出典: https://www.jal.co.jp/ar/ja/offers/A350-1000/

第27回 航空輸送技術講演会 (2024年1月26日)

主催：公益財団法人 航空輸送技術研究センター　後援：国土交通省航空局

「航空サイバーセキュリティ」

日本航空株式会社 安全推進部 大﨑 康二郎・セキュリティ戦略部 福島 雅哉

Ver.01

目次

1. 新しい脅威が顕在化（大崎）
2. 「航空サイバーセキュリティ」の必要性（福島）
3. 「航空サイバーセキュリティ」の進め方（福島）
4. 今後のチャレンジ（大崎）

1. 新しい脅威が顕在化
(航空サイバーリスク: 衛星測位システムへの干渉例)

衛星測位システム 干渉

◆航空サイバーリスクの顕在化

1. 衛星測位システム なりすまし事案

イラク上空で2023年9月に初報告。一例では他社の777が**イラク上空の機位表示だったが、(本来の衛星からではなく)地上からの偽信号によりイランに入域しそう**になり、イラク・バグダッド航空管制に以下のように問い合わせたと紹介がありました。

「今何時か、私たちはどこか？」

“What time is it, and Where are we ?"

東　西

紫：JAL欧州線　日本行

南

東　西

サイバーリスクが航空安全への影響が顕在化した初事例か。

※出典: OPS GROUP

なりすまし20例:747/777/737/E190/ビジネスジェット等

出典: OPSGROUP https://ops.group/blog/gps-spoof-attacks-irs/

衛星測位システム 干渉

◆航空サイバーリスクの顕在化

2. 対地接近警報装置*

他社で中東地域等で対地接近警報装置の**'Terrain (地表面) Ahead, Pull Up' 警報**が以下の2ケースで複数発生。

*EGPWS：Enhanced Ground Proximity Warning System

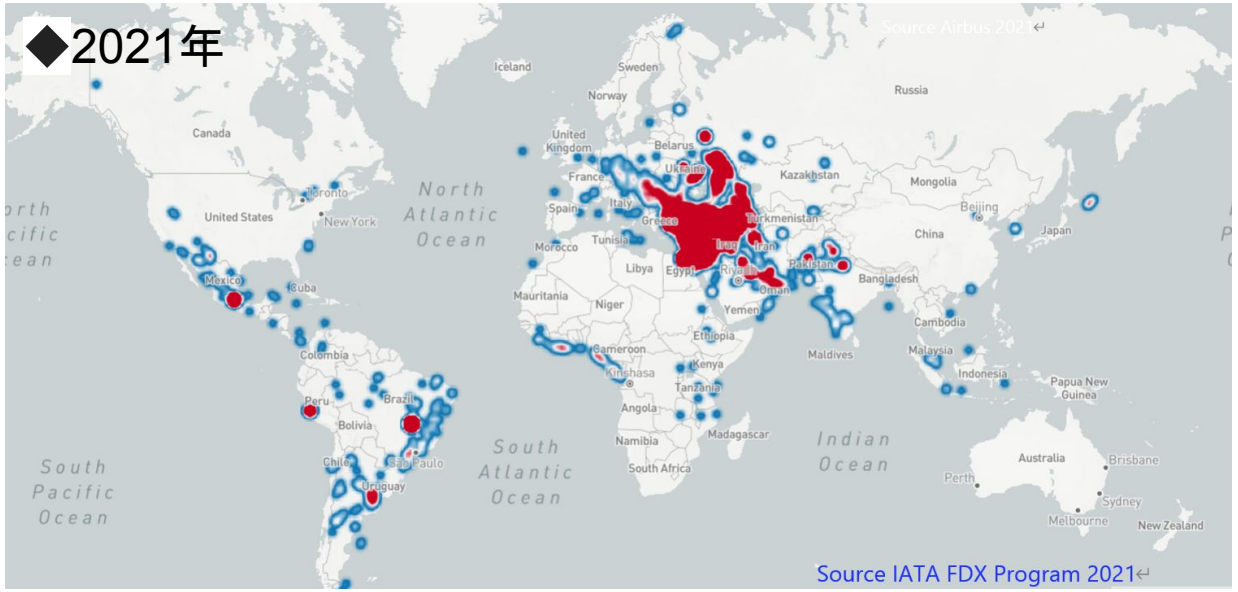
1) **巡航中**に発生

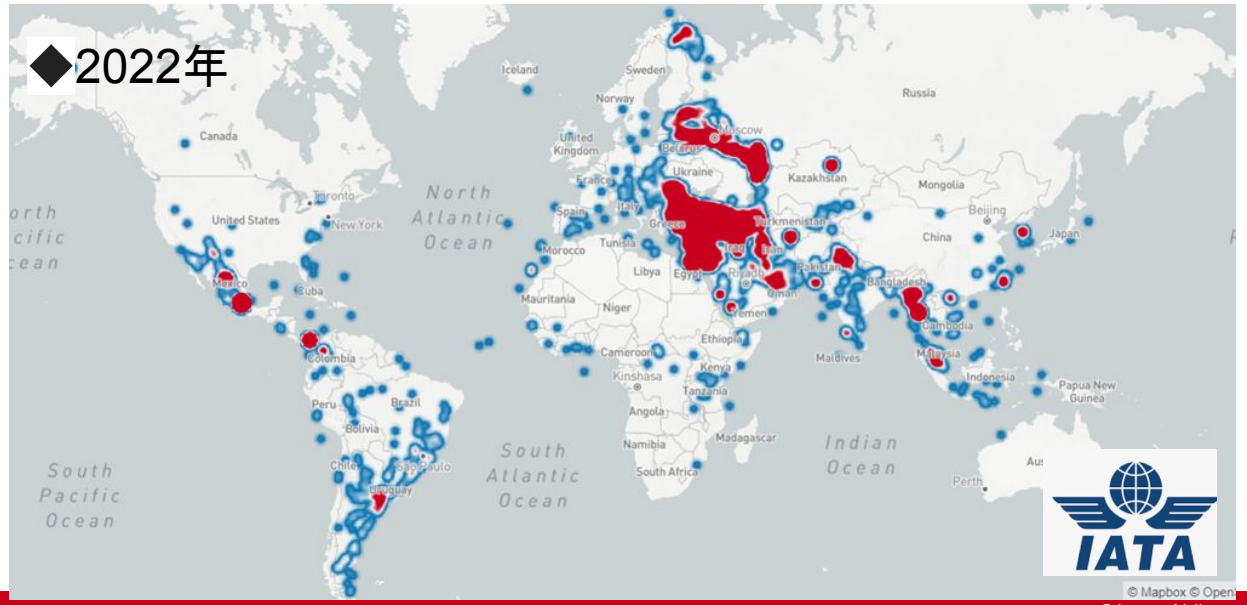
※右写真: 高度37,000フィート
(約11,000メートル)

2) **降下開始点(Top Of Decent)から着陸まで**

出典: https://www.reddit.com/r/aviation/comments/18kdo15/gps_loss_at_jedda_air_space_leads_to_false_egpws/

衛星測位システム 干渉





◆頻度：増加中（青、赤）

◆地域：拡大中

バルト海、黒海、中東、ミャンマー等で観測

※地政学上リスクのある地点での発生が多い

リスクの高まり

(今後、衛星使用の航法比率が一層の高まりが想定)

なお、本干渉の事例は、以下の典型例

①リスクの多様化

(フィジカルセキュリティーからサイバーセキュリティーへ)

②リスクの地域的拡大

(グローバル化)

＝＞今後、リスクの拡大への対応体制が必要

図出典：IATA Global Navigation Satellite System GNSS-Radio Frequency Interference Safety Risk Assessment(Sep.2023)
https://www.iata.org/contentassets/c8e90fe690ce4047a8edfa97f4824890/iata_safety_risk_assessment_gnss_interference.pdf

米欧当局、IATA、製造メーカーが注意喚起

◆FAA(米連邦航空局) 2023年11月

INFORMATION NOTE

Federal Aviation Administration

11 December 2023

Prepared by the Security & Hazardous Materials Safety Organization (ASH)

Worldwide – Global Positioning System/Global Navigation Satellite System (GPS/GNSS) Jamming and Potential Spoofing Poses Potential Aviation Safety Risk

Global Positioning System/Global Navigation Satellite System (GPS/GNSS) jamming and potential spoofing activities in conflict zones and areas of heightened tensions pose potential safety-of-flight risks to civil aviation operations in multiple Flight Information Regions (FIRs). Recent GPS/GNSS jamming and spoofing activities reported by various civil air operators in the Tel Aviv FIR (LLLL) and adjacent airspace follow similar upticks in GPS/GNSS interference reporting in the Baghdad and Baku FIRs (ORBB and UBBA, respectively).

◆EASA(欧州安全機関) 2023年11月(最新版)

EASA SIB No.: 2022-02R2

EASA
European Union Aviation Safety Agency

Safety Information Bulletin

Operations – ATM/ANS - Airworthiness

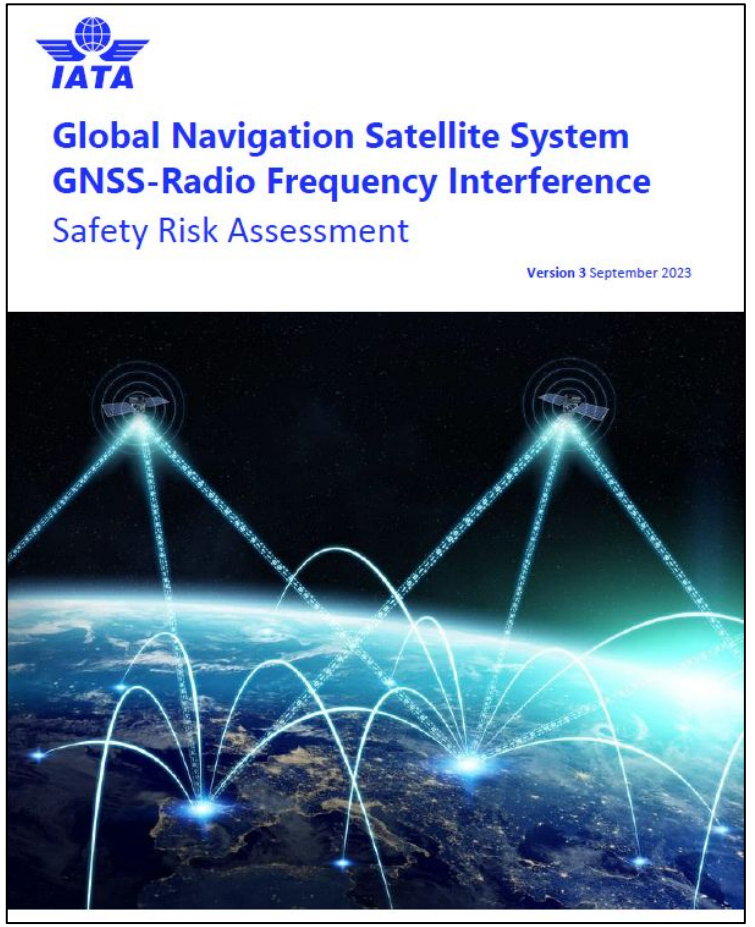
SIB No.: 2022-02R2

Issued: 06 November 2023

Subject: **Global Navigation Satellite System Outage and Alterations Leading to Navigation / Surveillance Degradation**

Revision:
This SIB revises EASA SIB 2022-02R1 dated 17 February 2023.

