# 米国航空産業で利用されるPKI

株式会社コスモス・コーポレイション
濱口　総志

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

# 概要

1. FPKIの概要

2. LSAP
   A)DO-178C

3. Spec42
   A) PIV-AVと航空業界認証基盤

4. LSAPソフトウェアのセキュアな電子的配布ソリューション

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

# 米国　FPKIの背景

E Governance Act of 2002
連邦政府の電子化に向けた法律

FISMA(Federal Information Security Management→Modernization Act)
連邦情報セキュリティマネジメント法

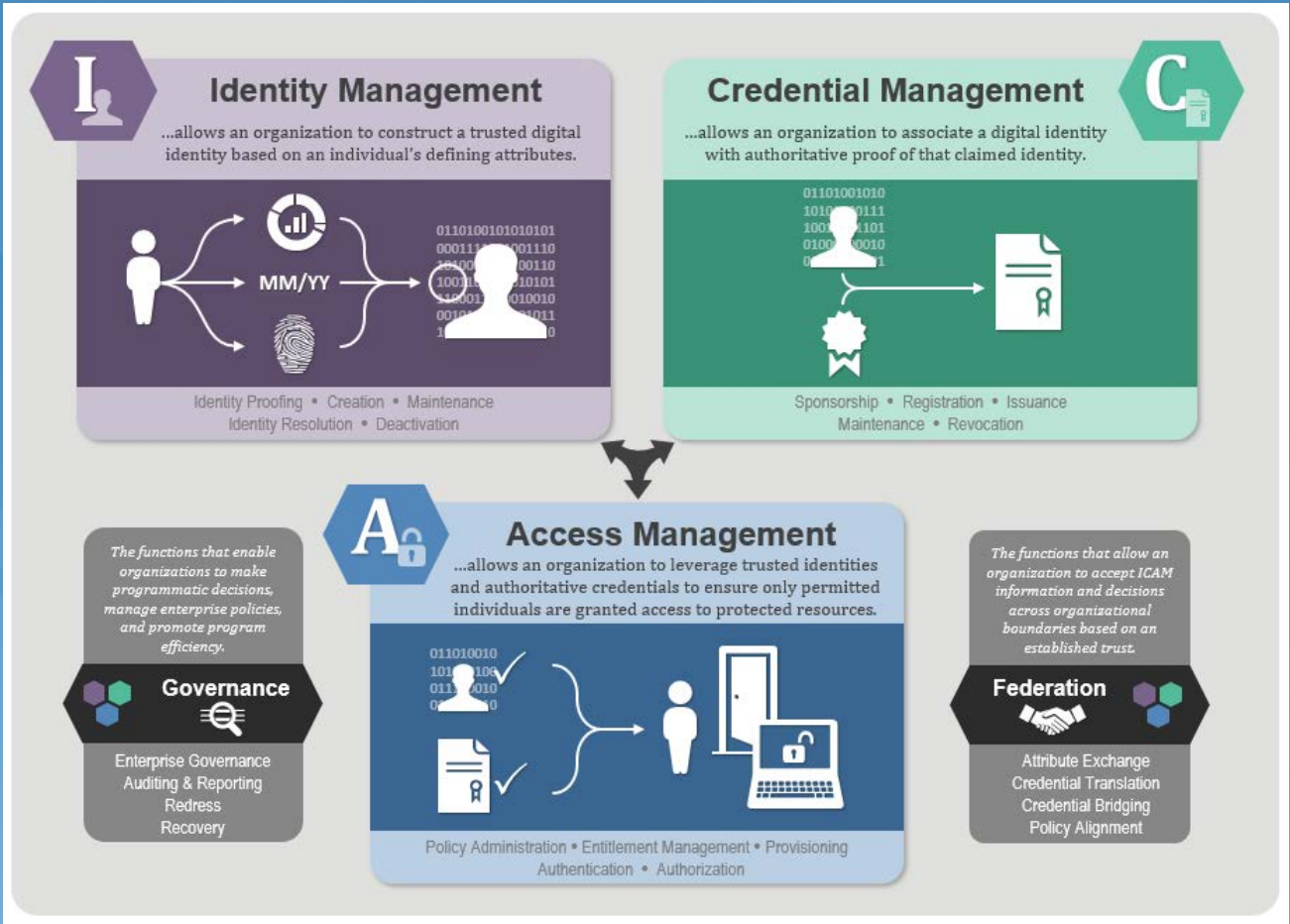
ICAM (Identity, Credential and Access Management)
適切な個人が適切な理由で適切な情報に適切な時にアクセスできるようにする

FICAM (Federal Identity, Credential and Access Management)
米国連邦政府のICAMの実装であり、政府機関統一のICAM基準、ベストプラクティス、実装ガイドを提供

