会社です。Pathfinder LSAP Suite は、次世代型航空機のために構築され、航空機をめぐるサイバーセキュリティにおける最適解を実装するために必要なあらゆるツールを提供しています。以下は、航空機のソフトウェア部品（LSAP）のセキュアな電子的配布ソリューションに関する紹介です。

---

「ライン交換ユニット（LRU：Line Replaceable Unit）」ソフトウェアは、従来の方法で更新する場合、航空機から一旦取外す必要があります。LRU は更新のためにメーカに戻されるか、若しくは、運航会社は特別な「携帯用データローディング装置（PDL：Portable Data Loader）」を使用してソフトウェアを更新します。これらの方法は両者とも、多大な時間、

労力、およびコストを要します。

次世代航空機は、「LSAP（Loadable Software Airplane Parts、ロード可能な航空機用ソフトウェアパーツ）」や「FLS（Field Loadable Software、フィールドローディング可能なソフトウェア）」を使用して、ソフトウェアを機上で更新する機能を備えています。

現状の規則では、そのような機上での更新に関して明確で簡略な方法が設けられておらず、特別条件が適用されます。現在の複雑なセキュリティ方式は、航空機運航会社に対して不必要な負担を課しています。

FAA（米国連邦航空局）は PS-AIR-21.16-02 を発し、ネットワークが非政府機関のものであって、航空機システムが非政府機関ネットワークを介して情報を受信するような、外部サービスやネットワークと直接接続する航空機システムにおける、最初の型式証明（TC：type certificate）、追加型式承認（STC：supplemental type certificate）、型式設計変更（amended TC）、又は追加型式設計変更（amended STC）の申請に対して、データの扱いは受信専用のみとする特別条件を発行する旨が記載されています。それらのネットワークには例えばインターネット、キャリアのネットワーク、空港・運航会社のワイヤレスネットワーク（Gatelink、 Wi-Fi 等）また、航空機システムに接続する携帯機器（iPad、EFB 等）などがあります。

Pathfinder LSAP Suite は ARINC 827 に基いて EDS クレートと呼ばれる電子的な入れ物に格納されます。EDS クレートは、ATA Spec.42 に則りデジタル署名が付与・検証されます。EDS クレートには、「装備品基準適合証（ARC：Authorized Release Certificate）」の「Electronic 8130-3, Form One and Form 1」を含みます。整備場におけるデジタル署名の使用は、保守作業に対する影響を最小限に抑え、運航会社での追加の IT 投資をほとんど要しないため、運航会社のコストを削減します。


航空機部品にデジタル署名を使用することによって、セキュリティ・プロセスは簡略化され、運航会社は、最小限のプロセス変更で既存の手続きをあまり変更せずにセキュアな運用

に移行することができます。デジタル署名の使用で、地上の通信環境がなくても機内におけるソフトウェアの EDS クレートの解凍や機上インストールを可能にしました。

---

弊社は、Carillon 社の日本代理店としてこれらのソフトウェア製品や電子証明書などを販売いたします。また、Carillon 社のノウハウを活用した国内ソリューションの構築などにも応じることが可能です。

また、A4A において Spec42 の検討を行っている DSWG（Digital Security Working Group）の会員メンバとして標準化活動にも参加しています。

略語

ACARS（automatic communications addressing and reporting system）
AIT（Automated Identification Technology）
LSAP（Loadable Software Aircraft Parts）
AHM（Airplane Health Management）
PIV-AV（Personal Identification Verification - Aviation）
CMB（Contact Memory Button）
RFID（Radio Frequency IDentification）

参考文献

(1) Identity Assurance in Commercial Aviation October 2007
http://www.evaaviation.com/wp-content/uploads/2017/02/W03_JV1_0-Future-of-Supplier-Portals.pdf
Exostar LLC.

(2) Secure Electronic Delivery of Software to the Aircraft
Carillon LSAP Suite catalogue