◆IATA 妨害へのリスクアセスメント マニュアル改訂 2023年9月



※ボーイング、エアバス社からも情報が周知されている

衛星測位システム 干渉 リスク分析

ボウタイ分析
(蝶ネクタイ分析/Bow-tie Analysis)

JAPAN AIRLINES

②ハザード(危険因子/Hazard)
・当該空域の運航

※引き金となる危険因子

①脅威(スレット Threats)
・**GPS妨害**
・**GPSなりすまし**

③トップイベント (Top event)
・航空機の航法、監視機能低下

※発生する(最初の(トップの))不安全事象

④最悪の結果(Consequences)
・**他空域に誤進入**(撃墜)
・**空中衝突**
※(上下・左右)間隔を確保せず衝突
※地上接近警報装置の偽警報により プルアップして他機と衝突
・**CFIT**((cee-fit)
(Controlled Flight Into Terrain))
※ 操縦士が気付かない内に(高地などの)地表に衝突
・**滑走路逸脱**

識別・防御バリア 十分機能せず

対応・復旧バリア 十分機能せず

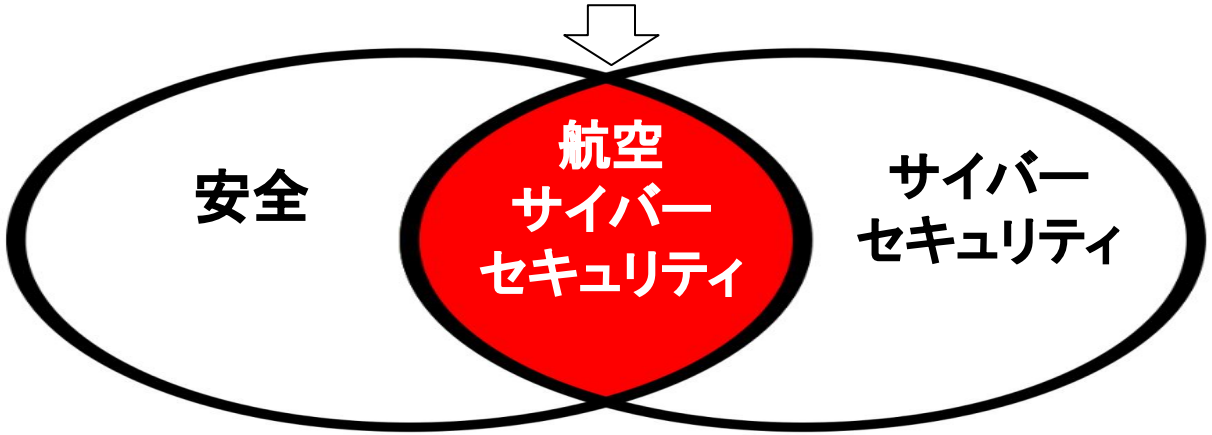
航空安全のテーマ「航空サイバーセキュリティ」

▸**「航空サイバーセキュリティ」(Aviation Cyber Security)**

衛星測位システム事例でも**「航空サイバーセキュリティ」は航空安全の課題として顕在化。**
⇒ITなど一部のチームの問題ではなく「安全問題」の領域がある

「航空サイバーセキュリティ」とは？
⇒安全とサイバーセキュリティの交差域 (赤)。

対象：航空の安全に潜在的に影響を与えるサイバーセキュリティリスク *(EU Part-ISより)*



⇒①システムは連関・接続(コネクティビティ)しており、また**②単独では脅威情報の把握・対応は困難**
⇒組織内外の横断的対応、脅威・対応法の共有が必要 (後述「4. 今後のチャレンジ」)

2.「航空サイバーセキュリティ」の必要性

航空機システムハッキングの報道　2015年

FBI: Hacker claimed to have taken over flight's engine controls

By Evan Perez, CNN

Updated 9:19 PM EDT Mon May 18, 2015

A cybersecurity consultant told the FBI he hacked into computer systems aboard airliners up to 20 times and managed to control an aircraft engine during a flight, according to federal court documents.

Chris Roberts was detained by the FBI in April following a United Airlines flight to Syracuse, New York, after officials saw Twitter posts he made discussing hacking into the plane he was traveling on.

An FBI search warrant application filed in the U.S. District Court for the Northern District of New York describes the investigation of Roberts for possible computer crimes.

https://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html

FBI: ハッカーは飛行機のエンジン制御を乗っ取ったと主張

CNNのイヴァン・ペレスによる報道

2015年5月18日月曜日午後9時19分更新

連邦裁判所の文書によると、サイバーセキュリティコンサルタントは、航空機内のコンピュータシステムに何度も侵入し、飛行中に航空機のエンジンを制御することに成功したとFBIに告白しました。

クリス・ロバーツは、ユナイテッド航空のフライトでニューヨーク州シラキュースへ向かう途中で FBIに拘束されました。当局は、彼が乗っていた飛行機に侵入することについてツイッターで投稿した内容を見て気付いたためです。

ニューヨーク北地区連邦地方裁判所に提出されたFBIの家宅捜索令状申請書には、ロバーツ氏が可能なコンピュータ犯罪の疑いで調査された事実が記載されています。

※CNNサイトから引用

IFEシステムハッキングのブログ記事

RESEARCH | DECEMBER 20, 2016

In Flight Hacking System

By Ruben Santamarta

In my five years with IOActive, I've had the opportunity to visit some awesome places, often thousands of kilometers from home. So flying has obviously been an integral part of my routine. You might not think that's such a big deal, unless like me, you're afraid of flying. I don't think I can completely get rid of that anxiety; after dozens of flights my hands still sweat during takeoff, but I've learned to live with it, even enjoying it sometimes…and spending some flights hacking stuff.

https://ioactive.com/in-flight-hacking-system/

研究 | 2016年12月20日

インフライトハッキングシステム

ルベン・サンタマルタによる

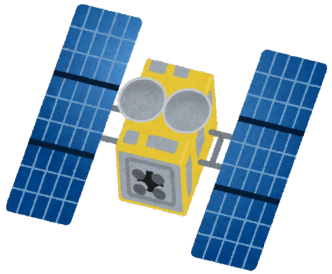
IOActiveでの5年間にわたり、私は素晴らしい場所を訪れる機会がありました。しばしば自宅から数千キロメートルも離れた場所です。飛行は私の日常の一部となってきました。あなたがそれほど大したことではないと思うかもしれませんが、私のように飛行が怖いと感じる人にとってはそうではありません。何十ものフライトを経験しても、私は離陸時に手が汗ばむのですが、それに慣れることを学びました。時にはそれを楽しむことさえあります …そして、いくつかのフライトでハッキングをしています。