OMB M-04-04
NIST SP 800-63
認証の保証レベル(LoA)を規定（IAL, FAL, AAL）

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

# FICAM

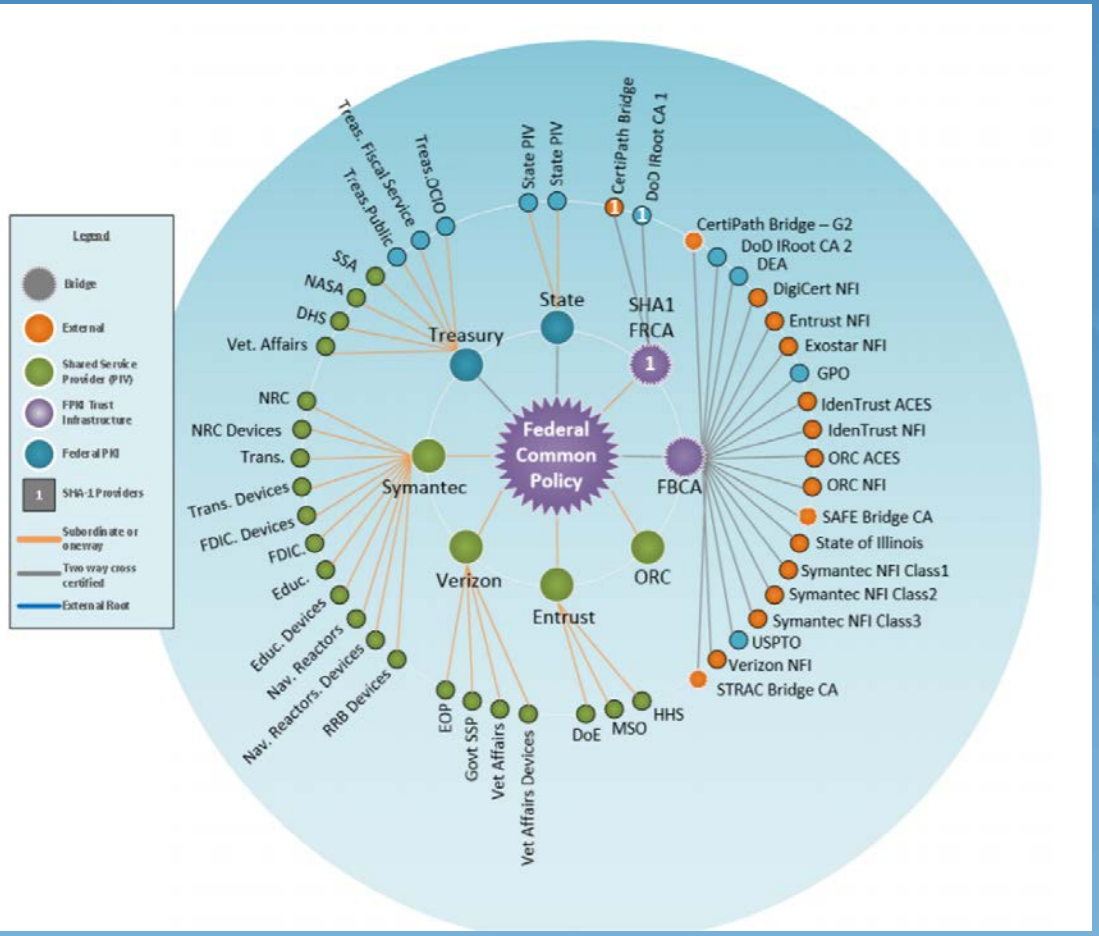



Cosmos

POFESSIONALS OF SAFETY ENGINEERING

出典：Idmanagement.gov

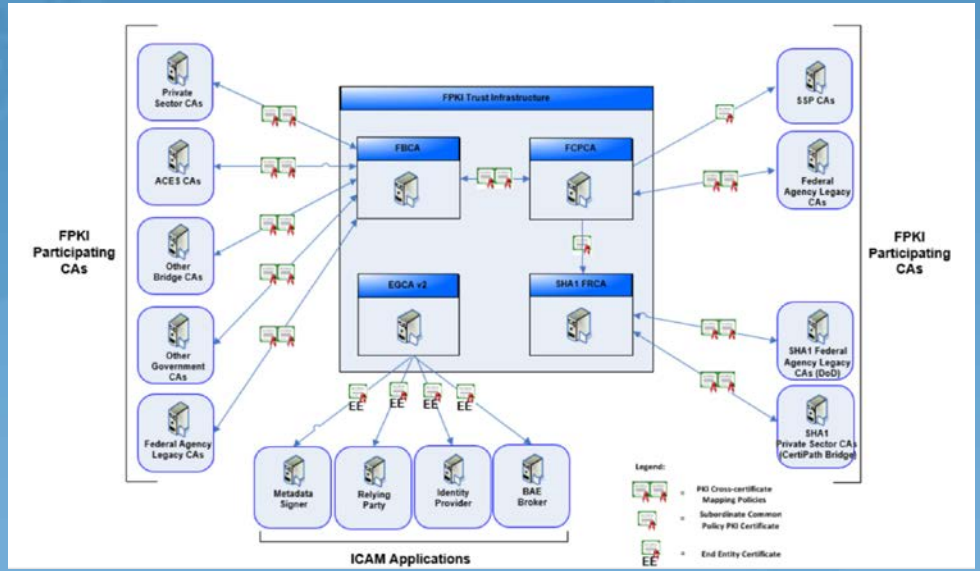
# FPKIのトポロジー




出典：Idmanagement.gov

# FPKIトポロジーのコア

- FCPCA, Federal Common Policy CA
  - FPKIのトラストアンカー
- SHA1 FRCA
  - レガシー
- FBCA, Federal Bridge CA
  - トラストハブ、ブリッジ
- EGCA, e-Gov CA
  - ICAM Application
- SSA, Shared Service Provider
  - 政府専用認証局（民間／政府機関）




出典：Idmanagement.gov

# FPKI × LoA (NIST SP 800-63)

| Certificate Policy | ID Proofing | Token | Token and Credential Management | Overall LOA Equivalence |
|---|---|---|---|---|
| Common-Auth<br>PIV-I Auth<br>SHA1 Auth | LOA 4 | LOA 4 | LOA 4 | LOA 4 |
| Common –SW | LOA 4 | LOA 3 | LOA 4 | LOA 3 |
| Common-HW<br>PIV-I HW<br>SHA1-HW | LOA 4 | LOA 4 | LOA 4 | LOA 4 |
| Common-High<br>FBCA-High | LOA 4 | LOA 4 | LOA 4 | LOA 4 |
| FBCA Basic | LOA 3 | LOA 3 | LOA 3 | LOA 3 |
| FBCA Medium<br>FBCA Medium CBP | LOA 3 | LOA 3 | LOA 4 | LOA 3 |
| FBCA MediumHW<br>FBCA MediumHW-CBP | LOA 3 | LOA 4 | LOA 4 | LOA 3 |
| Common-cardAuth<br>PIVI-cardAuth<br>SHA1-cardAuth | LOA 4 | LOA 2 | LOA 4 | LOA 2 |

出典：Idmanagement.gov

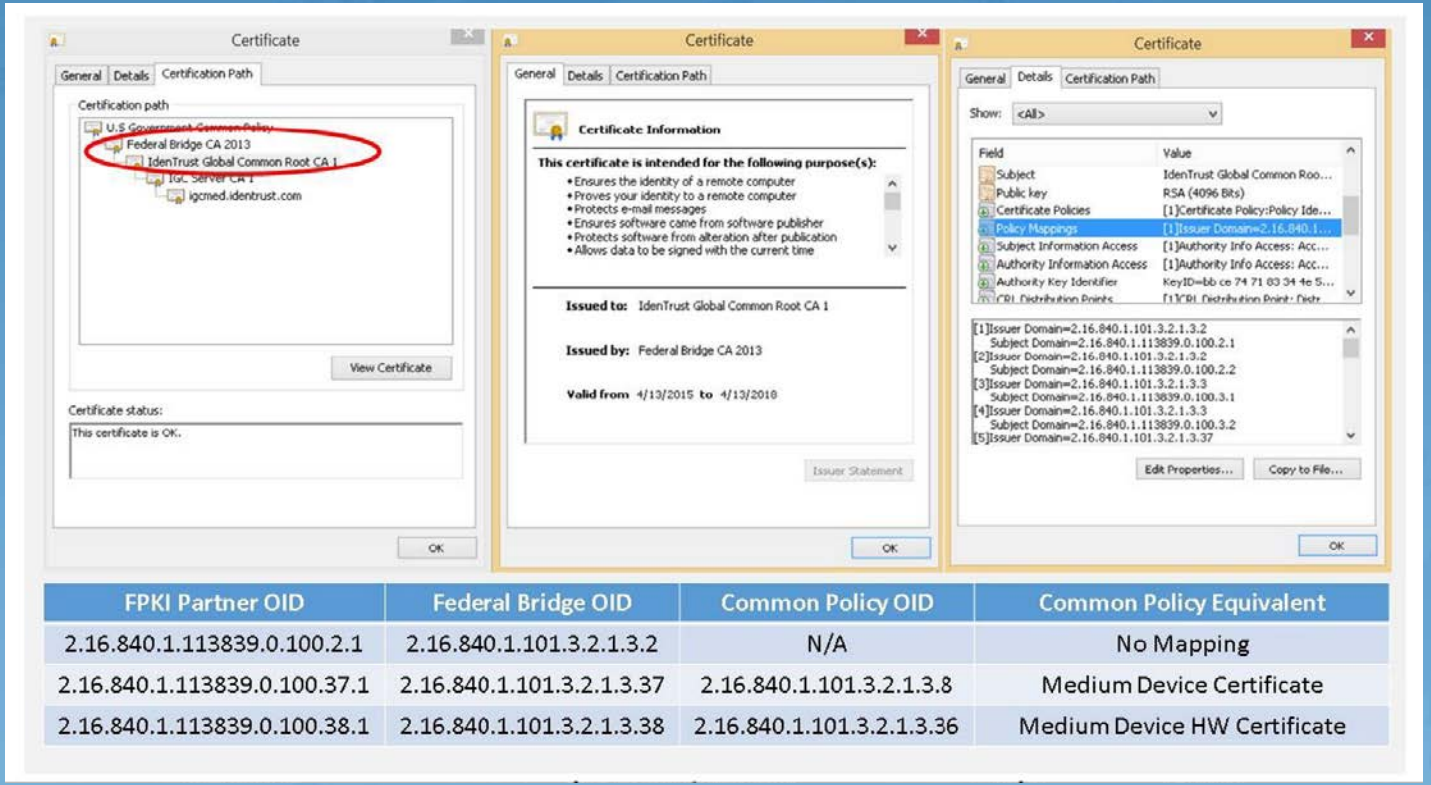
# ポリシーマッピング

- 相互認証（Cross-certificate)の前提条件としてのポリシーマッピング
- 相互認証する認証局が互いの証明書ポリシーを確認し、
比較可能であり、同等であることを認める

| FCPCA Policy | FCPCA OID | FBCA OID | FBCA Policy |
|---|---|---|---|
| common-policy | 2.16.840.1.101.3.2.1.3.6 | 2.16.840.1.101.3.2.1.3.3 | FBCA-medium |
| common-High | 2.16.840.1.101.3.2.1.3.16 | 2.16.840.1.101.3.2.1.3.4 | FBCA-High |
| common-HW | 2.16.840.1.101.3.2.1.3.7 | 2.16.840.1.101.3.2.1.3.12 | FBCA-mediumHW |
| common-devices | 2.16.840.1.101.3.2.1.3.8 | 2.16.840.1.101.3.2.1.3.37 | FBCA-mediumDevice |
| common-devicesHW | 2.16.840.1.101.3.2.1.3.36 | 2.16.840.1.101.3.2.1.3.38 | FBCA-mediumDevice-HW |

