令和２年度内外一体の経済成長戦略構築にかかる国際経済調査事業
（民間航空機サイバーセキュリティのルール形成
（国際標準化含む）戦略に係る調査研究）

調査報告書

令和３年３月

株式会社ＩＨＩ
航空・宇宙・防衛事業領域
技術開発センター

目　　次

第１章　調査目的

近年、自動車を中心として、モビリティにおけるコネクテッド化が進む中、外部からのサイバー攻撃への対応等、走行の安全性を確保するセキュリティに係る開発や指標の整備が進んでいる。航空機の世界でも、２０３０年代にはハイブリッド電動航空機の市場投入が見込まれており、こうした電動航空機の研究開発競争と併行して、サイバーセキュリティの議論が加速しつつある。

日本企業の電動化技術は、欧米の機体・エンジンメーカから大きく期待を寄せられている。経済産業省では、２０１９年１月に日本とボーイングの間において将来航空機の技術開発にかかる協力覚書(注1)を締結しており、協力分野の一つとして電動化技術が上げられていることからも、瞭然である。

他方、こうした技術開発と両輪で、ルール形成の領域にも注力していくことが肝要であり、特に電動航空機はこれまでの航空機とは全く異なる推進構造やシステム構造となることが想定されていることから、機体の安全性の証明にあたっても新たな基準が必要である。特に昨今、こうした技術面での安全性証明に加え、欧米規制当局からサイバーセキュリティへの関心が高まっている。

こと航空機における特有事項として、部品点数が約１００万点と自動車の１０倍以上の数で構成されており、システムが上位システムと連携する複雑なサイバー環境が議論される点、故障したら止まるではなく故障しても動き続けなければならないという設計思想の下、多重的なセキュリティ設計が求められる点が挙げられる。また最終的には、ＦＡＡ／ＥＡＳＡ等の欧米規制当局から認証を得る必要があり、機体の安全証明ノウハウをその初期から当局との間で議論しなければ、従来のように認証に於けるノウハウが欧米寡占状態されることとなる。こうした状況を防ぐためにも、ルール形成の検討初期段階から議論に関与しておくことが重要と考えられる。

実際、世界に目を向けると、ＳＡＥ、ＲＴＣＡ、ＥＵＲＯＣＡＥといった民間標準化団体を主戦場として、航空機メーカ、電機メーカ、ＦＡＡ／ＥＡＳＡ等の各国規制当局によって既に活発な議論が開始されている。民間標準化団体にて形成された種々の規格は、各国規制当局によって準用されるケースが多く、我が国としてもこうした取組状況を確実に把握し、議論に参加する体制を作り上げて行くことが急務である。

そこで本事業では、特に電動航空機におけるサイバーセキュリティの議論に着目し、国際標準化団体におけるサイバーセキュリティのルール形成動向を把握する。中長期的には、日本企業がそうした議論の場に於いて関与・リードできる領域を特定し、働きかけを開始したい。具体的には、A.主にＳＡＥ、ＲＴＣＡ、ＥＵＲＯＣＡＥ内の各コミッティで進む航空機サイバーセキュリティに係るルール形成動向、また国内での規程やガイドラインの現状を把握するとともに、B.日本の企業等がＳＡＥ、ＲＴＣＡ、ＥＵＲＯＣＡＥ等の場におけるルールづくりの段階から関与できる可能性のあるセキュリティ項目を特定し、我が国として国際ルール形成の場に臨むためのプロトタイプモデルを検討する。

また国内での産業サイバーセキュリティに関する取組ついては、経済産業省が、サプライチ

ェーン全体でのセキュリティ確保に向け、２０１９年４月に「サイバー・フィジカル・セキュリティ対策フレームワーク（ＣＰＳＦ）」[注2]を策定しており、こうした取組を参照しながら、将来的な連携も視野に調査を実施する。

注１：https://www.meti.go.jp/press/2018/01/20190115007/20190115007.html
注２：https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

第２章　調査内容および実施方法

２．１　ＳＡＥ、ＲＴＣＡ、ＥＵＲＯＣＡＥにおける標準化動向調査

２．１．１　調査内容

電動航空機におけるサイバーセキュリティの基準形成の動向について、規格標準化団体であるＳＡＥ、ＲＴＣＡ、ＥＵＲＯＣＡＥを中心とした動向調査を実施する。特に重要なコミッティとして、以下のコミッティにおける最新動向を整理する。

ＳＡＥ	Ｇ－３２	Ｃｙｂｅｒ　Ｐｈｙｓｉｃａｌ　Ｓｙｓｔｅｍｓ　Ｓｅｃｕｒｉｔｙ
ＲＴＣＡ	ＳＣ－２１６	Ａｅｒｏｎａｕｔｉｃａｌ　Ｓｙｓｔｅｍｓ　Ｓｅｃｕｒｉｔｙ
ＥＵＲＯＣＡＥ	ＷＧ－７２	Ａｅｒｏｎａｕｔｉｃａｌ　Ｓｙｓｔｅｍｓ　Ｓｅｃｕｒｉｔｙ

２．１．２　実施方法

各規格標準化団体のＷＥＢサイトに記載される情報から動向を調査するとともに、参加可能なコミッティには参加して情報収集を行い、得られた情報を元に最新動向を整理する。

２．２　国内における電動航空機に関連するサイバーセキュリティ規格の動向調査

２．２．１　調査内容

国内での電動航空機に関連するサイバーセキュリティ基準形成の動向について、経済産業省の策定した「サイバー・フィジカル・セキュリティ対策フレームワーク（ＣＰＳＦ）」を中心に整理を実施する。

２．２．２　実施方法

ＣＰＳＦの内容を確認すると共に、ＲＴＣＡの発行したドキュメント（ＤＯ－３２６Ａ、ＤＯ－３５５Ａ，ＤＯ－３５６Ａ）とＣＰＳＦの比較を行い、差分を抽出する。

２．３　日本のポテンシャル調査

２．３．１　調査内容

２．１項および２．２項の結果を踏まえ、航空業界において議論が必要な分野を抽出する。その上で、国際標準化の議論のトレンドから日本企業が議論の段階から参画可能性のあるセキュリティ分野を特定する。

２．３．２　実施方法

２．１項および２．２項の調査結果を用いてＪＡＸＡ等と意見交換を行ったうえで、議論が必要な分野の抽出と、来年度以降に日本が国際標準化団体へ参画できる可能性のあるセキュリティ分野を洗い出す。