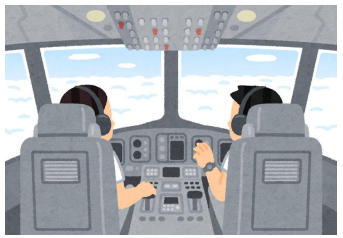
※IOActiveサイトから引用

通信のデジタル化が進む
サイバー攻撃の影響は？

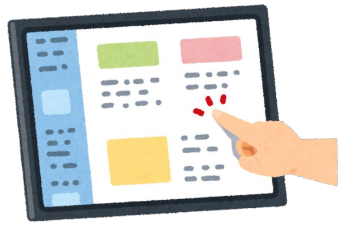
インターネット通信は
サイバー攻撃者の通り道

乗務員の端末も
インターネット接続する
リスクはないか？





セキュリティは完璧か？
（安全神話かもしれない）



システムに不具合
はつきもの
（設計ミス、設定ミス、機器故障）

航空機も
サイバー攻撃の
対象になり得る

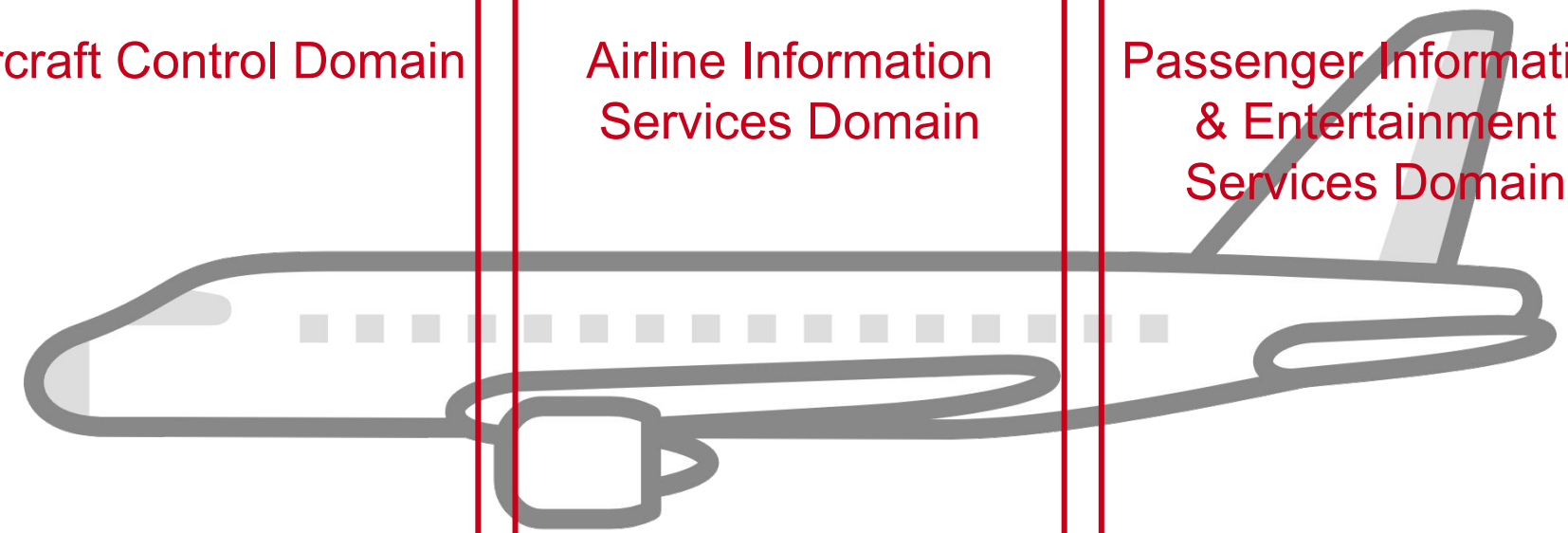
サイバー攻撃への
対応は想定済か？
対処を訓練済か？

機内には
システム多数
（IFE、機内WiFi、
電波を発する持ち
込み機器）

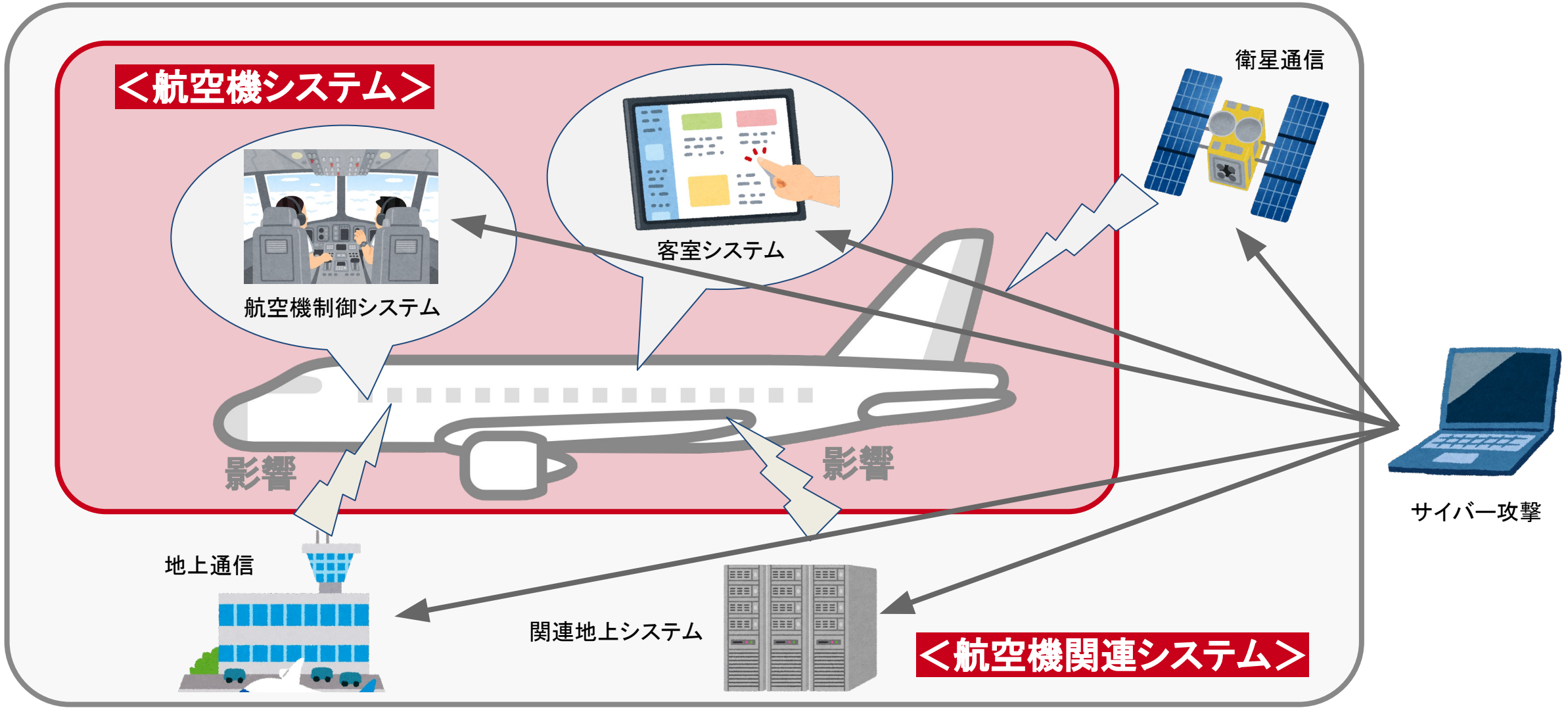
Aircraft Control Domain

Airline Information
Services Domain

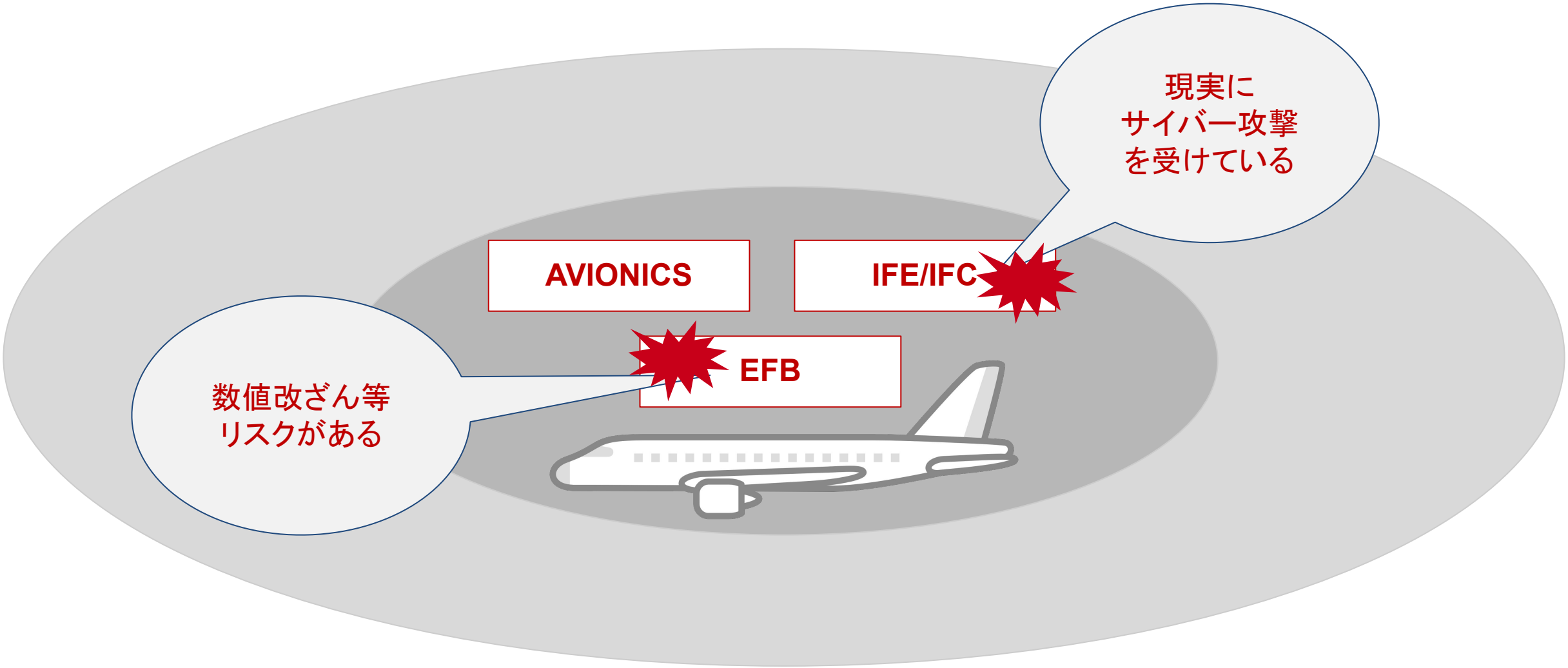
Passenger Information
& Entertainment
Services Domain



【サイバー攻撃の対象と攻撃の経路】
・サイバー攻撃の対象：航空機システムが直接的な標的になるとは限らない。
・サイバー攻撃の経路：サプライチェーンの複雑化でサイバー攻撃の経路も多様化。