出典：Idmanagement.gov

# ポリシーマッピング(証明書の拡張領域)




| FPKI Partner OID | Federal Bridge OID | Common Policy OID | Common Policy Equivalent |
|---|---|---|---|
| 2.16.840.1.113839.0.100.2.1 | 2.16.840.1.101.3.2.1.3.2 | N/A | No Mapping |
| 2.16.840.1.113839.0.100.37.1 | 2.16.840.1.101.3.2.1.3.37 | 2.16.840.1.101.3.2.1.3.8 | Medium Device Certificate |
| 2.16.840.1.113839.0.100.38.1 | 2.16.840.1.101.3.2.1.3.38 | 2.16.840.1.101.3.2.1.3.36 | Medium Device HW Certificate |

出典：Idmanagement.gov

# PIV (Personal Identity Verification)

連邦政府職員（及び契約者）向けIDカード

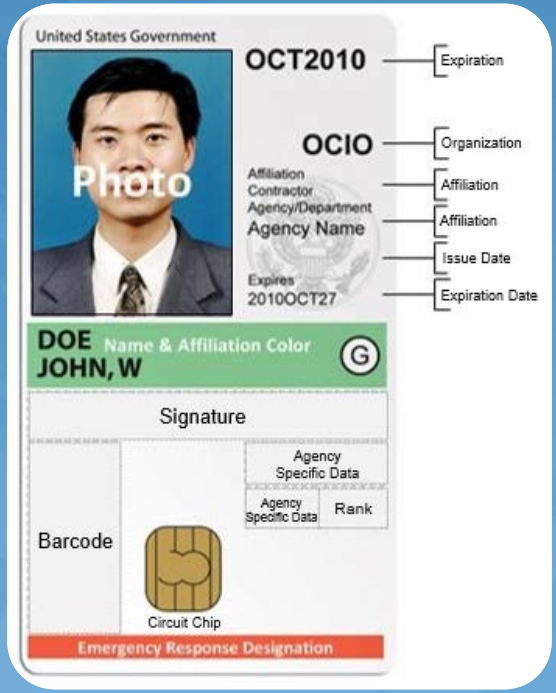
- HSPD12 (Homeland Security Presidential Directive)
- NIST FIPS 201