２．４　電動航空機のサイバーセキュリティに関する国際標準化戦略

２．４．１　調査内容

２．１項～２．３項を踏まえ、電動航空機の分野の国際標準化の動きに日本が関与するための戦略を検討し、報告書にまとめる。戦略立案の中では、国内業界団体との連携方法や、規制当局との関係構築強化の要否を含め、検討する。

加えて、「サイバー・フィジカル・セキュリティ対策フレームワーク（ＣＰＳＦ）」も参考に、国内航空産業サプライチェーン全体でのセキュリティ確保に向けたセキュリティ対策等の整理を実施する。

２．４．２　実施方法

２．１項～２．３項の結果を用いて、電動航空機のサイバーセキュリティ分野における標準化戦略をまとめる。加えて、将来の電動航空機を想定したシステムを対象にセキュリティ確保について整理する。整理においてはＣＰＳＦで推奨されているフレームワークを用いた整理を行う。

第３章　調査結果

３．１　ＳＡＥ、ＲＴＣＡ、ＥＵＲＯＣＡＥにおける標準化動向調査

３．１．１　ＳＡＥ　Ｇ－３２

３．１．１．１　コミッティ概要

ＳＡＥ　Ｉｎｔｅｒｎａｔｉｏｎａｌは、航空宇宙、自動車、商用車業界の１２８，０００人を超えるエンジニアと関連する技術専門家で構成されるグローバルな協会である(注1)。ＳＡＥ　Ｉｎｔｅｒｎａｔｉｏｎａｌの規格は、世界中のモビリティエンジニアリングを進歩させるために使用され，ＳＡＥで開発される技術標準は、航空宇宙、自動車、商用車などのモビリティ業界に対する組織の重要な規定の１つである。現在，ＳＡＥには約１０，０００のドキュメントがあり，４５０を超える小委員会とタスクグループを含む２４０を超えるＳＡＥ技術委員会で構成される。標準化の作業は、９，０００人を超えるエンジニア、および世界中の他の資格のある専門家のボランティアの努力によって承認、改訂、および保守されている(注2)。

航空宇宙関連の標準規格の開発において、図３．１．１．１－１に示すコミッティが存在しており、それぞれの分野における標準規格の作成、改訂を行っている。Ｇ－３２はＣｙｂｅｒ　Ｐｈｙｓｉｃａｌ　Ｓｙｓｔｅｍｓ　Ｓｅｃｕｒｉｔｙに関する規格の作成を担当している。

注１：ＳＡＥウェブサイト（https://www.sae.org/about）
注２：ＳＡＥ標準化ウェブサイト（https://www.sae.org/servlets/works/）

３．１．１．２　ＷＥＢサイトから入手した情報

ＳＡＥ　Ｇ－３２は以下に示すＷＥＢサイトで検討状況等を確認することが可能で、現在は表３．１．１．２－１に示す３文書について検討を行っている。

https://www.sae.org/servlets/works/committeeHome.do?comtID=TEAG32

３．１．１．３　会合に参加して入手した情報

それぞれの文書に対して週１時間の会合（ＳｗＡは週２日）を行い、記載内容に対する議論を行っている。１０月下旬からＧ－３２に参加し、議論内容の聞き取りを開始した。表３．１．１．３－１～表３．１．１．３－３に参加時の議論内容を示す。

ＪＡ７４９６（ＣＰＳＳＥＰ）は本調査事業中に文書作成が完了し、１／１９～２／１５の期間において投票が行われたが否決された。現在は，投票期間中に受けた２００件を超えるコメントに対して文書への反映内容を検討している。

ＪＡ６６７８（ＳｗＡ）は表３．１．１．３－２に示すとおり、２０２１年末までに文書完成を目指し、２０２２年に発行される計画であるが、ＪＡ６８０１（ＨｗＡ）は調査期間中に発行までのスケジュールに関する情報は入手できなかった。

３．１．２　ＲＴＣＡ　ＳＣ－２１６

３．１．２．１　コミッティ概要

ＲＴＣＡは、１９３５年に航空無線技術委員会として設立された非営利の民間団体である。ますますグローバル化する企業における重要な航空近代化の問題について、多様で競合する利害関係者の間でコンセンサスを構築するための最高の官民パートナーシップの場を設け，変化する世界の航空環境に対応し、航空エコシステムの安全性、セキュリティ、および全体的な健全性を確保する標準の作成と実装を目指している(注1)。

ＳＣ－２１６は２００７年６月に設立され、耐空性セキュリティの方法と考慮事項を開発している。ＳＣ－２１６ではＤＯ－３５６とＥＵＲＯＣＡＥのＥＤ－２０３内の特定の記述を合致させることを目指している(注2)。

注１：ＲＴＣＡウェブサイト（https://www.rtca.org/about/）

注２：ＳＣ－２１６ウェブサイト（https://www.rtca.org/sc-216/）

３．１．２．２　ＷＥＢサイトから入手した情報

ＳＣ－２１６では、表３．１．２．２－１に示す３文書の発行が完了している。また、これら以外の文書の改訂をＥＵＲＯＣＡＥと合同で行っている。２０２０／９に実施された合同会議の議事録がＷＥＢに公開(注1)されており、その議事録の内容を表３．１．２．２－２に示す。

注１：https://www.rtca.org/wp-content/uploads/2020/09/WG-72_SC-216_Plenary-18-September-2020-Minutes-v1-0.pdf

３．１．２．３　会合に参加して入手した情報

ＲＴＣＡ　ＳＣ－２１６のＷＥＢサイトには、次回会合のＡｇｅｎｄａが掲載されており、そのＡｇｅｎｄａにはリモート会議用のＷｅｂＥｘのリンクも貼られている。リンクから会合へ参加した。

会合内容は、月曜および火曜がＥＤ－２０１Ａ(注1)を検討しているサブグループＳＧ４の会合、水曜および木曜がＥＤ－ＩＳＥＭ(注1)を検討しているサブグループＳＧ３の会合、金曜が全体会議であり、月水金に参加した。表３．１．２．３－１に各会合での議論内容を示す。