【航空機やその運航に影響し得るリスク・すでに顕在化しつつあるリスク ＜一次影響＞】



【航空機やその運航に影響し得るリスク・すでに顕在化しつつあるリスク ＜二次影響＞】

JAPAN AIRLINES

SPOOFING
問題が顕在化

GPS

衛星通信攻撃
事例が発生

SATCOM

データ改ざん
事例が発生

ADS-B

プロバイダの
サイバー被害

CHART

AVIONICS

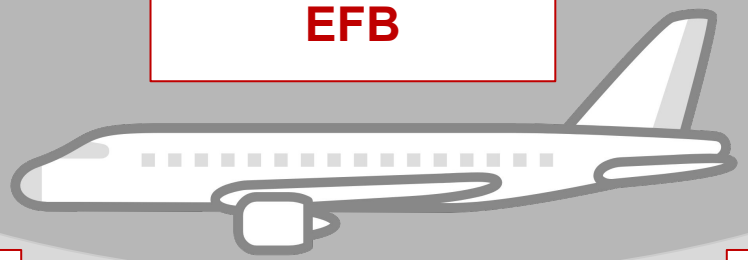
IFE/IFC

ACARS

EFB

W/B

CELLULAR



FLIGHT PLAN

MAINTENACE-PC

GATE-LINK

ウイルス感染
リスクあり

ベンダーへの
サイバー攻撃

【航空機やその運航に影響し得るリスク・すでに顕在化しつつあるリスク ＜環境面＞】

JAPAN AIRLINES

OEM

MANUFACTURER

ATC

ランサム被害
事例あり

ランサム被害
事例あり

SATCOM

GPS

ADS-B

CHART

AVIONICS

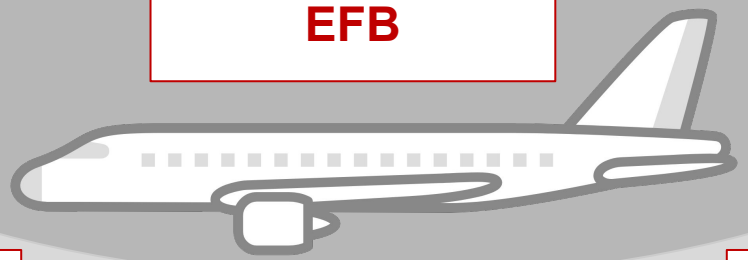
IFE/IFC

ACARS

EFB

W/B

CELLULAR



FLIGHT PLAN

GATE-LINK

MAINTENACE-PC

サイバー被害
リスク高い

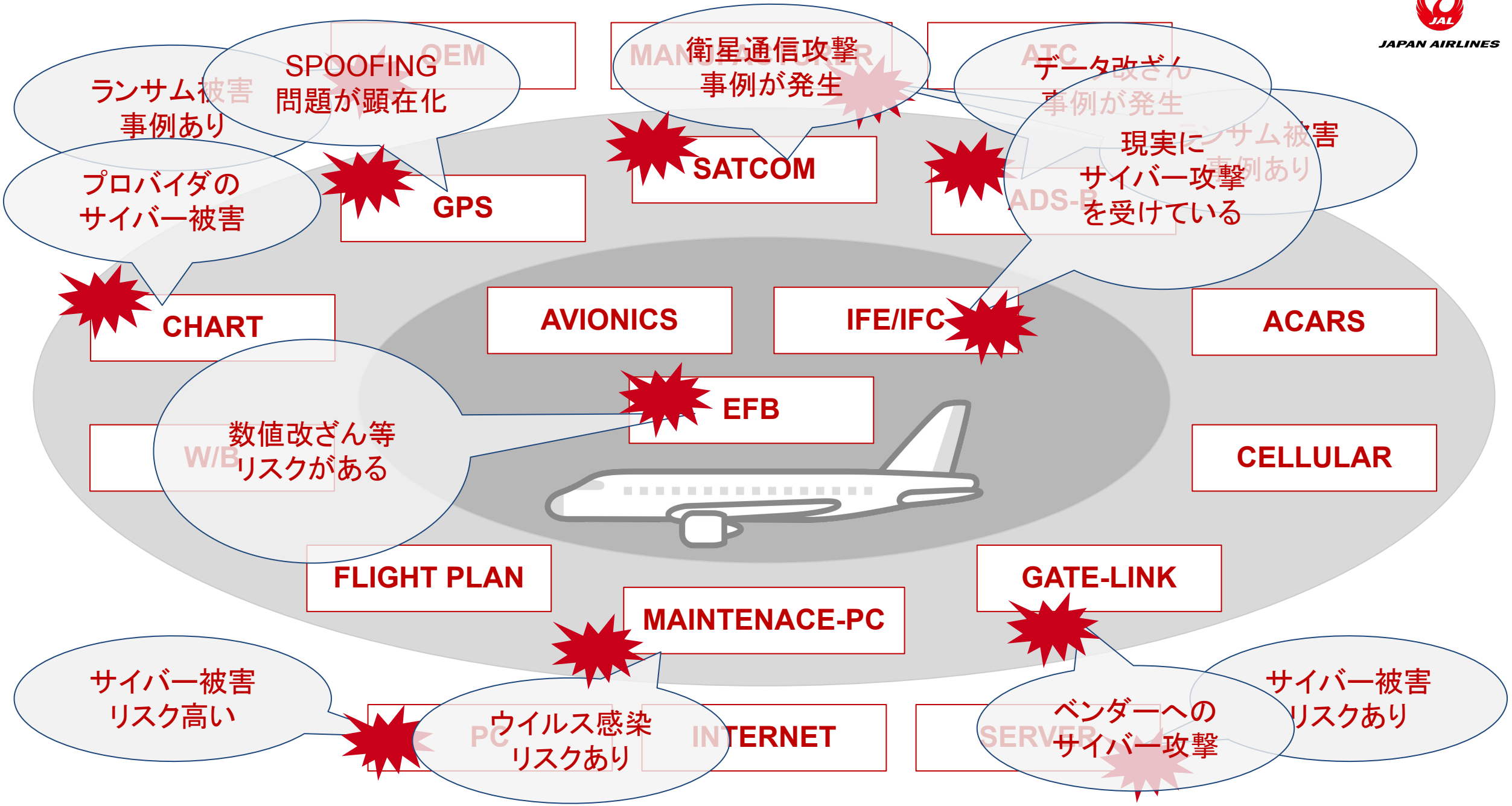
PC

INTERNET

SERVER

サイバー被害
リスクあり

【サイバーの視点でみた場合のリスク】



高まりつつある航空機に関わるサイバーのリスク

【航空機の変化（ハザード）】

- 航空機部品のソフトウェア化
- 航空機のコネクティッド化も進む
- 航空機の通信のデジタル化が加速
- 航空機のオペレーションにおけるデジタル依存度が高まり（GPS利用など）

【脅威の増大】

- 社会のあらゆる側面でデジタル技術の活用が進みサイバーの脅威が増大（航空機も標的）
- サイバーは深刻な経済被害をもたらす脅威となった（単なる迷惑行為の次元ではない）
- 病院システムをはじめ人命に関わる分野にもサイバーの被害が広がりつつある
- 航空機は「テロ」「サイバー」の両側面から標的とされる公算大

⇒リスクの顕在化を確認して対策に着手していては手遅れになる恐れがある

3.「航空サイバーセキュリティ」の進め方

国際民間航空条約 第17附属書（2017年4月有効）

4.9 Measures relating to cyber threats

4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

4.9.2 Recommendation.—Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.

4.9 サイバー脅威に関連する対策

4.9.1 各契約国は、国内の民間航空保安プログラムまたはその他の関連する国内文書で定義された運航者またはエンティティが、民間航空目的で使用される重要な情報技術および通信技術のシステムおよびデータを特定し、リスク評価に応じて、適切な対策を開発し、実施することを確保しなければなりません。これにより、これらのシステムおよびデータが違法な干渉から保護されます。

4.9.2 推奨事項 — 各契約国は、実施される対策が特定された重要なシステムおよび /またはデータの機密性、整合性、可用性を適切に保護することを確保すべきです。対策には、デザインによるセキュリティ、サプライチェーンのセキュリティ、ネットワークの分離、および適切な場合にはリモートアクセス機能の保護または制限が含まれるべきです。これは、関連する国内当局によって実施されるリスク評価に従って行われるべきです。

※具体的な対策はICAO Doc 8973の（18章）

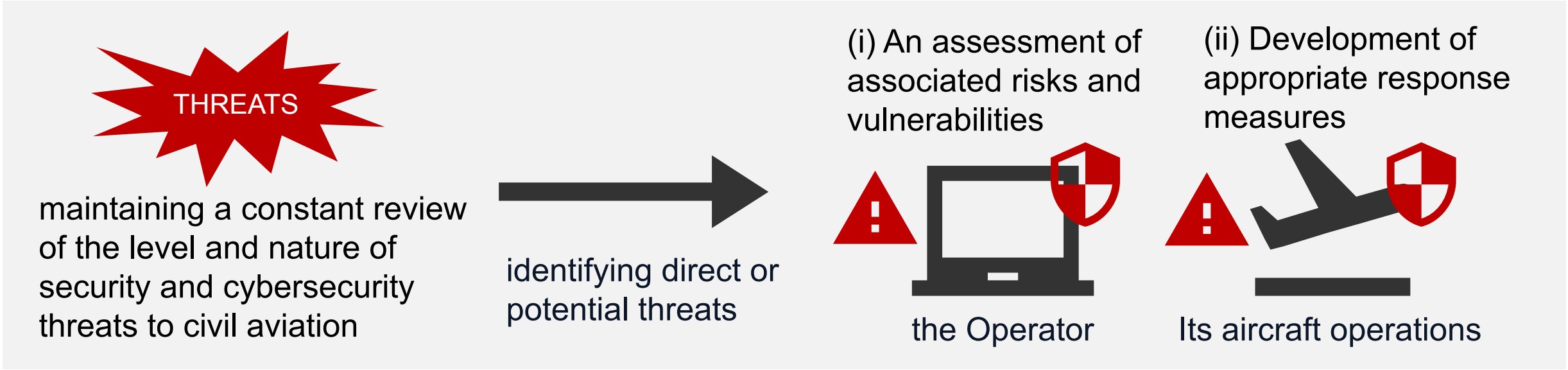
IATA安全監査要件への航空サイバーセキュリティ追加

IOSA Standards Manual Ed14/2021年9月有効 SEC4.1.1

The Operator shall have processes for maintaining a constant review of the level and nature of security and cybersecurity threats to civil aviation, and for identifying direct or potential threats against the Operator and/or its aircraft operations. For threats that have been identified, such processes shall include:

(i) An assessment of associated risks and vulnerabilities; ＜関連するリスクと脆弱性の評価＞

(ii) Development of appropriate response measures. ＜適切な対応策の構築＞



IATA安全監査要件への航空サイバーセキュリティ追加

具体的監査項目（Auditor Actions）

Identified/Assessed process(es) for monitoring level and nature of security threats to civil aviation (focus: identification of threats to operator, assessment of associated risks, development of response measures).

Interviewed responsible manager(s).

Examined methods used to monitor security threats to civil aviation. ＜脅威の監視方法＞

Examined selected records of threats identified, risk assessments and appropriate response measures. ＜観測された脅威、リスクアセスメント、対策に関する記録＞

SEC4.1.1のガイダンス（抜粋）

To ensure threat assessment remains up to date and relevant to the changing environment, an operator will have mechanisms in place that allow it to collect real-time (or close to real-time) security threat information from both open and, if possible, restricted sources. Included would be relevant information shared or provided by applicable states for the purpose of assisting the operator in (1) identifying direct or potential threats to its operations and (2) conducting effective security risk assessments.

EASA Part-IS (Information Security)

2023年2月7日のIATA発信情報（GOVAF1635）

EASA Part-IS

EASA Part-IS Implementing Regulation 2023/203 applies as of February 2026 to a wide range of stakeholders, including European Union Aviation Safety Agency (EASA) registered carriers, airports, and competent authorities. Part-IS aims to protect aviation safety against information security risks through the implementation of an information security management system including both internal and external reporting schemes. IATA is engaging with EASA to seek further Acceptable Means of Compliance (AMCs) and Guidance Material (GM) for airlines, to ensure that they are properly oriented and facilitate compliance.

EASA Part-IS

EASA Part-IS（欧州航空安全機関 Part-IS）は、2023/203号によって適用され、2026年2月から欧州航空安全機関（EASA）の登録キャリア、空港、および主管当局を含む幅広いステークホルダーに適用されます。Part-ISは、情報セキュリティリスクに対する航空の安全を保護することを目的としています。内部および外部の報告スキームを含む情報セキュリティ管理システムの実施を通じて、航空の安全が確保されることを目指しています。IATAは、航空会社に対して適切な指針とコンプライアンスを容易にするために、EASAと連携して受け入れ可能な遵守手段（AMC）およびガイダンス資料（GM）をさらに求めています。

＊EASA:European Union Aviation Safety Agency（欧州安全機関）

EASA Part-IS (Information Security)

2023年2月7日のIATA発信情報（GOVAF1635）

Actions required

In a context of the proliferation of cybersecurity rules in different parts of the world, IATA and its governance groups are committed to continuing work on standards and guidance material aimed at strengthening the implementation of airline cybersecurity management programs within IOSA (IOSA Cybersecurity for Safety, Security, and Airworthiness - CSSA), with a view to such standards potentially being considered acceptable means of compliance at some point in the future.

In the meantime, airlines are advised to assess the content of the regulations and the scope of their information security management system.

IATA GOVAF1635

必要なアクション

世界各地でサイバーセキュリティルールが増えている状況において、IATAおよびそのガバナンスグループは、IOSA内（IOSA Cybersecurity for Safety, Security, and Airworthiness - CSSA）における航空会社のサイバーセキュリティ管理プログラムの実施を強化するための標準とガイダンス資料に関する作業を継続することを約束しています。将来的には、これらの標準が将来的に適合手段として認められる可能性も考慮されています。

一方、航空会社には、規制の内容と情報セキュリティ管理システムの範囲を評価することが推奨されています。

IATA GOVAF1635

「航空サイバーセキュリティ」のフレームワーク

【既存のフレームワーク】

- 安全：SMS（Safety Management System）
- 保安：SeMS（Security Management System）
- サイバーセキュリティ：ISMS（Information Security Management System）
  - ISMSに関する国際規格：ISO27001
  - 米国のサイバーセキュリティフレームワーク：NIST* Cybersecurity Framework（CSF）

*NIST：National Institute of Standards and Technology（米国標準技術研究所）

【航空の安全を目的とするサイバーセキュリティのフレームワーク】

- 航空サイバーセキュリティ：（標準化の途上）
  - 欧州のレギュレーション：EASA* Part-IS (Information Security)

*EASA：European Union Aviation Safety Agency（欧州航空安全機関）

⇒サイバーセキュリティは、航空の安全の新たなハザードもしくは脅威

⇒航空の安全を目的とする「航空サイバーセキュリティ」の構築が急務

⇒「航空サイバーセキュリティ」を実現するためのフレームワークが必要

SMS（安全管理システム）

SMS（安全管理システム）

1. 安全方針と安全目標	①マネジメントの関与 ②安全に関わる責任と説明責任 ③安全に関わる責任者の指名 ④SMSの文書化 ⑤緊急対応計画の調整	経営の関与・責任者
2. 安全リスクマネジメント	⑥ハザードの特定 ⑦安全リスクの評価と軽減	リスク特定・評価
3. 安全保証	⑧安全性能の監視と測定 ⑨変更管理 ⑩SMSの継続的な改善	継続的改善
4. 安全の理解促進	⑪訓練および教育 ⑫安全に関するコミュニケーション	力量・周知