証明書

- PIV Authentication
- Card Authentication
- Digital Signature
- Encryption

用途：

- PACS、LACS
- 署名
- 暗号化



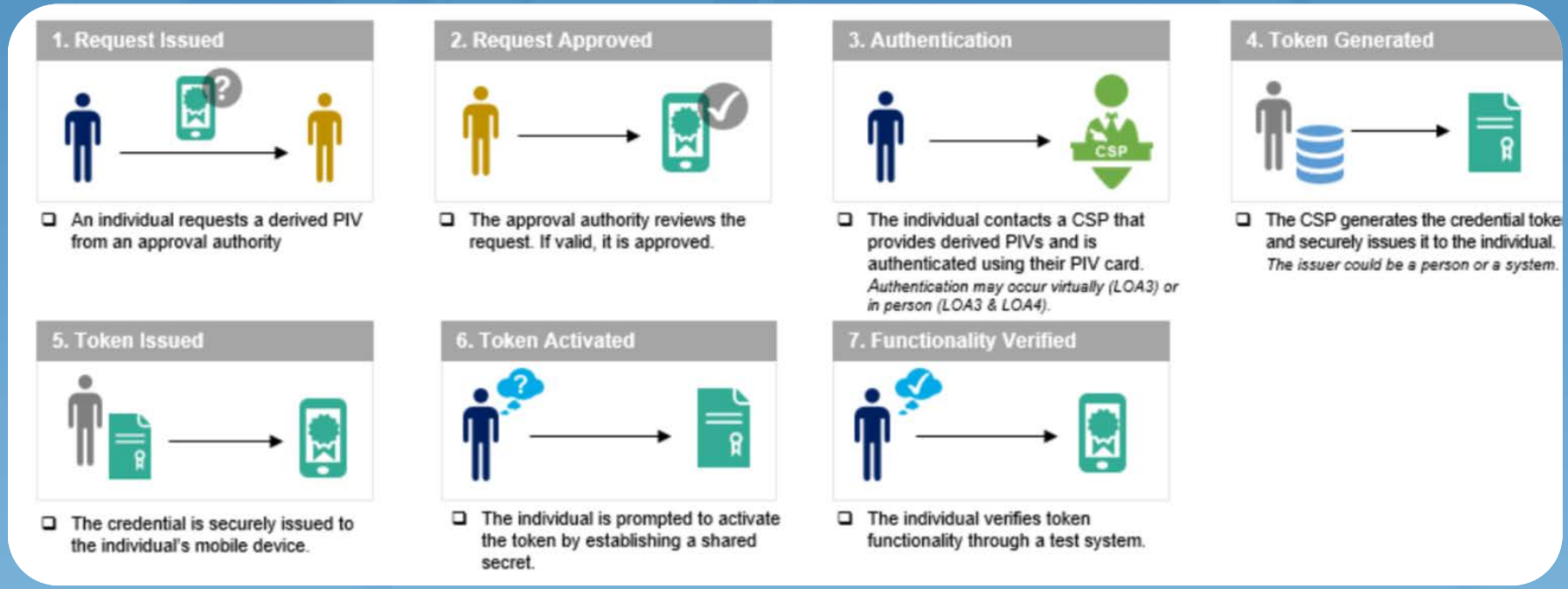

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

出典：Wikipedia

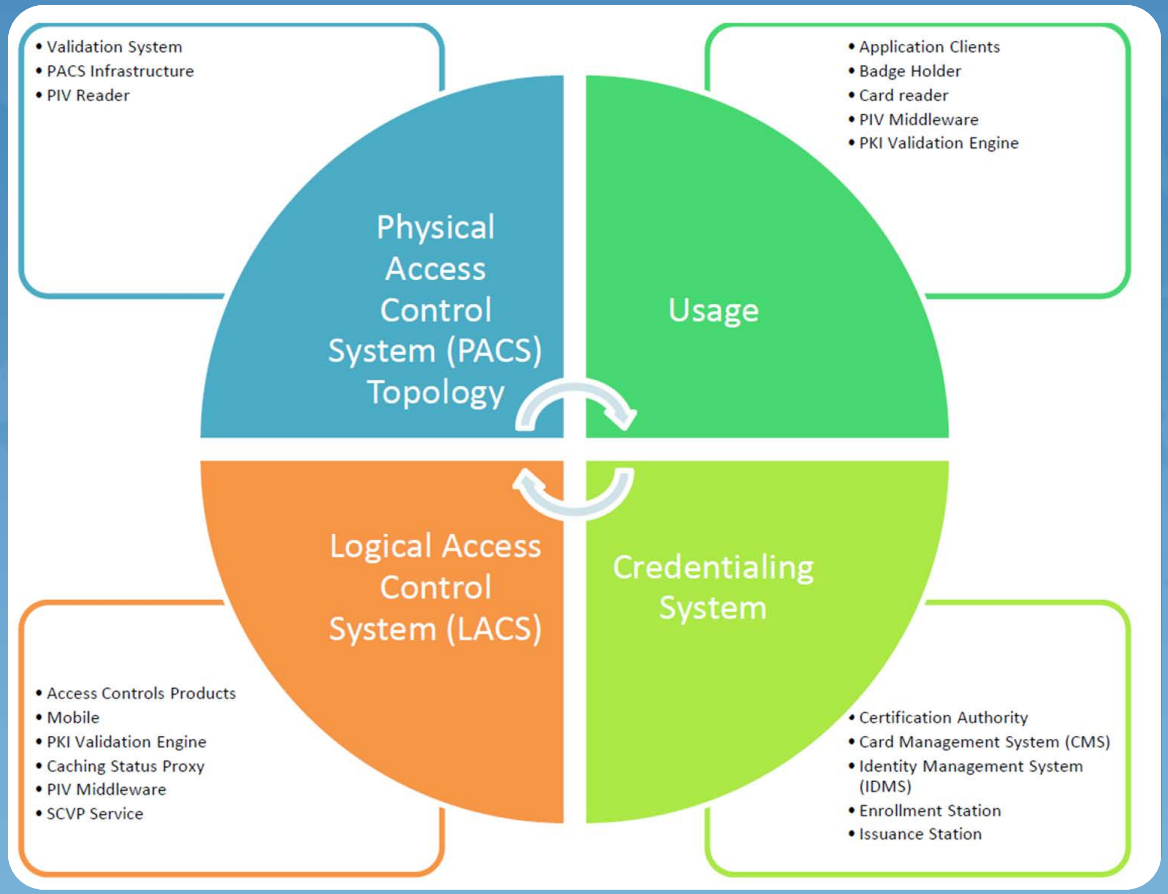
# Derived PIV

PIVカードの所持者が、PIVクレデンシャルをスマホに格納する仕組み
LoA3orLoA4




出典：Idmanagement.gov

# FICAM Test Program




出典：Idmanagement.gov

# And PIV-I (Interoperable)…

PIVのスキームを民間に拡大

PIVの技術標準に適合した民間向けIDカード＋PIV-I証明書

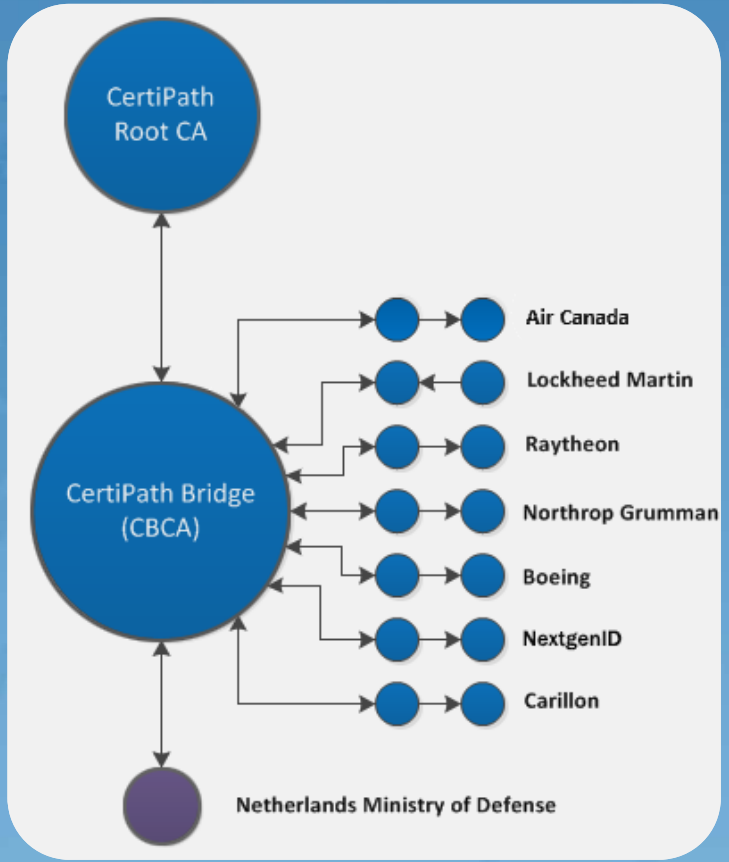
PIV向け環境（つまり政府システム、政府施設等）で検証可能（相互運用性）

出典：Idmanagement.gov

# 航空業界向けPKI

- 航空宇宙／防衛産業向けブリッジCA
- CertiPath Bridge CA

- 業界の出資で設立
- CBCAとの相互認証には、PMAの承認が必要




出典：www.certipath.com

# 航空産業の機能--過去と現在

| 機能 | 以前 | 現在 |
| --- | --- | --- |
| 配布される航空機のソフトウェア | フロッピーディスクまたは他の物理メディアを使用 | 電子的に配布（数千の部品） |
| 航空機ソフトウェア部品へのロード | データローダおよびその他のメンテナンス機器 | PKI署名付きパーツ、オンボードネットワーク経由のロード |
| フライトオペレーションデータのオフロード | 物理接続による手動転送 | 無線接続による自動転送 |
| メンテナンス記録の文書化 | 整備士による紙ベースおよび署名 | 電子証明書付き |
| 承認済みリリース証明書 | 紙ベースで倉庫に保管 | 電子署名付き証明書 |
| 従量とバランスデータと計算 | 複雑な多段階のプロセス | 飛行機のデータに基づいて自動化 |
| 航空機のIPネットワークにワイヤレス接続 | N/A | 航空機との間でデータを認証し、安全に転送する |

参照：http://www.ataebiz.org/eBusiness%20Forum/2017%20-%20Amsterdam/Presentations/11-SecuringYourDataBrossard.pdf

# LSAPとは

航空機の技術発展により、部品機能の高度化・複合化が進み、装備品が機械制御から電気的な制御に移行。ソフトウェアを組み込んだ部品が増加。

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）と呼ぶ。

LSAP搭載数の目安

1000 software parts


40 system/software suppliers over three continents


200 software parts


50 software parts

From Airbus presented at the 2006 ATA e-Business Forum

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

# ソフトウェア信頼性基準　DO-178C

ソフトウェア搭載部品の増加に伴い、その部品自身の信頼性や安定性が重要な課題

FAA（アメリカ連邦航空局）では、ソフトウェアおよび制御される装置を含むシステムの製造基準としてRTCA DO-178C（RTCA：Radio Technical Commission for Aeronautics）という規格を定め、認証も行うしくみを作成

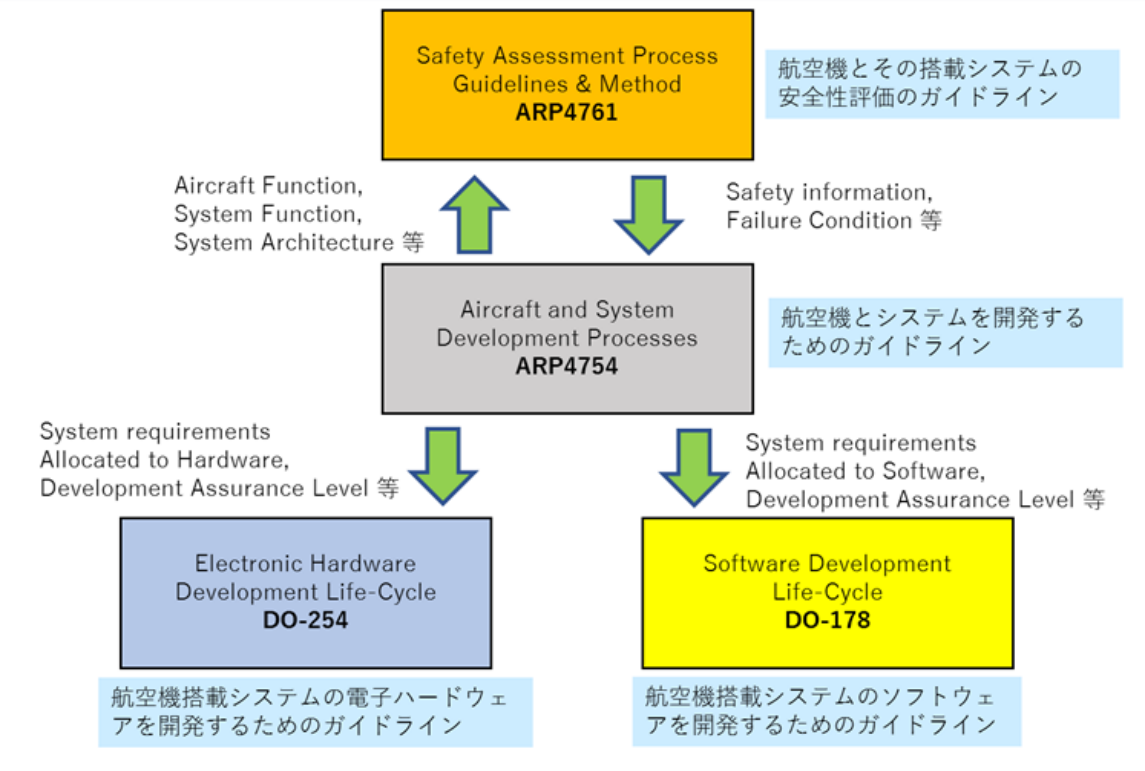



図　各ガイドライン文書の位置付け

出典：RTCA/DO-178Cの詳細　MHIエアロスペースシステムズ株式会社より
http://www.masc.co.jp/techf/documents/ObjectivesAndToolInDO178C.pdf