注１：表３．１．３．２－１参照

３．１．３　ＥＵＲＯＣＡＥ　ＷＧ－７２

３．１．３．１　コミッティ概要

ＥＵＲＯＣＡＥ（Ｅｕｒｏｐｅａｎ　Ｏｒｇａｎｉｚａｔｉｏｎ　ｆｏｒ　Ｃｉｖｉｌ　Ａｖｉａｔｉｏｎ　Ｅｑｕｉｐｍｅｎｔ：欧州民間航空機器機構）は、世界的に認められた航空業界標準の開発におけるヨーロッパのリーダーであり，業界のニーズに応じて、業界/メンバごとに次のような標準を開発している。

・メンバの最先端の専門知識に基づいて構築し、世界的な航空の課題に対応
・国際的に採用される目的に適合
・運用、開発、規制のプロセスをサポート

ＷＧ－７２はＡｅｒｏｎａｕｔｉｃａｌ　Ｓｙｓｔｅｍｓ　Ｓｅｃｕｒｉｔｙという名称で、サイバーセキュリティに関する標準化を行っているコミュニティである(注2)。

注１：https://www.eurocae.net/

注２：https://www.eurocae.net/news/posts/2018/june/eurocae-wg-72-aeronautical-systems-security-three-calls-for-participation/

３．１．３．２　ＷＥＢサイトから入手した情報

ＥＵＲＯＣＡＥ　ＷＧ－７２では、現在、表３．１．３．２－１に示す５つの文書を改訂，発行に向けて検討している。

３．１．３．３　会合に参加して入手した情報

ＥＵＲＯＣＡＥはＲＴＣＡと合同で規格の検討を行っており、 その内容は３．１．２．３項参照。

３．２　国内における電動航空機に関連するサイバーセキュリティ規格の動向調査

３．２．１　サイバー・フィジカル・セキュリティ対策フレームワーク（ＣＰＳＦ）とＲＴＣＡ文書との差分抽出

経産省により制定されたＣＰＳＦは、ＮＩＳＴ(注1)のＣＳＦ(注2)を参考に作成されており，セキュリティ対策に重点を置いてセキュリティ種別ごとに対策方法をまとめた文書である。一方、ＤＯ－３２６Ａ／３５５Ａ／３５６Ａは、開発や継続的な保守・運用等のプロセスに応じて実施すべき活動（ベストプラクティス）をまとめた文書である。本調査により両文書を比較した結果の概要を図３．２．１－１に示す。図３．２．１－１に示すように，単純に両文書を比較しただけでは，ＣＰＳＦの多くの項目が網羅されていないことが判明した。

図３．２．１－１を元に，ＣＰＳＦの要件カテゴリに含まれる要件のうち，ＤＯ－３２６Ａ／３５５Ａ／３５６Ａの要件が一つでも割り当たった要件の割合を集計した内容を表３．２．２－２に示す。これより，ＲＴＣＡ文書の記載が少ない要件カテゴリは，以下である。

・ＣＰＳ．ＢＥ（ビジネス環境）
・ＣＰＳ．ＳＣ（サプライチェーンリスク管理）
・ＣＰＳ．ＲＰ（対応計画）
・ＣＰＳ．ＣＯ（伝達）

ＣＰＳＦとＲＴＣＡの文書は，それぞれ，対象，用途が異なる文書であるため，多くの項目

が抽出されたものと考える。さらに，本調査によりＲＴＣＡ文書では他の多くの文書を参照していることが判明しており(注 3)，ＣＰＳＦとＲＴＣＡドキュメントの差分から日本が参画可能性のあるセキュリティ分野を抽出するためには，これら参照されている文書の内容確認も必要であることに加えて，現在ＳＡＥおよびＲＴＣＡで改訂，発行を検討している文書についても確認する必要がある。ただし，３．１項の動向調査結果を参考に，それぞれの文書に記載される内容を想定し，以下の項目に差分があると想定した。図３．２．１－２に推定も含めた差分調査結果の概要を示す。

これらから、サプライチェーンに対するリスクへの対応、具体的には、調達元・調達先がそれぞれ実施すべきセキュリティ管理やセキュリティプロセスについての言及がＲＴＣＡ／ＳＡＥ文書には少ないと想定される。また、ＰＳＩＲＴ(注 4)，ＣＳＩＲＴ(注 5)，ＳＯＣ(注 6)といった組織的なセキュリティに関する記述がないと想定される。

注１：National Institute of Standards and Technology：米国国立標準技術研究所
注２：NIST Cybersecurity Framework：ＮＩＳＴの提唱するサイバーセキュリティフレームワーク
注３：表３．２．１－２参照
注４：Product Security Incident Response Team：自社製品の脆弱性に対するリスクに対応する組織
注５：Computer Security Incident Response Team：コンピュータやネットワーク上でセキュリティに関する問題が起きてないか監視すると共に，問題発生時には原因解析や影響範囲の調査を行う組織
注６：Security Operation Center：サイバー攻撃の検出や分析を行い，的確なアドバイスを提供する役割を持つ部門や専門組織

３．３　日本のポテンシャル調査

３．３．１　日本が参画可能性のあるセキュリティ分野

自動車業界においては，日本の自動車メーカは電動車両や自動運転車両の開発を手掛けるだけでなく，サービス提供，保守・運用等全般にわたって主導的な立場をとっている。そのため，国際的な規格の標準化や認証においても主導権をとれるよう積極的な活動を行っている。これに対して航空機産業では，規格の標準化はＳＡＥ，ＲＴＣＡ，ＥＵＲＯＣＡＥと言った欧米の標準化団体が主導しており，日本の企業は標準化活動には十分に参画できていない。航空機の部品開発を担当する場合においては上位システムを担当するメーカから提示される要求を満足するよう開発を行えばよいが，航空機電動化に際し航空機開発へシステムでの参画を目指すためには、航空機全体でのシステムの理解が必要である。

将来の航空機のネットワークとして，３．４．１．４項に示すように機内ネットワークを統合したｅ－Ｅｎａｂｌｅｄ航空機が提唱されている。本調査ではＣＰＳＦが推奨するフレームワークを用いてｅ－Ｅｎａｂｌｅｄ航空機のモデル化を行った（３．４．４項参照)。日本が参画可能なセキュリティ分野の抽出方法として，まずはこのモデルをたたき台として国内の意見集約を行い，システムおよびセキュリティリスク等をブラッシュアップした上で，欧米の機体完成機メーカとも意見交換を行い，日本が参画可能な機器やシステムを模索していく方法が考えられる。