（出典）安全管理システム（SMM）

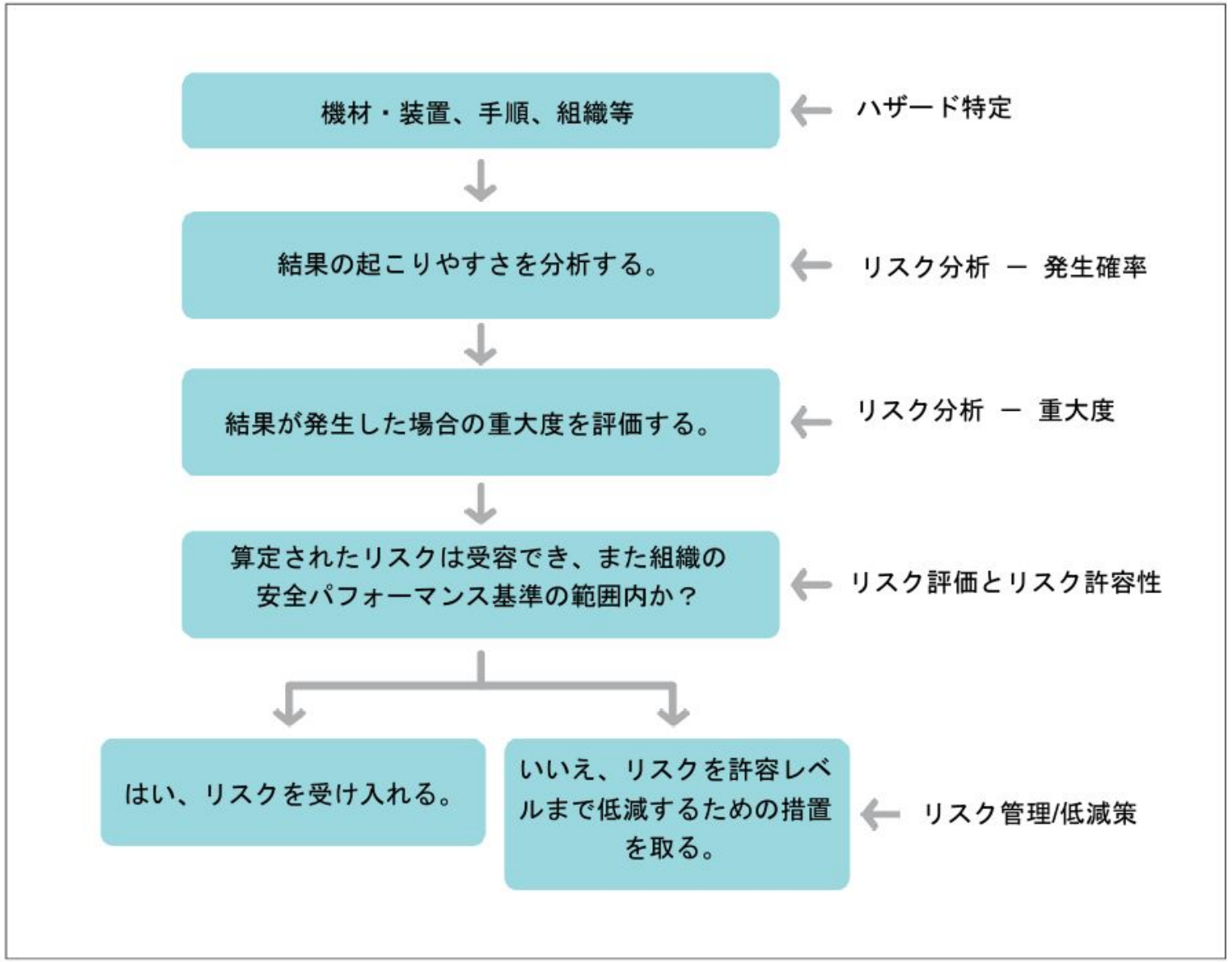


図 9-1. ハザード特定とリスクマネジメントのプロセス

リスク特定・評価

管理システムを構築する上で、リスクの特定とその評価は、もっとも重要なプロセスのひとつ

ISMS（情報セキュリティマネジメントシステム）

ISMS（情報セキュリティマネジメントシステム）（ISO27001）

4. 組織の状況	①組織及びその状況の理解、②利害関係者のニーズ及び期待の理解 ③ISMSの適用範囲の決定、④ISMSの構築（文書化）
5. リーダーシップ	①リーダーシップ及びコミットメント ②方針、③組織の役割、責任及び権限
6. 計画	①リスク及び機会に対処する活動（資産目録、リスクアセスメント） ②情報セキュリティ目的及びそれを達成するための計画策定
7. 支援	①資源、②力量、③認識、④コミュニケーション、⑤文書化した情報
8. 運用	①運用の計画及び管理 ②情報セキュリティリスクアセスメント ③情報セキュリティリスク対応
9. パフォーマンス改善	①監視、測定、分析及び評価、②内部監査、③マネジメントレビュー
10. 改善	①不適合及び是正処置、②継続的改善