# ソフトウェアレベル

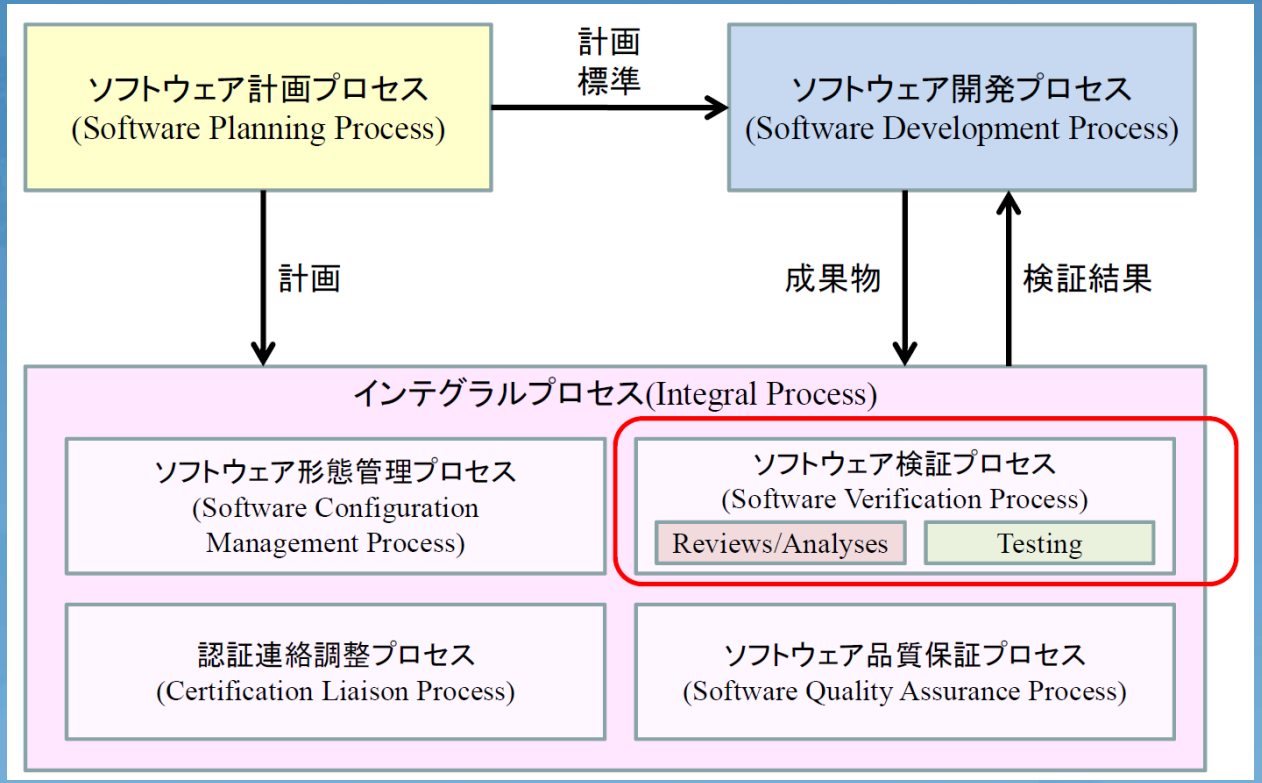
DO-178Cでは、故障状態におけるカテゴリに応じて、5段階のソフトウェアレベルを定義している。
このソフトウェアレベルに応じて、要求事項が変わる。

| 故障状態のカテゴリ | 内容 | ソフトウェアレベル |
|---|---|---|
| 壊滅的 | 安全な飛行状態と着陸が不可能となる故障状態 | A |
| 危険／非常に重大 | 航空機の能力または悪状況により乗務員の対応能力が任務遂行不可まで低下し、生命にかかわる負傷者が出るような故障状態 | B |
| 重大 | 航空機の能力または悪状況により乗務員の対応能力が任務遂行の妨げになるほど低下し、乗員乗客が不快症状となるような故障状態 | C |
| 軽微 | 航空機の安全が著しく低下することはなく、乗員は対応能力範囲内で任務を遂行できるような故障状態 | D |
| 影響なし | 航空機の操縦能力や乗員負荷に影響しない故障状態 | E |

# ソフトウェアプロセス

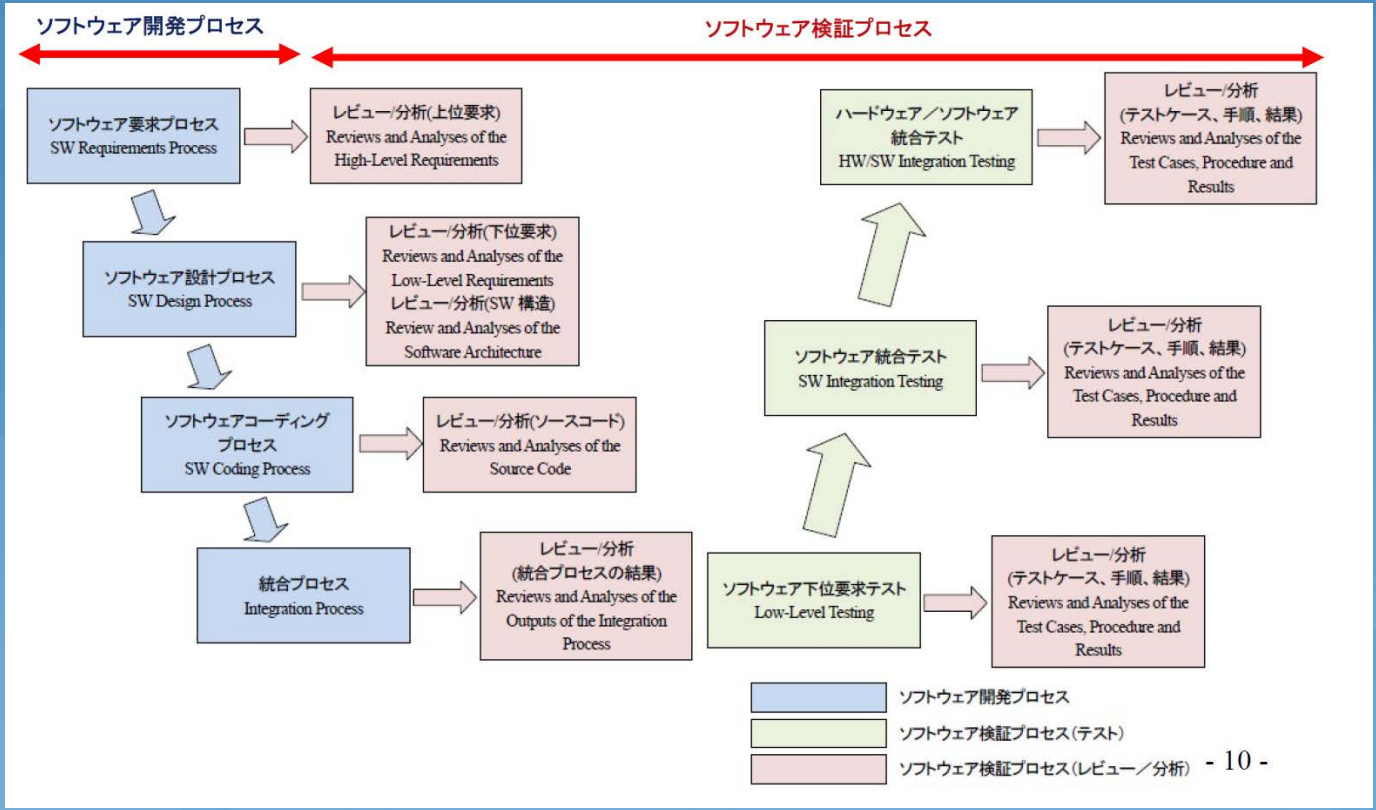
DO-178Cでは、次の3つのソフトウェアプロセスを定義している。
・ソフトウェア計画プロセス
・ソフトウェア開発プロセス
・インテグラルプロセス