３．２．１項に示すとおり，今回のＣＰＳＦとＲＴＣＡ文書の比較ではサプライチェーンや組織的なセキュリティが，日本の参画可能性のあるセキュリティ分野と推定したが，この調査結果を確実なものにするためにも、上記のような欧米の機体完成機メーカとの意見交換により，課題，対応策の提案を繰り返し，日本が参画可能な機器やシステムの模索を行うと同時に標準化活動へも入り込めるセキュリティ分野を模索していくのが良いと考える。

３．３．２　国内業界団体との連携

国内業界団体として，航空機電動化に向けて活動を実施しており，サイバーセキュリティに関して連携できる団体としてＪＡＸＡの航空機電動化（ＥＣＬＡＩＲ）コンソーシアムを連携先として選択した。

３．３．２．１　ＪＡＸＡ　航空機電動化（ＥＣＬＡＩＲ）コンソーシアム

ＥＣＬＡＩＲコンソーシアムと今後の進め方について議論し，航空機の電動化が進むことで，ネットワークに接続される機器が増え，セキュリティリスクが増大する。よって，航空機電動化を進める上でサイバーセキュリティへの対応が必要である認識を共有した。しかしながら，日本が参画可能性のあるセキュリティ分野については，組織としての議論が必要との認識であり，次年度以降に議論する，また，ＥＬＣＡＩＲで実施するかどうかは，ステアリング会議で議論するとの回答であった。

表３．３．２．１－１にＥＣＬＡＩＲコンソーシアムとの会議における打合覚を示す。

３．４　電動航空機のサイバーセキュリティに関する国際標準化戦略

３．１項～３．３項の結果を受けて，電動航空機のサイバーセキュリティに関する国際標準化戦略を提言するにあたり，現状の整理（３．４．１項参照）および現状の分析（３．４．２項参照）を行い，戦略の立案を実施した。

３．４．１　現状の整理

３．４．１．１　国内外の組織

欧米および日本の航空局および標準化団体の関係を図３．４．１．１－１に示す。前述のとおり、欧米には航空に関する標準化制定団体として、米国はＲＴＣＡ、欧州はＥＵＲＯＣＡＥが存在しており、共同で規格の制定を行っている。ＳＡＥはＲＴＣＡ／ＥＵＲＯＣＡＥで制定される規格を補完する規格の制定を行っている。これら団体で制定された規格は、米国ではＦＡＡ（米国連邦航空局)、欧州ではＥＡＳＡ（欧州航空安全機関）にてAMC（Ａｃｃｅｐｔａｂｌｅ　Ｍｅａｎｓ　ｏｆ　Ｃｏｍｐｌｉａｎｃｅ）が発行され、これらの規格を使用して認証を行うことが宣言されている。

一方、日本では航空局は国土交通省　航空局（ＪＣＡＢ）がその役割を有しているが、航空に関する標準化制定団体は存在していない。

３．４．１．２　航空機サイバーセキュリティに関する国際標準規格

各国際標準化団体で航空機サイバーセキュリティに関して検討を進めている規格について図３．４．１．２－１に示す。ＲＴＧＣＡ／ＥＵＲＯＣＡＥは体系的にサイバーセキュリティに関する規格の制定を進めている。図中で未発行のＥＤ－ＩＳＥＭ／ＤＯ－ＩＳＥＭ（Ｉｎｆ

ｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ　Ｅｖｅｎｔ　Ｍａｎａｇｅｍｅｎｔ）も２０２１年９月に発行予定であり、さらに、２０２１年内にはＥＡＳＡにてAMC（Ａｃｃｅｐｔａｂｌｅ　Ｍｅａｎｓ　ｏｆ　Ｃｏｍｐｌｉａｎｃｅ）が発行される予定である。

一方、ＳＡＥについては、３．１．１．３項に示すとおり、ＣＰＳＳ　Ｅｎｇ．　Ｐｌａｎは投票の結果、否決され、現在は投票時に受けたコメントの反映，検討を行っている。発行時期は未定である。ＳｗＡは２０２２年に発行される計画であるが，ＨｗＡは発行時期の計画が示されてなく，ＳｗＡより後の発行となる見込みである。

３．４．１．３　国内の航空機サイバーセキュリティに関する活動

航空機のサイバーセキュリティに関して、本事業の調査にて確認できた国内の団体を整理し、図３．４．１．３－１にまとめた。航空機装備品認証技術イニシアティブはＤＯ－３２６Ａ／３５６Ａに関して内容の理解や改訂状況の確認を行っている。さらに，把握した内容に関してセミナーを開催して国内への展開を行っている。

ＪＡＸＡの航空機電動化（ＥＣＬＡＩＲ）コンソーシアムでは、「航空機電動化技術標準化ワーキンググループ」を設置し、ＳＡＥの各コミッティ（Ｅ－４０、ＡＥ－７、ＡＥ－９）に参加して動向を調査し，標準・基準の制定状況をモニタしている。入手した情報はコンソーシアム内に展開し，参加団体からの意見を集約している。

産業サイバーセキュリティ研究会は、経産省のサイバーセキュリティ課が主催し、各業界（ビル、電力、防衛装備等々）で分科会を形成し、それぞれの業界の特性に応じたセキュリティ対策を検討しているが、航空業界の分科会は活動が行われていない。

３．４．１．４　将来の電動航空機像

現在の航空機には様々な通信ネットワークが搭載されており、大別すると、制御系、地上との通信系、乗客のエンタメ系と言った３種類に大別される。将来の航空機では、ｅ－Ｅｎａｂｌｅｄ航空機と称され、これらの通信を１つのネットワークとすることで軽量化、低コスト化が期待される。一方で，セキュリティ対策がさらに重要になってくる。図３．４．１．４－１にｅ－Ｅｎａｂｌｅｄ航空機の構成を示す。

Ｂｏｅｉｎｇ社のＢ７８７が世界で最初のｅ－Ｅｎａｂｌｅｄの可能性を有した航空機であると紹介されている(注 1)が，その範囲はメンテナンス性向上や運航の効率化に限定されている。ｅ－Ｅｎａｂｌｅｄ航空機の目指す姿は，制御系まで含めて高度に統合された通信ネットワークであり，従来の航空機とは全く異なるネットワーク構成になると想定されるため，従来機の改修では適用できず，これから開発が行われる新たな機体に適用されるものと想定される。航空機電動化では，最速で２０３０年代に運航開始となる細胴機へ推進系のハイブリッド化が適用され，その後２０４０年代に広胴機へ適用され，２０５０年代には全電動の航空機が実現されると想定されている(注 2)。制御系まで統合されたｅ－Ｅｎａｂｌｅｄ航空機がいつ実現されるか明確な指針は示されていないが，最速の場合，２０３０年代に運航開始となる細胴機へ適用される。