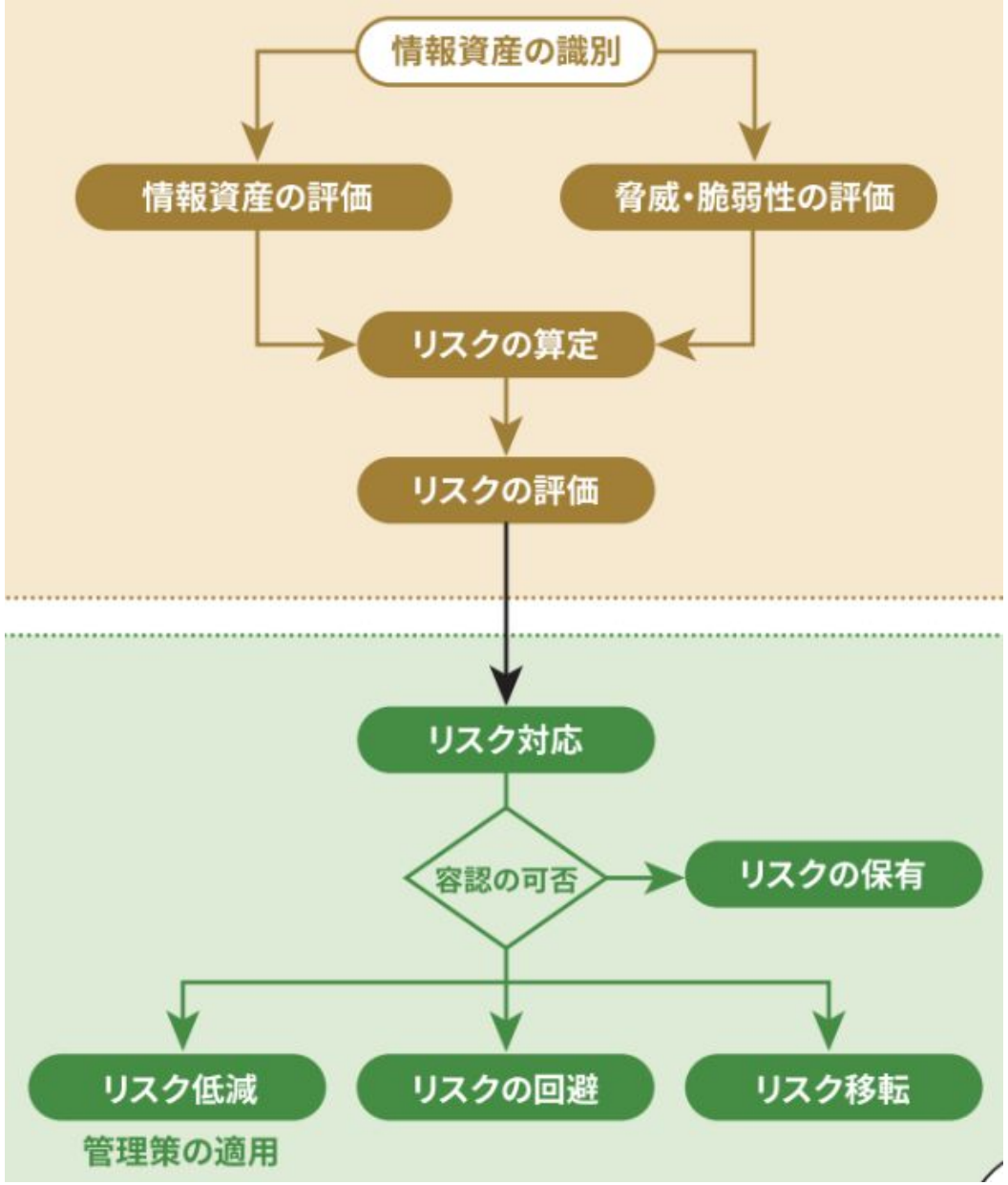
経営の関与・責任者

リスク特定・評価

力量・周知

継続的改善

（出典）ISM Web store「ISMSリスクマネジメントの流れ – ISO/IEC 27001:2022（JIS Q 27001:2023）」



リスク特定・評価

ISMSにおけるリスクは情報資産の機密性、完全性、可用性の喪失に関わる。

＜リスクの特定の例＞

1）情報資産の識別
2）情報資産の評価
3）脅威・脆弱性の評価
4）リスクの算出と評価

（出典）NIST Cybersecurity Framework

Figure 1: Framework Core Structure

NIST CSF

発生防止のバリア
（Preventive Barrier）
1）特定
2）防御

影響緩和のバリア
（Mitigative Barrier）
3）検知
4）対応
5）復旧

（出典）NIST Cybersecurity Framework

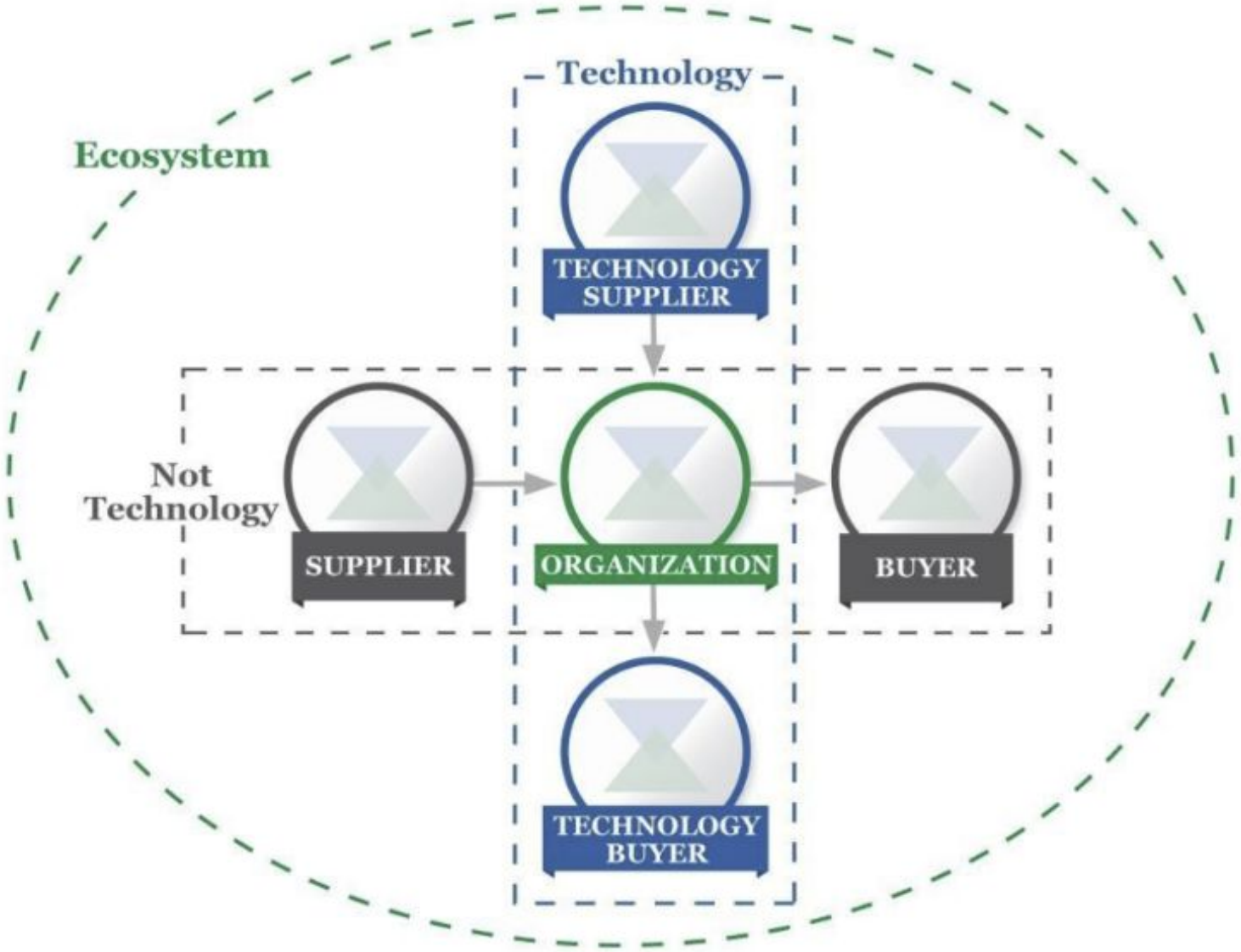


Figure 3: Cyber Supply Chain Relationships

NIST CSF

サプライチェーンリスクマネジメント（SCRM）は、組織の重要な機能のひとつとされる。

航空サイバーセキュリティ・マネジメントシステム

EASA Part-IS ＝ SMS ＋ ISMS

「航空サイバーセキュリティ」のレギュレーション

EASA Part-IS

IS.I.OR.100 スコープ
IS.I.OR.200 情報セキュリティマネジメントシステム
IS.I.OR.205 情報セキュリティリスク評価
IS.I.OR.210 情報セキュリティリスク対応
IS.I.OR.215 情報セキュリティ内部報告スキーム
IS.I.OR.220 セキュリティインシデントの検出、対処および復旧
IS.I.OR.225 関連当局より通知を受けた課題への対応
IS.I.OR.230 情報セキュリティ外部報告スキーム
IS.I.OR.235 情報セキュリティマネジメント業務の委託
IS.I.OR.240 人的資源の要件
IS.I.OR.245 記録管理
IS.I.OR.250 情報セキュリティマネジメントマニュアル
IS.I.OR.255 情報セキュリティ管理体制の変更
IS.I.OR.260 継続的な改善

経営の関与・責任者
リスク特定・評価
報告スキーム
インシデント対応
サプライチェーン
力量・周知
継続的改善

EASA Part-IS

Subject matter

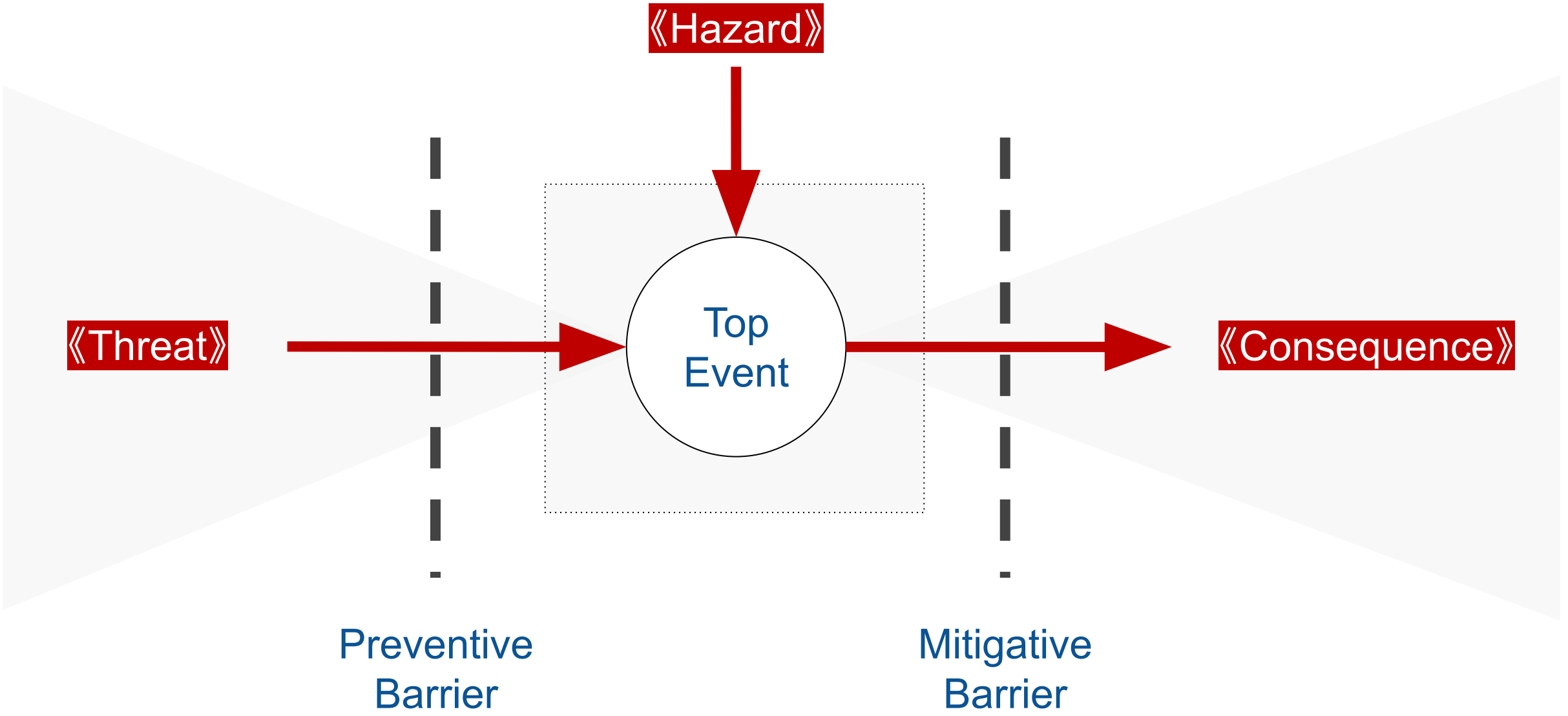
This Regulation sets out the requirements to be met by the organisations and competent authorities in order:

1) to identify and manage information security risks with potential impact on aviation safety which could affect information and communication technology systems and data used for civil aviation purposes,
2) to detect information security events and identify those which are considered information security incidents with potential impact on aviation safety,
3) to respond to, and recover from, those information security incidents.

この規制は、以下の要件を設定します。

1) 組織や適格機関は、航空安全に影響を及ぼす可能性のある情報セキュリティリスクを特定し、管理する必要があります。
2) 民間航空目的で使用される情報通信技術システムやデータに影響を与える可能性のある情報セキュリティイベントを検出し、それらを情報セキュリティインシデントとして認識する必要があります。
3) それらの情報セキュリティインシデントに対応し、回復する必要があります。

EASA Part-IS リスク分析のモデル（蝶ネクタイ分析）



EASA Part-IS 航空安全に影響を及ぼす可能性のある情報セキュリティリスク

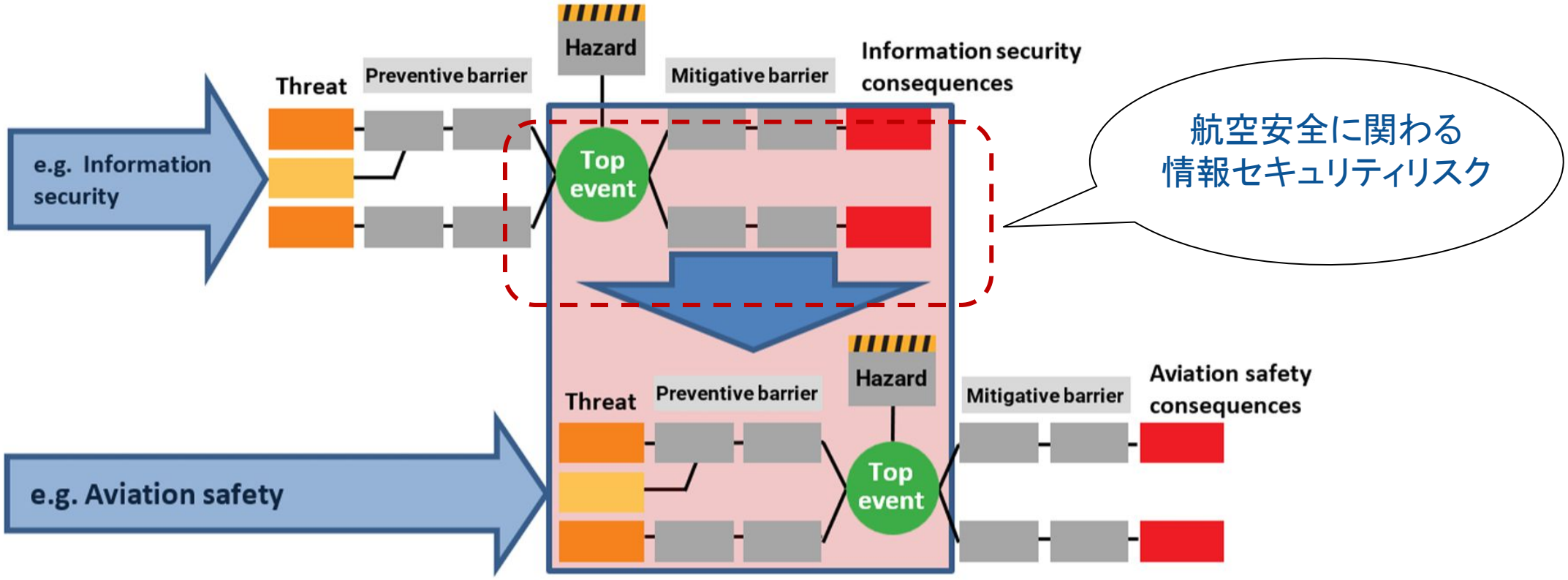


Figure 1: Bow-tie representation of management of aviation safety risks posed by information security threats

EASA Part-IS（205） リスク特定の要件

IS.I.OR.205（一部）

(a) The organisation shall identify all its elements which could be exposed to information security risks. That shall include:

(1) the organisation's **activities, facilities and resources, as well as the services** the organisation operates, provides, receives or maintains;

(2) the **equipment, systems, data and information** that contribute to the functioning of the elements listed in point (1).

(b) The organisation shall identify the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.