各プロセス毎に、ソフトウェアレベルに応じた達成すべき目標が定められている。




出典：RTCA/DO-178Cの詳細　MHIエアロスペースシステムズ株式会社、
http://www.masc.co.jp/techf/documents/ObjectivesAndToolInDO178C.pdf

# ソフトウェア開発プロセスとソフトウェア検証






出典：RTCA/DO-178Cの詳細　MHIエアロスペースシステムズ株式会社、
http://www.masc.co.jp/techf/documents/ObjectivesAndToolInDO178C.pdf

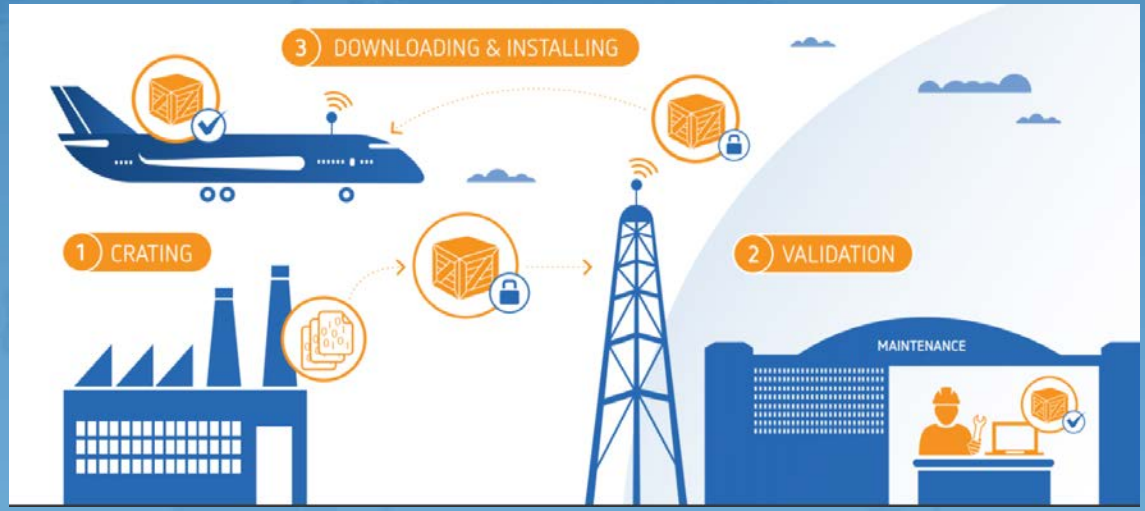
# LSAPソフトウェアのセキュアな電子的配布

## Carillon社のLSAP-Suite

ボーイングが787でLSAP対応で採用

DO178Cで評価済みのソフトウェア部品（LSAP)をEDSクレート（AR INC827）に格納し、EDSクレートに電子署名

EDSクレートは、航空会社、メインテナンス会社、機内で署名／検証される



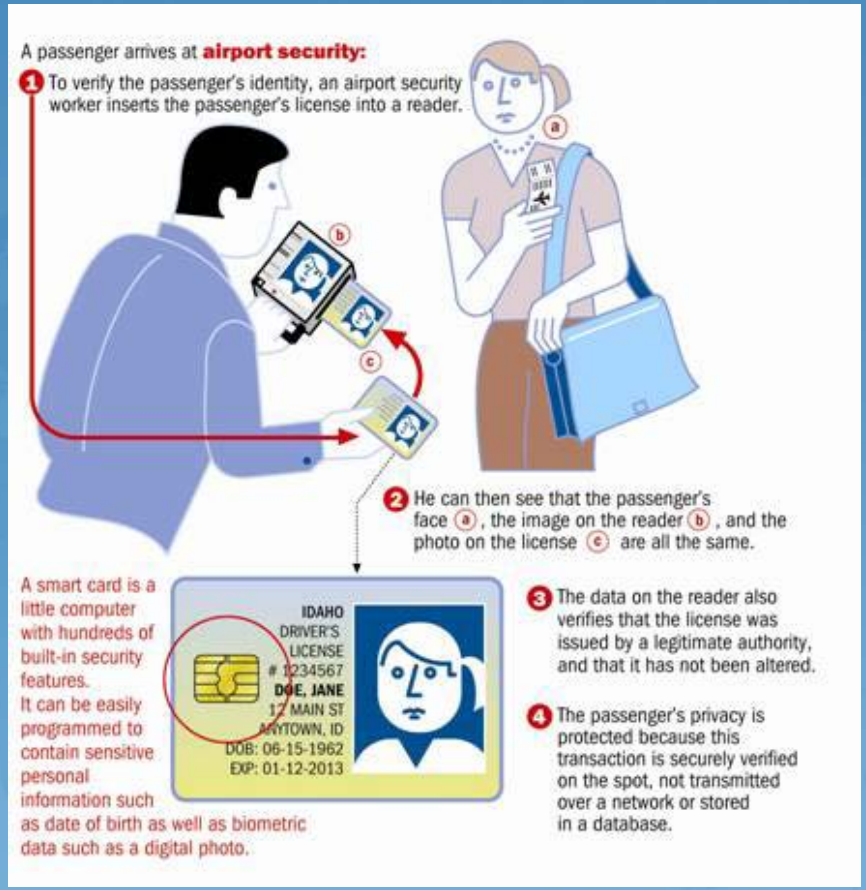

出典：https://www.carillon.ca/

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

# ATA Spec 42

DO-178Cの沿って厳格に作られた航空機部品のソフトウェアは、実際に飛ぶ航空機に搭載され、運用が始まる。運用後は、ソフトウェアの修正や改造が行われると、部品の製造会社からCDやネットワークを介して航空会社やMRO事業者に送られる。