さらに，航空機の電動化が進むと通信ネットワークに接続される機器が増加するため，これらの機器に対してもセキュリティ対策が必要となってくる。

注１：https://www.boeing.com/commercial/aeromagazine/articles/qtr_01_09/pdfs/AERO_Q109_article04.pdf

注２：https://www.aero.jaxa.jp/about/hub/eclair/pdf/eclair_vision.pdf

３．４．２　現状の分析

産業サイバーセキュリティ研究会にて活動されている産業分野は，国内に一定の市場規模があり，国内でのサイバーセキュリティに関する規格化が必要な分野である。一方で，航空産業は，国内の市場規模が小さく世界の市場に進出する必要があり，かつ，欧米の企業が市場を席捲している現状においては，欧米の認証をいかに上手く取得できるかが重要である。

一般的に海外の都合だけで決められた標準・基準に従わざるを得ない状況は，参入障壁を高めることとなるため，航空機電動化（ＥＣＬＡＩＲ）コンソーシアムでは，航空機電動化技術標準化ワーキンググループを設置し，ＳＡＥの様々な技術分野のコミッティに参加して情報収集を行い，参入障壁とならないよう調査をおこなっている。

本調査によりサイバーセキュリティの各コミュニティに参加することで，これらコミュニティで検討されている文書は今まさに整備を行っている段階であることが判明したため，このタイミングで上手く標準化活動に入り込むことが重要である。

ＲＴＣＡ／ＥＵＲＯＣＡＥで検討している文書は，早ければ２０３０年代に運用開始が想定される細胴機の開発に適用されると想定する。一方，ＳＡＥで検討している規格は制定にまだ時間が必要であり，かつ，ＲＴＣＡ／ＥＵＲＯＣＡＥの補完文書という位置づけであるため，実際の航空機開発への適用時期はまだ遅いと想定する。

規格の内容について，今回調査した範囲においては，国際標準化団体で議論されているサイバーセキュリティに関する規格は日本に不利にはなってなく、通例として受け入れられる範囲にとどまっているが，これについては，機体完成機メーカや装備品メーカの意見を広く伺う必要があると考える。また，ｅ－Ｅｎａｂｌｅｄ航空機のように従来とは全く異なる機体システムに対しても十分な検討ができるよう，航空業界に留まらず，ＩＴ系メーカからも意見集約が必要である。

今後としては、国際標準化団体で制定される標準・基準が不利な内容とならないようこれら標準化団体を定点観察し、国内の航空機産業のメーカだけでなくＩＴ系メーカも含めた知識や知恵を集結し、国際標準化団体へフィードバックする道筋を得ることが必要である。

３．４．３　戦略

３．４．３．１　国際標準化団体の定点観察

本調査で実施した国際標準化団体の会合へは継続して参加し情報収集を行うことを提言する。具体的には，今後の調査を国の活動とするために，どこかの国の機関を活動母体として定点観察を継続し，集めた意見は，機関に参加する企業を展開し，意見集約を行うことを想定する。

国際標準化団体の会合は欧州から米国西海岸が参加可能な時間帯で設定されており，日本は深夜の時間帯となる。Ｃｏｖｉｄ－１９の状況が改善されれば対面による会議も開催されるが，その場合でもリモート会議が併用されると想定する。対面またはリモートでの参加，どちらも一長一短あり，会合のたびにどちらで参加するか検討するのがよいと思うが，１つの企業から参加した場合，技術が限定的になると想定されるため，機関に参加する企業にて担当分けを行い，調査することを提言する。調査結果は参画企業で共有すると共に意見交換を行う。

３．４．３．２　攻める領域の選定

ｅ－Ｅｎａｂｌｅｄ航空機のモデル（３．４．４項参照）を，活動母体に参画する企業に展開，意見集約し，モデルをブラッシュアップした上で，欧米の機体完成機メーカと意見交換を行うことで，日本の参画可能性を模索することを提言する。

ＣＰＳＦとの差分の洗い出しについては，各団体の文書の発行を待って追加の調査を行い，本調査で推定した箇所を補完する調査を行うことを提言する。

航空機電動化では様々なシステム形態が検討されており，これらのシステムを今回のモデルに適用した場合，収集がつかなくなる恐れが生じたため，今回は従来航空機のネットワークを１つに統合するという視点でモデルを作成した。航空機の電動化が進んだ場合，様々な機器が機体ネットワークに接続されることからリスクも増えると想定されるため，これらの観点も含めて意見集約を行う。集めた意見をモデルに反映し，欧米の機体完成機メーカとの意見交換を行うことで，日本が参画可能なシステム，機器を模索する。

欧米の機体完成機メーカとの意見交換は，国際標準化団体へ出席することで機体完成機メーカとのコネクションを作り，意見交換の可能性を探ることを想定する。

３．４．３．１項で実施する各国際標準化団体の定点観察により，各団体の文書の改訂・発行状況を把握し，発行された文書の内容確認を行う。

３．４．３．３　体制

日本全体の活動とするためにも国の機関に活動母体を置くことが望ましい。航空機の電動化が進み，サイバーセキュリティがますます重要になってくることもあり，活動母体としては航空機電動化（ＥＣＬＡＩＲ）コンソーシアム内の航空機電動化技術標準化ワーキンググループを第１候補とすることを提言する。

図３．４．３．３－１に来年度以降の活動体制のイメージ図を示す。

３．４．３．４　スケジュール

活動スケジュールとして，国内の意見集約は定期的に実施するが，３．４．３．１項の国際標準化団体の定点観察により各団体で実施している文書改訂のタイミングに合わせて各団体への提案を行うことを提案する。提案活動のスケジュールを表３．４．３．４－１に示す。

３．４．４　ＣＰＳＦを用いた将来電動航空機に対するセキュリティ対策

ＣＰＳＦを用いた将来電動航空機に対するセキュリティ対策を考えるにあたり，航空機全体および航空機周辺の環境も含めて検討する必要があると考え，本事業では３．４．１．４項で示したｅ－Ｅｎａｂｌｅｄ航空機を題材として採用した。図３．４．４－１にＣＰＳＦで提唱されるモデル用いてｅ－Ｅｎａｂｌｅｄ航空機を整理した結果を示す。