(a)組織は、情報セキュリティリスクにさらされる可能性のあるすべての要素を特定しなければなりません。これには以下が含まれます：

（1）組織の**活動、施設、リソース**、および組織が運営、提供、受け取り、または維持する**サービス**、

（2）要素（1）にリストされた機能に貢献する**設備、システム、データ、および情報**。

(b)組織は、他の組織とのインターフェースを特定し、相互の情報セキュリティリスクにさらされる可能性があるかを特定しなければなりません。

EASA Part-IS（205） リスク評価の例（考え方はSMSと共通）

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario — potential of occurrence	**Low safety consequences**	**Moderate safety consequences**	**High safety consequences**
High	Conditionally acceptable	**Not acceptable**	**Not acceptable**
Medium	Acceptable	Conditionally acceptable	**Not acceptable**
Low	Acceptable	Acceptable	Conditionally acceptable*

Figure 1: Example of a risk acceptance matrix for comparison purposes

EASA Part-IS（220） インシデントへの対応・復旧

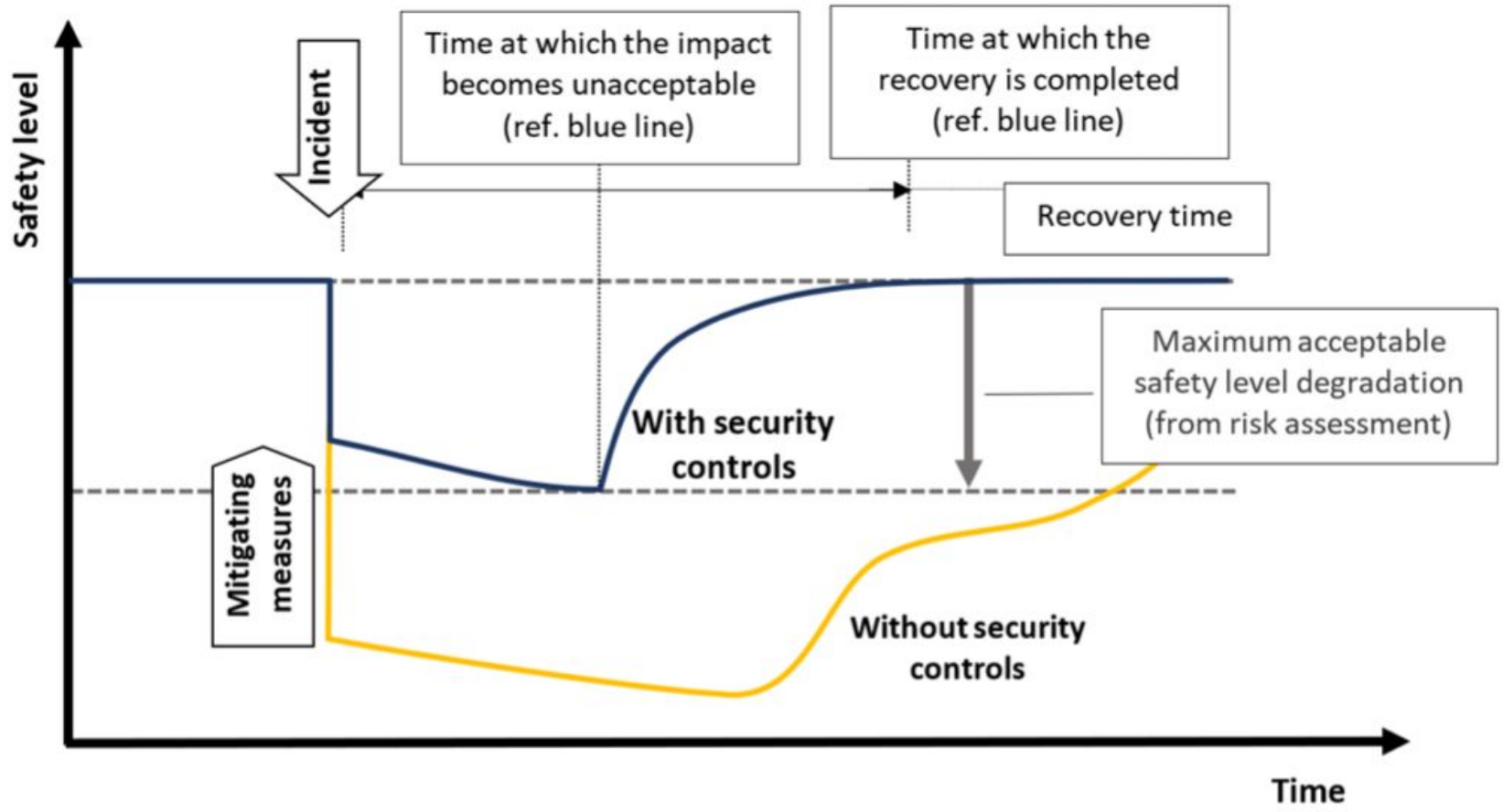
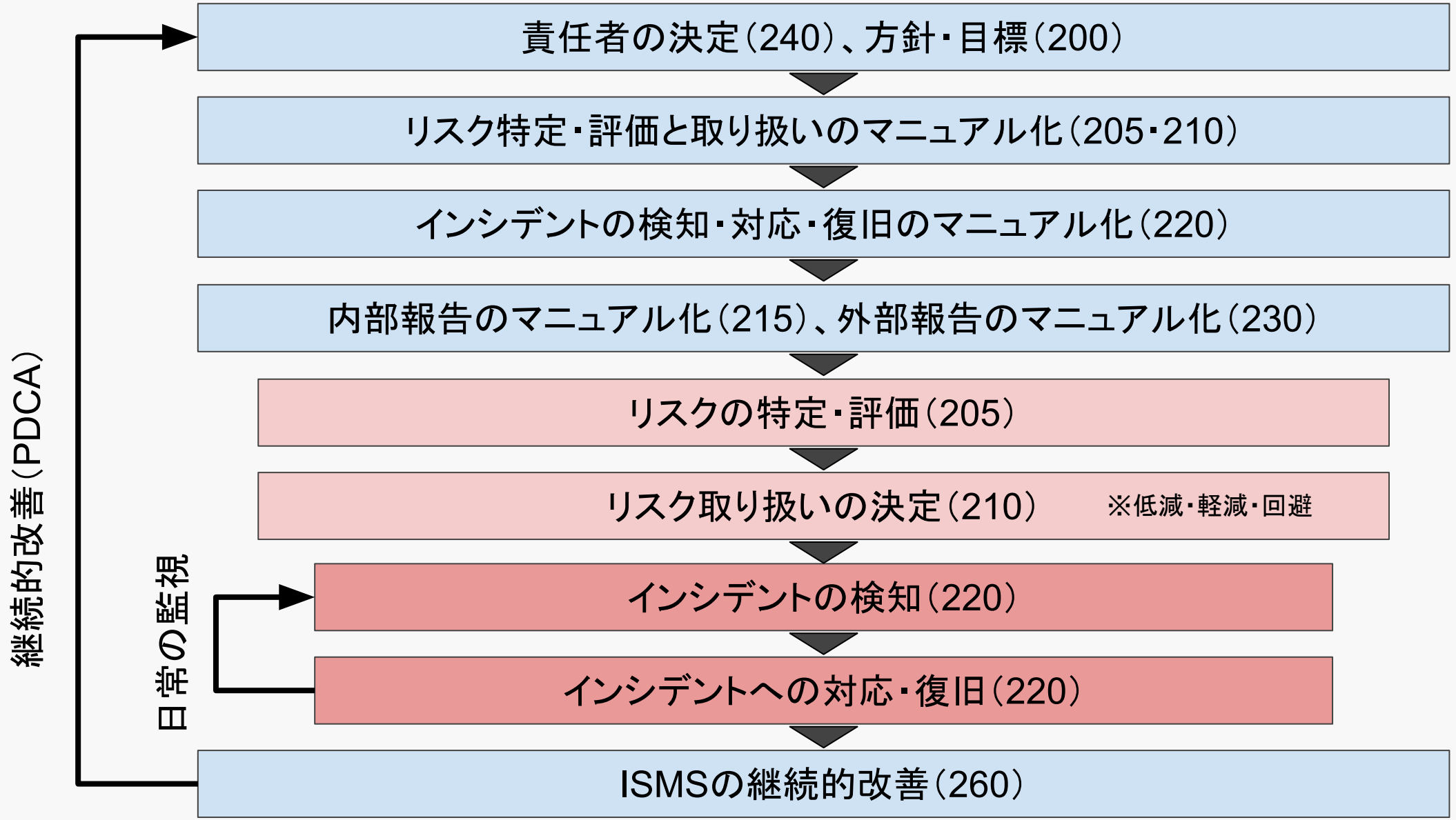


Figure 1: Conceptual framework for the definition of the response and recovery objectives

EASA Part-IS　航空サイバーセキュリティのフレームワークのアウトライン



航空会社に求められる対応

【航空機のリスク評価】
- 航空機やオペレーションのデジタル依存度の高まり（GPSなど）は新たなリスク
- 航空安全に影響するサイバーセキュリティリスクの特定と評価が急務

【「航空サイバーセキュリティ」を構築するための活動に着手】
- 「航空サイバーセキュリティ」の構築には時間を要する
- 「航空サイバーセキュリティ」のレギュレーション化を見据え、準備的取り組みの早期開始が必要
- 「航空サイバーセキュリティ」は業界共通の課題であり、官民が協力して推進する体制が必要

今後必要になると考えられる具体的な取り組み
⇒「航空サイバーセキュリティ」の体制を構築し、リスク評価や対応の検討に着手
⇒「航空サイバーセキュリティ」のリスクの監視を開始し、継続的改善に取り組む
⇒「航空サイバーセキュリティ」を官民で協力して構築する活動に着手する

4. 今後のチャレンジ

スケジュール

	2023	2024	2025	2026	2027
EU、米国、IATAの動き	●2023.7： EU Part-IS 要件適合方法発表			**●2026.2： EU Part-IS EU籍航空会社義務化**	
	■2023.3： 米国TSAが基本要件発表※				
		◎2024.2(?)：IATA 安全監査(IOSA) 要件原案			**◎2027.1(?)：IATA 安全監査(IOSA)要件化** ※Part-ISがベース

※**米国TSA**(Transportation Security Administration・運輸保安庁) は基本要件発表。
(石油パイプライン、鉄道から対応を着手しており、要件が明確化の時期は未定)
https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

※**JAL**では事務局を安全推進本部、事務局補佐をIT企画本部で毎月勉強会を開始。

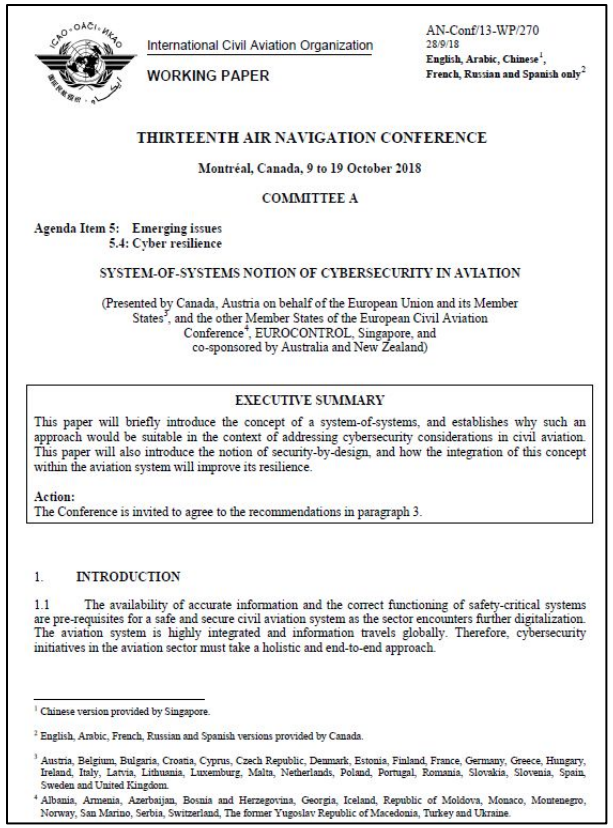
ICAO: 航空は「複数システムの全体システム」

航空の「システムのシステム(SoS)」サイバーセキュリティー概念 2018年

‘System-Of-Systems(SoS) cybersecurity notion in aviation’

⇒サイバーセキュリティ上各々のシステムを護る必要

ICAO:International Civil Aviation Organization(国際民間航空機関)
ワーキングペーパー



International Civil Aviation Organization

WORKING PAPER

AN-Conf/13-WP/270
28/9/18
English, Arabic, Chinese[1], French, Russian and Spanish only[2]

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

SYSTEM-OF-SYSTEMS NOTION OF CYBERSECURITY IN AVIATION

(Presented by Canada, Austria on behalf of the European Union and its Member States[3], and the other Member States of the European Civil Aviation Conference[4], EUROCONTROL, Singapore, and co-sponsored by Australia and New Zealand)

EXECUTIVE SUMMARY

This paper will briefly introduce the concept of a system-of-systems, and establishes why such an approach would be suitable in the context of addressing cybersecurity considerations in civil aviation. This paper will also introduce the notion of security-by-design, and how the integration of this concept within the aviation system will improve its resilience.