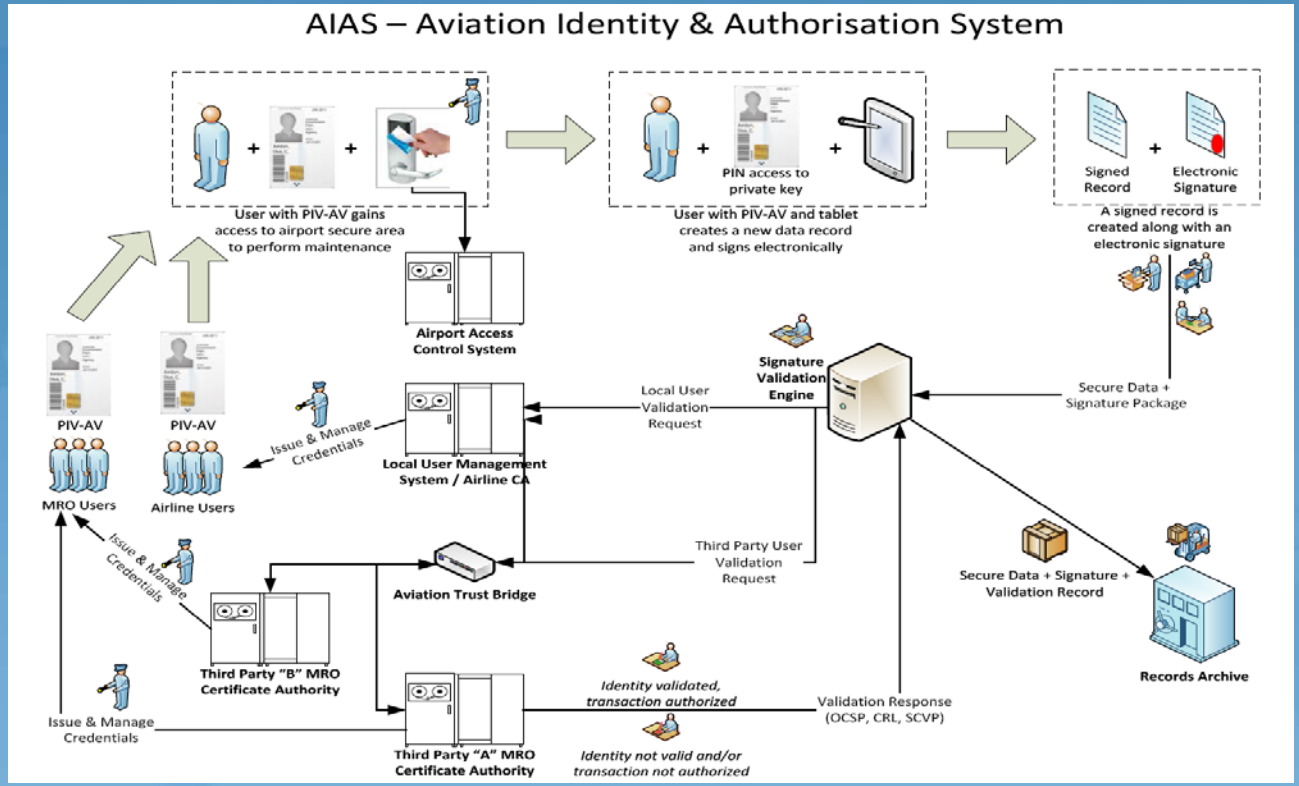
ATA Spec42（ATA：Air Transport Association of America）により空港職員や整備員・パイロット、部品製造会社技術員などの航空業界全体に対して、共通的な個人認証を行う為、PIV-AVカードによる身元確認および認証の基盤をグローバル統一的に標準化しようとしている。




出典： Aviation Identification & Authorisation System
https://www.iata.org/whatwedo/ops-infra/Documents/Aviation_Identification_%20Authorisation_System_-_White_Paper_-_v1_2015.pdf

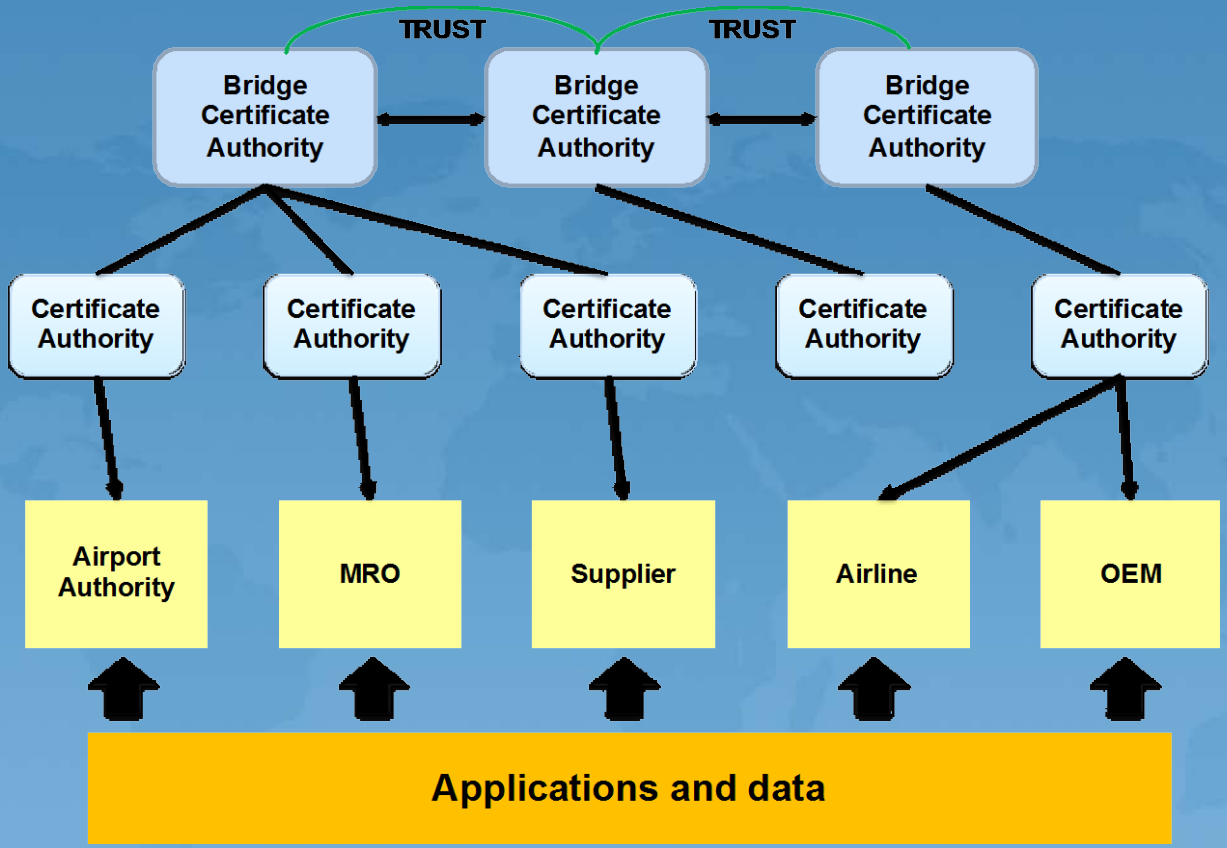
# PIV (PIV-AV:Aviation)

## IATA Aviation Identification & Authorisation System(2015.8)




出典: Aviation Identification & Authorisation System
https://www.iata.org/whatwedo/ops-infra/Documents/Aviation_Identification_%20Authorisation_System_-_White_Paper_-_v1_2015.pdf