３．４．４．１　モデル説明

第１層は、空港、管制塔、機体メーカ、エアライン、部品メーカなど航空機の飛行にかかわるソシキが属する。第２層は機上システム、コントローラ、電子フライトバッグ（ＥＦＢ）、アビオニクス、乗務員などｅ－Ｅｎａｂｌｅｄ航空機を構成する、システム、モノ、ヒトが属する。航空機電動化が進むにつれて，様々な機器が図中のＣｅｎｔｒａｌ　ＧＷの下に接続されると想定するが，航空機電動化のシステムはそれ自体で様々なシステムが提案・検討されている状況で

あり，今回のモデルに加えると収集がつかないことが想定されたため，今後のベースとなるよう，今回は従来の航空機に対して機内ネットワークを１つに統合したシステムを想定した。ただし、統合した１つの機内ネットワークの中に、飛行に関する制御用のシステム、乗務員が客室支援に利用する乗務員用のシステム、飛行中の娯楽を提供する乗客用のシステムと３つの役割で構成要素を分類している。第３層は管制情報処理システム、リモート操舵システム、ＳＡＴＣＯＭ、Ｃｅｎｔｒａｌ ＧＷなど機内、地上間でデータをやり取りするためのシステム、モノ、データが属する。

３．４．４．２　ｅ－Ｅｎａｂｌｅｄ航空機で実現できる機能

ｅ－Ｅｎａｂｌｅｄ航空機を考えた場合，これまで接続されていなかった機器がネットワークにつながることで，以下のような機能が実現できる。

- 地上，衛星通信を介した自動運転，リモート操縦
- 地上，衛星通信を介したソフトウェア更新
- 航空機同士の通信による衝突回避
- ブラックボックス代替となるログ，動画等の記録
- リアルタイムに収集可能な情報をもとにした事故分析
- 機内Ｗｉｆｉの充実により、ショッピングやカード決済など地上と同様のネットサービスの利用
- ＥＦＢや乗務員用デバイスなどを利用した乗客支援

３．４．４．３　想定される脅威

図３．４．４－１における脅威として以下が考えられる。

３．４．４．３．１　ｅ－Ｅｎａｂｌｅｄ航空機自体の脅威

- 制御系とエンターテイメント系の接続による乗客の持ち込みデバイス経由の攻撃
- ソフトウェアの適用範囲の拡大による攻撃対象の増加
- 更新（ＯＴＡ）に伴うメンテナンスの無線化と、ＵＰＤＡＴＥ頻度が高くなることによる攻撃機会の増加
- ＥＦＢや乗務員デバイスが機外でウィルス感染し､機内システムへ影響を与えるなど乗務員デバイス経由の被害
- 飛行にかかわる制御用システムのＯＳが汎用化することによる攻撃の容易化

３．４．４．３．２　組織にまたがる脅威

- サプライチェーン攻撃
- 自動航行・リモート操縦に関連する機能や通信を狙う攻撃

３．４．４．３．３　セーフティに関わる脅威

- セキュリティ侵害時の復旧

  セキュリティ侵害時の復旧では、セキュリティインシデントが発生した場合、フェールセーフな方向に対処すべきである。飛行中の航空機は、自動車などと異なり、セキュリティインシデントが発生した場合も機能を停止させず、飛び続けることが優先されるべきだと考えられる。そのため、復旧時の対応方法にも、航空機のセーフティの考え方を紐づける必要が

ある。

３．４．４．４　セキュリティ対策，考慮事項

図３．４．４－１におけるセキュリティ対策、考慮事項として以下が考えられる。

- 乗客デバイスから乗務員用Ｗｉｆｉへは進入不可，乗客デバイスおよび乗務員Ｗｉｆｉからは制御系へは進入不可となる機構が必要。
- 乗客同士でカード情報等を窃取されないよう乗客用Ｗｉｆｉもセキュリティ対策が必要。
- 制御系は攻撃を受けた場合でも停止はできないため，切り離して飛行を継続できる冗長構成が必要。
- 乗務員が使用するＥＦＢが地上でウィルス感染等しない対策が必要。
- 調達、テスト段階での受け取りテストを行いサプライチェーンのセキュリティ確保が必要。
- 方式が明らかになっている既存の認証・暗号は攻撃者に研究されている可能性があるため、独自の認証・暗号化が必要。
- 同一型式の航空機におけるセキュリティ対策が完全に一致している場合に発生する影響拡大の防止策（航空会社ごとに別の方式を用いる等）が必要。

本事業で洗い出されたセキュリティ対策は上記のとおりであるが，システムの詳細な検討に合わせて，脅威・脆弱性・リスクを全て網羅した上で繰り返し評価を行っていく必要があると考える。ｅ－Ｅｎａｂｌｅｄ航空機について詳細化を行い，フレームワーク上に書き表し，ＣＰＳＦのコンセプトに基づいたリスクアセスメントを完成機メーカやＩＴ系メーカの知見も取り込んで進めていく必要があると考える。

表３．１．１．２－１　ＳＡＥ　Ｇ－３２検討文書

文書番号	文書名	検討内容
JA7496	Cyber Physical Systems Security Engineering Plan (CPSSEP)	サイバー・フィジカル　セキュリティのリスクの特徴付け、脆弱性評価、緩和策提示。脆弱性の悪用に関する知識提供。ベストプラクティス特定。ハードウェアおよびソフトウェアでの保証のギャップを埋め、システムエンジニアリングの取り組みを通じて全体的なアプローチを統合する方法について検討している。
JA6678	Cyber Physical Systems Security Software Assurance (SwA)	システムズエンジニアリングにおけるサイバー・フィジカルシステムのソフトウェアの脆弱性、ライフサイクル全体を通じたセキュリティの確保と復元力評価方法について検討している。
JA6801	Cyber Physical Systems Security Hardware Assurance (HwA)	システムズエンジニアリングにおけるサイバー・フィジカルシステムのハードウェアの弱点と脆弱性、ライフサイクル全体を通じたセキュリティの確保と復元力評価方法について検討している。