Action:
The Conference is invited to agree to the recommendations in paragraph 3.

1. INTRODUCTION

1.1 The availability of accurate information and the correct functioning of safety-critical systems are pre-requisites for a safe and secure civil aviation system as the sector encounters further digitalization. The aviation system is highly integrated and information travels globally. Therefore, cybersecurity initiatives in the aviation sector must take a holistic and end-to-end approach.

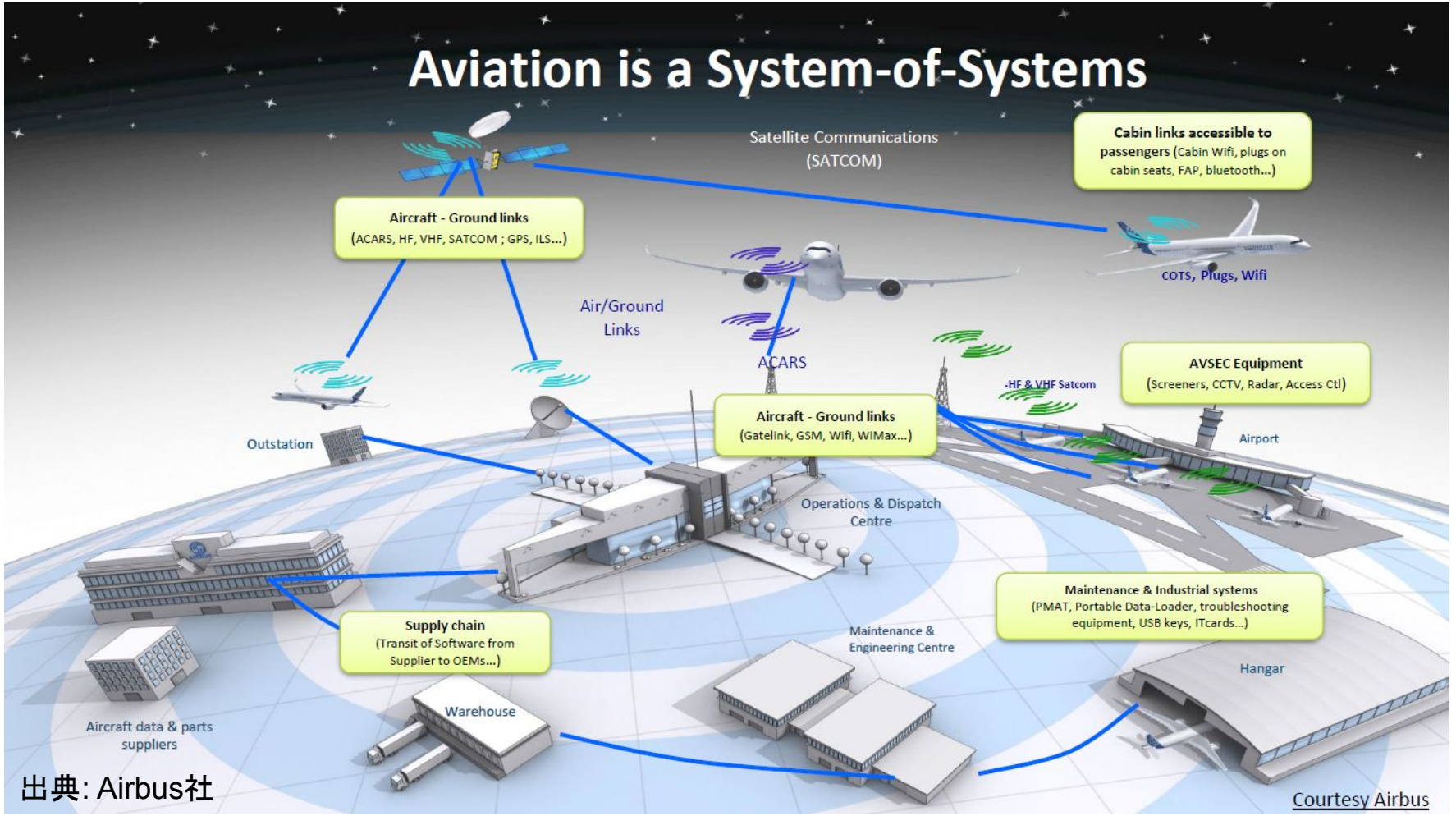
[1] Chinese version provided by Singapore.

[2] English, Arabic, French, Russian and Spanish versions provided by Canada.

[3] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[4] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

https://www.icao.int/Meetings/anconf13/Documents/WP/wp_270_en.pdf



出典: Airbus社

今後のチャレンジ①

「航空サイバーセキュリティ」は航空安全の大きなテーマです。
**　航空システムは複数システムの統合体です。**
<u>1) 本邦でも、航空安全の観点から国も関与して、製造者、整備、航空事業者、管制、空港等を含めた航空システム全体の安全を護るためのサイバーリスク品質管理体制の整備が望まれます。</u>

※**欧州のPart-IS(Information Security)**のレギュレーションでは、製造段階から、整備、空港、管制、運航者、訓練組織等に**品質管理体制**の整備を各々求めており、航空全体での体制確立を目指しています。

*FSTD:Flight Simulation Training Devices

出典:Swiss Aviation Safety and Operations Conference SASOC 2022・EASA Part-IS 資料一部改変

今後のチャレンジ②

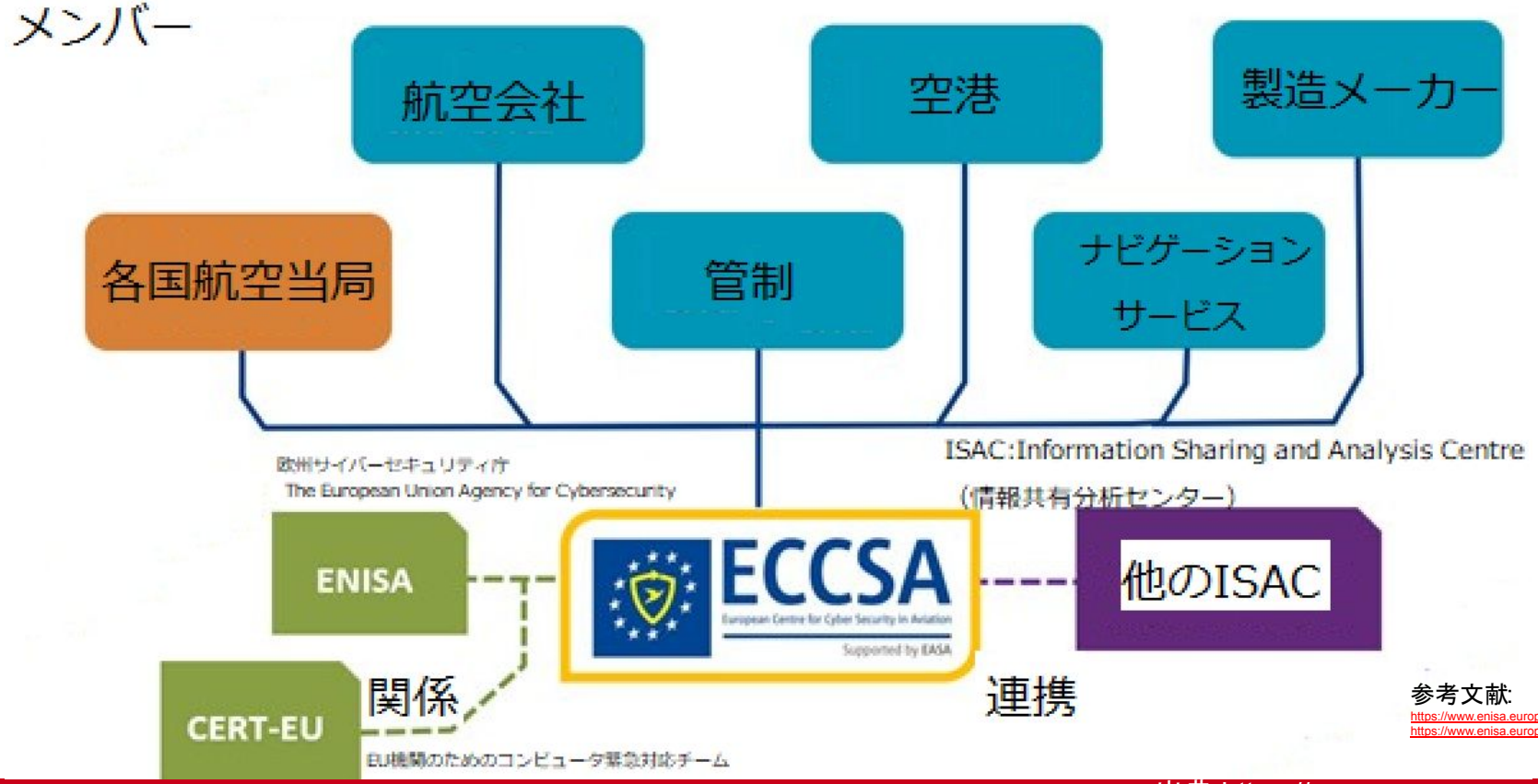
「航空サイバーセキュリティ」は航空安全の大きなテーマです。

<u>2) 単独では脅威情報の把握・対応は困難なため、本邦でも知見の共有の枠組み整備が望まれます</u>。

※参考: クレジットカード業界：クレジットカード番号漏洩の検知や不正検知のルールなどを共有。

※欧州では航空サイバーセキュリティに特化した情報共有分析センターが設立済。

ECCSA (European Centre for Cybersecurity in Aviation) 2017年設立



参考文献:
https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models
https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

出典 https://www.easa.europa.eu/en/eccsa を日本語化

「航空サイバーセキュリティ」は航空安全の大きなテーマです。
ご助力をお願いいたします。