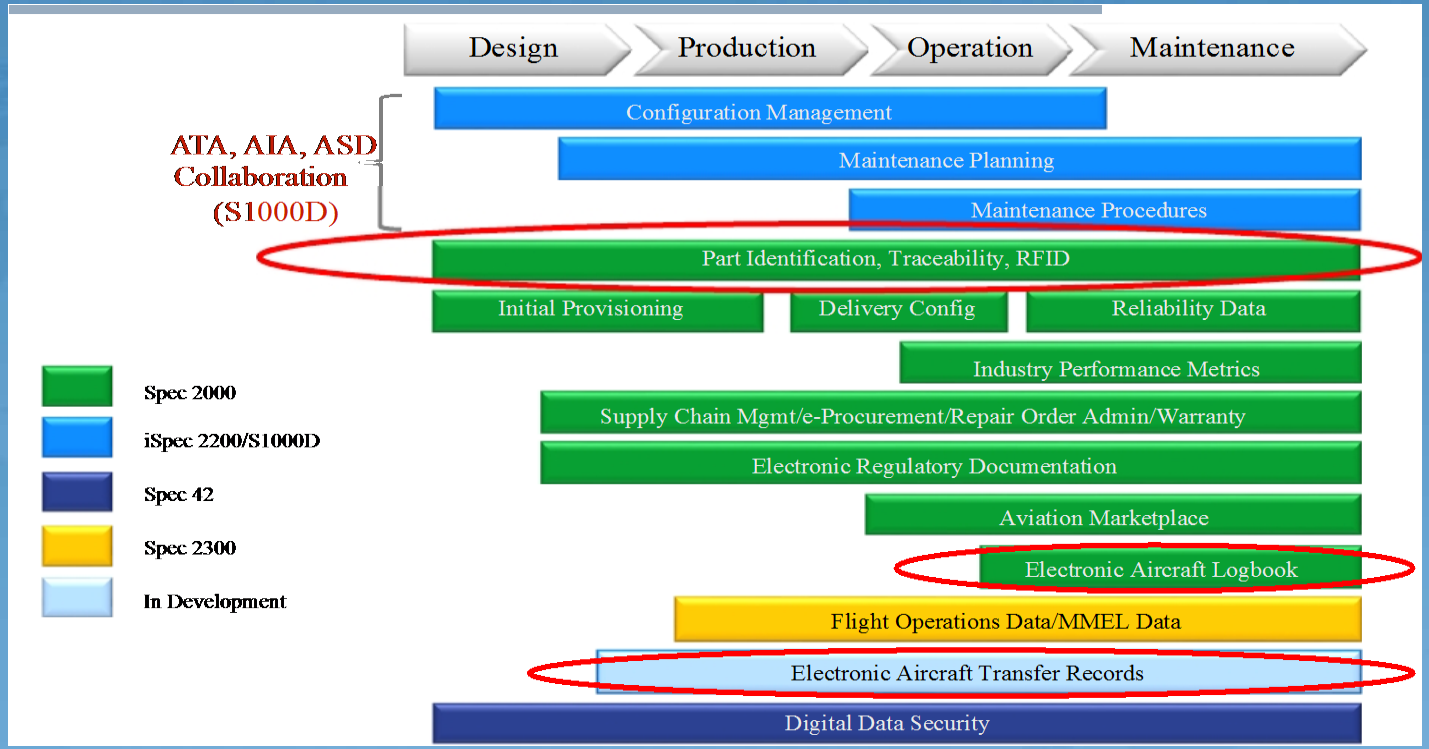
# Bridge Trust Model - Federation




出典：Securing Your Data –ATA Spec 42,
http://www.ataebiz.org/eBusiness%20Forum/2017%20-%20Amsterdam/Presentations/11-SecuringYourDataBrossard.pdf

# ATA e-Business program

ATA e-Business Programは、民間航空業界が協力し技術・整備・部材管理・飛行運用・航空機譲渡を支援する情報交換のための基準（Spec2000、iSpec2200/S1000D、Spec2300、Spec42）を作成・維持更新



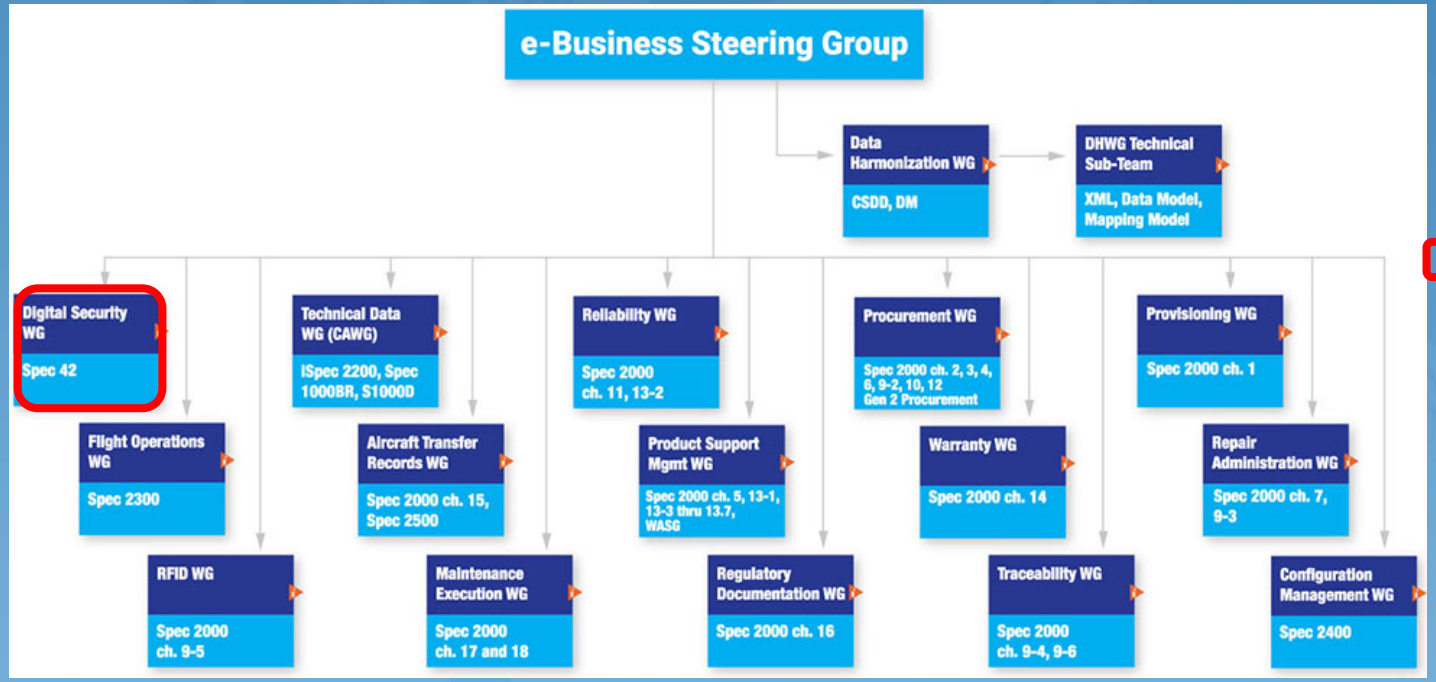

出典：日本航空宇宙工業会 http://www.sjac.or.jp/common/pdf/kaihou/201708/20170806.pdf

# ATA e-Business Standards

Common Support Data Dictionary (CSDD)
iSpec 2200: Information Standards for Aviation Maintenance
iSpec 220 Extract - ATA Standard Numbering System
Spec 2300 - Data Exchange Standard for Flight Operations
S1000D, International Specification for Technical Publications
Spec 1000BR - Civil Aviation S1000D Business Rules
Spec 2000 - Provisioning (ch. 1)
Spec 2000 - Procurement Planning (ch. 2)
Spec 2000 - Materiel Management (ch. 3 – 4, 6)
Spec 2000 - Repair Order Administration (ch. 7)
Spec 2000 - Automated Identification and Data Capture (ch. 9)
Spec 2000 - Reliability Data Collection and Exchange (ch. 11)
Spec 2000 - Airline Inventory Redistribution System - AIRS (ch. 12)
Spec 2000 - Industry Metrics (ch. 13)
Spec 2000 - Warranty Claims (ch. 14)
Spec 2000 - Aircraft Transfer Parts List (ch. 15)
Spec 2000 - Authorized Release Certificate (ch. 16)
Spec 2000 - Electronic Logbook (ch. 17)
Spec 42 - Aviation Industry Standards for Digital Information Security
World Airlines and Suppliers Guide (WASG)
Spec 100 - Manufacturers Technical Data
Spec 101 - Ground Equipment Technical Data

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

# Working Groups




Spec42のWG

Aircraft Transfer Records WG
Configuration Management WG
Data Harmonization WG
DHWG Technical Sub-Team
Digital Security WG
Flight Operations WG
Maintenance Execution WG
Procurement WG
Product Support Mgmt WG
Provisioning WG
Regulatory Documentation WG
Reliability WG
Repair Administration WG
RFID WG

図 E-Business Steering Group
<出典：http://www.ataebiz.org/Pages/working-groups.aspx>

# 関連標準

- ARINC 665 and 827 standards: Loadable Software Aircraft Parts
- ATA Spec 42 PKI Implementation Guidance for Aircraft
- Also known as 8130-3 (United States), Form One (Canada) Each component of an aircraft is tracked, its lifecycle documented
- Aviation Identification & Authorisation System Whitepaper Version 1 August 2015

# ご清聴ありがとうございました

**株式会社コスモス・コーポレイション**

ITセキュリティ部

濱口　総志
Tel:　0598-30-5911
E-Mail:　s.hamaguchi@cosmos-corp.com
URL:　www.safetyweb.co.jp/

Cosmos
POFESSIONALS OF SAFETY ENGINEERING