表３．１．１．３－１　ＳＡＥ議論内容（Ｍａｉｎ）

日時(JPT)	出席者数	議論内容
Day1 1:00~2:00	約 35 名	4.2 項「CPSS Lifecycle Management Process」、4.2.3 項「CPSS Lifecycle Supporting Process」に追加した記載内容について議論
Day2 7:00~8:00	約 17 名	4.2.3 項~4.2.7 項に関して集めたコメントについて１つずつ内容確認 今後の予定として、1/20 に Ballot(投票）予定。
－	－	Ballot 期間（1/19~2/15）に入ったと連絡あり。各自内容確認し、コメントを作成する時間確保のため 1/20、27 の会合キャンセルとの連絡あり。 Voting メンバはコメントと投票を､それ以外のメンバからもコメントは受け付ける。
Day3 1:00~1:30	約 34 名	Ballot の仕方について解説。質問受付 その場での質問として, ・コメントはいつ反映されるのか？ ・コメント反映後に Vote では？ 等があった。次週も質問を受け付ける。
Day4	－	会議には参加してないが、ＷＥＢに Ballot の結果が掲載された。 賛成９名、反対１１名、辞退３名、未投票３４名 で否決された。

表３．１．１．３－２　ＳＡＥ議論内容（ＳｗＡ）

<table>
<tr><th>日時(JPT)</th><th>出席者数</th><th>議論内容</th></tr>
<tr><td>Day1
3:00~4:00</td><td>約 12 名</td><td>13.2 項「Prepare for Security aspects of verification」の記載内容について議論</td></tr>
<tr><td>Day2
3:00~4:00</td><td>約 16 名</td><td>CPSS software に対する Static/Dynamic/Hybrid test、 および Review に対する定義について議論</td></tr>
<tr><td>Day3
3:00~4:00</td><td>約 16 名</td><td>13.2.6 項「Security aspects technical objective white/gray/black box testing」に関して議論</td></tr>
<tr><td>Day4
3:00~4:00</td><td>約 17 名</td><td>9.2.1 項「Reporting Requirements for Non-conformances of Failures」に関して議論</td></tr>
<tr><td>Day5
3:00~4:00</td><td>約 15 名</td><td>同上</td></tr>
<tr><td>Day6
3:00~4:00</td><td>約 20 名</td><td>年末までにすべての章を完成させる下表の計画が示された。
年末までに完了させるために Mtg を 60 分→90 分に延長する。
<table>
<tr><th>項目</th><th>進捗</th><th>期限</th><th>懸念事項</th></tr>
<tr><td>Integral</td><td>案のみ</td><td>12/E</td><td></td></tr>
<tr><td>Acquisition</td><td>案のみ</td><td>9/E</td><td></td></tr>
<tr><td>Planning</td><td>50% Reviewed</td><td>11/E</td><td></td></tr>
<tr><td>Requirement</td><td>Draft</td><td>4/E</td><td></td></tr>
<tr><td>Architecture & Design</td><td>案のみ</td><td>8/E</td><td>担当不在</td></tr>
<tr><td>Implementation</td><td>案のみ</td><td>6/E</td><td></td></tr>
<tr><td>Verification</td><td>30% Reviewed</td><td>2/E</td><td></td></tr>
<tr><td>Lifecycle Support</td><td>案のみ</td><td>10/E</td><td>担当不在</td></tr>
</table>
</td></tr>
</table>

表３．１．１．３－３　ＳＡＥ議論内容（ＨｗＡ）

日時(JPT)	出席者数	議論内容
Day1 1:00~2:00	約 17 名	章立てについて議論 ・Req. definition ・Establish assurance Claims ・Assessment defining the assurance case ・Residual risk analysis ・Implement assurance Plan ・Verification & Validation
Day2 1:00~2:00	約 16 名	Industry　news の紹介 2021CY の計画（次回 1Q/2Q の目標提案） Main(CPSSEP)への引用箇所の確認
Day3 5:00~6:00	約 12 名	Industry news の紹介 2021CY の計画（1Q/2Q の目標）は次回提案 Main(CPSSEP)の Ballot 期間中に F/B したく、System 要求定義のための HwA の活動、アウトプットについて議論 【HwA の活動】 1.システム要求のレビュ 2.H/W に保有されるクリティカル情報の識別 3.H/W に影響のあるセキュリティ要求の洗い出し 4.システムの要素、脅威から H/W のリスク評価 5.CWE(注 1)をガイダンスとしてリスク回避策立案
Day4 1:00~2:00	約 15 名	上記【HwA の活動】を 6 章に入れ込み、その前後の文章を議論
Day5 5:00~6:00	約 10 名	前日と同様に 6 章について議論。 他の章の構成（統廃合）について議論

表３．１．２．２－１　ＲＴＣＡ　ＳＣ－２１６　発行済み文書

文書番号	文書名	概要
DO-326A	Airworthiness Security Process Specification	最新版は２０１４／８に発行されている。関連する地上システムや環境を含む航空機全体の情報セキュリティについて記述されており、航空機システムセキュリティに関連する文書のコアとなる文書である。
DO-355A	Information Security Guidance & Continuing Airworthiness	最新版は２０２０／９に発行されている。航空機に関連する情報セキュリティの脅威について、運用・整備時に実施すべき内容について整理されている。
DO-356A	Airworthiness Security Methods & Considerations	最新版は２０１８／６に発行されている。ＥＵＲＯＣＡＥとの共同で発行された文書（ＥＵＲＯＣＡＥでの文書番号はＥＤ－２０３Ａ）。耐空性セキュリティプロセスで使用する手法やガイドラインを記述している。

表３．１．２．２－２　ＲＴＣＡ／ＥＵＲＯＣＡＥ合同会議（２０２０／9）議事録概要

日時：2020/9/18
場所：Web 会議
参加者：約 50 名。日本企業として Panasonic Avionics が参加しているが、日本人の参加は無し。
　　EUROCAE と RTCA の合同で実施。
議事：

- ✓ ED-205A 改訂に向けてスケジュールの提示。2021/6 にドラフト発行予定。
- ✓ ED-204A/DO-355A 発行済み。改訂前にもらった指摘に対する状況の紹介
- ✓ 次のドキュメント（ED-XXX　Information Security Event Management(ISEM)）の進捗。2021/3Q 発行予定。
- ✓ ED-201A の改訂進捗状況。~2020/12 ドラフト完、2021/3~コメント集約
- ✓ ED と DO のリンク付けの進捗
- ✓ 他の WG との協働
  - ・ WG-114、SAE G-34 が航空機システムに搭載する AI について検討しており、コメント提出。
  - ・ SAE G-32 から検討中の文書について紹介。ED-20X を補完する文書との位置づけ。
  - ・ WG-105/RTCA SC-228 は UAS を検討しており、関係構築が必要。
  - ・ WG-112 は VTOL を検討しており、ED-203A に反映が必要かもしれない。
  - ・ SAE　E-36 はエンジン制御システムを検討しているが、COVID-19 の影響で会合無し。

表３．１．２．３－１　ＲＴＣＡ／ＥＵＲＯＣＡＥ合同会議で入手した情報（２０２０／１２）

SubGr.	日時(JPT)	出席者数	議論内容
SG4	Day1(月) 23:00~4:00	約 46 名	ED-201/DO-xxx 「 Aeronautical Information Systems Security Framework Guidance」について、各社から集めたコメント１つずつ対応を議論。
SG3	Day2(水) 23:00~4:00	約 46 名	ED-ISEM/DO-ISEM「Information Security Event Management」の３章「Organize & Prepare」、４章「Detect Security Event」について各担当の作成内容について議論。
Plenary	Day3(金) 23:00~1:00	約 50 名	各 SG の状況報告： ・SG2:ED-205A/DO-xxx「Process Standard for Security Certification and Declaration of ATM ANS Ground Systems」について TOR(注 1) を開始すると報告 ・SG3：ED-ISEM/DO-ISEM　COVID の影響もあり、かなり遅れており、3 月迄は隔週で Mtg を行う。また、2021/3 の OC(注 2) に向けてアクションを厳しく管理していくと報告 ・SG4：ED-201A/DO-xxx　全コメントに対して検討実施済みと報告。2021/3 の OC に向けて準備していくと報告 その他： 他のグループとのリエゾンについて、European Cybersecurity Standards Coordination Group で各規格の差分を検討しており、次回会合は 2021/1/26 との紹介があった。 次回会合の予定 2021/3/15-19　Virtual　Mtg 2021/6/7-11　Face to Face Mtg in Europe 2021/9/13-17　Face to Face Mtg in DC.

表３．１．３．２－１　ＥＵＲＯＣＡＥ　ＷＧ－７２検討文書

文書番号	文書名	概要
ED-201A	Aeronautical Information System Security Framework Guideline	初版のＥＤ－２０１は２０１５年に発行されが，文書内で引用している標準が改訂されたため、本書もA改訂として改訂内容を検討している。ＥＡＳＡからの指示により航空業界全体に共通するルール（Ｈｏｒｉｚｏｎｔａｌ　Ｒｕｌｅ）となるよう改訂内容を検討している。
ED-203A	Airworthiness Security Methods & Considerations	２０１８年6月にＲＴＣＡと共同で発行された文書（ＲＴＣＡでの文書番号はＤＯ－３５６Ａ）で、耐空性セキュリティプロセスで使用される手法やガイドラインについて記述されている。
ED-204A	Information Security Guidance for Continuing Airworthiness	ＲＴＣＡと共同で発行された文書（ＲＴＣＡでの文書番号はＤＯ－３５５Ａ）で、航空機に関連する情報セキュリティの脅威について、運用・整備時に実施すべき内容について整理している。
ED-205A	Process Standard for Security Certification & Declaration of ATM ANS Ground Systems	初版のＥＤ－２０５は２０１９年3月に発行され、地上のＡＴＭ／ＡＮＳシステムのセキュリティを評価するプロセスを明示している。A改訂を目指して改訂内容を検討している。
ED-ISEM	Information Security Event Management	ＥＤ－ＩＳＥＭは運用後にサイバー攻撃等のイベントが発生した場合に実施するプロセスについて記載される。２０２１年9月に新規発行を目指して記載内容を検討している。

表３．２．１－１　カテゴリ別のＲＴＣＡ文書シリーズ記載率

ＣＰＳＦカテゴリ略称（名称）	ＲＴＣＡ文書記載率
CPS.AM（資産管理）	100.0%
CPS.BE（ビジネス環境）	0.0%
CPS.GV（ガバナンス）	75.0%
CPS.RA（リスク評価）	100.0%
CPS.RM（リスク管理戦略）	100.0%
CPS.SC（サプライチェーンリスク管理）	36.4%
CPS.AC（アイデンティティ管理、認証及びアクセス制御）	100.0%
CPS.AT（意識向上及びトレーニング）	100.0%
CPS.DS（データセキュリティ）	46.7%
CPS.IP（情報を保護するためのプロセス及び手順）	50.0%
CPS.MA（保守）	50.0%
CPS.PT（保護技術）	100.0%
CPS.AE（異変とイベント）	80.0%
CPS.CM（セキュリティの継続的なモニタリング）	83.3%
CPS.DP（検知プロセス）	50.0%
CPS.RP（対応計画）	25.0%
CPS.CO（伝達）	0.0%
CPS.AN（分析）	100.0%
CPS.MI（低減）	100.0%
CPS.IM（改善）	50.0%

表３．２．１－２　ＲＴＣＡ文書からの参照文書

発行元	文書番号	文書名
ISO	ISO27005:2011, Guide 73:2009	Information Technology - security techniques - information security risk management
NIST	Special Publication 800-162	Guide to attribute based access control (ABAC) definition and considerations
	NIST 800-57	Recommendation for key management
FAA/EASA	AC25.1309/AMC 25.1309	System design and analysis
	14 CFR 21.50/EASA Reg 21.61	Instructions for continued airworthiness and manufacture's maintenance manuals having airworthiness limitations sections.
SAE/EUROCAE	ARP4754A/ED-19A	Guidelines for development of Civil Aircraft and Systems
	ARP4761/ED-135	Safety Assessment Process for Civil Airborne Systems
EUROCAE	ED-201	Aeronautical Information System Security Framework Guidance
RTCA/EUROCAE	DO-326A/ED-202A	Airworthiness Security Process Specification
	DO-254/ED-80	Design Assurance Guidance for Airborne Electronic Hardware
	DO-178C/ED-12C	Software Considerations in Airborne Systems and Equipment Certification
	DO-330/ED-215	Software Tool Qualification
	DO-297/ED-124	Integrated Modular Avionics (IMA) Development
ARINC	ARINC653	software specification for space and time partitioning in safety-critical avionics real-time operating systems (RTOS).

表３．３．２．１－１　電動化（ＥＣＬＡＩＲ）コンソーシアムとの議論内容

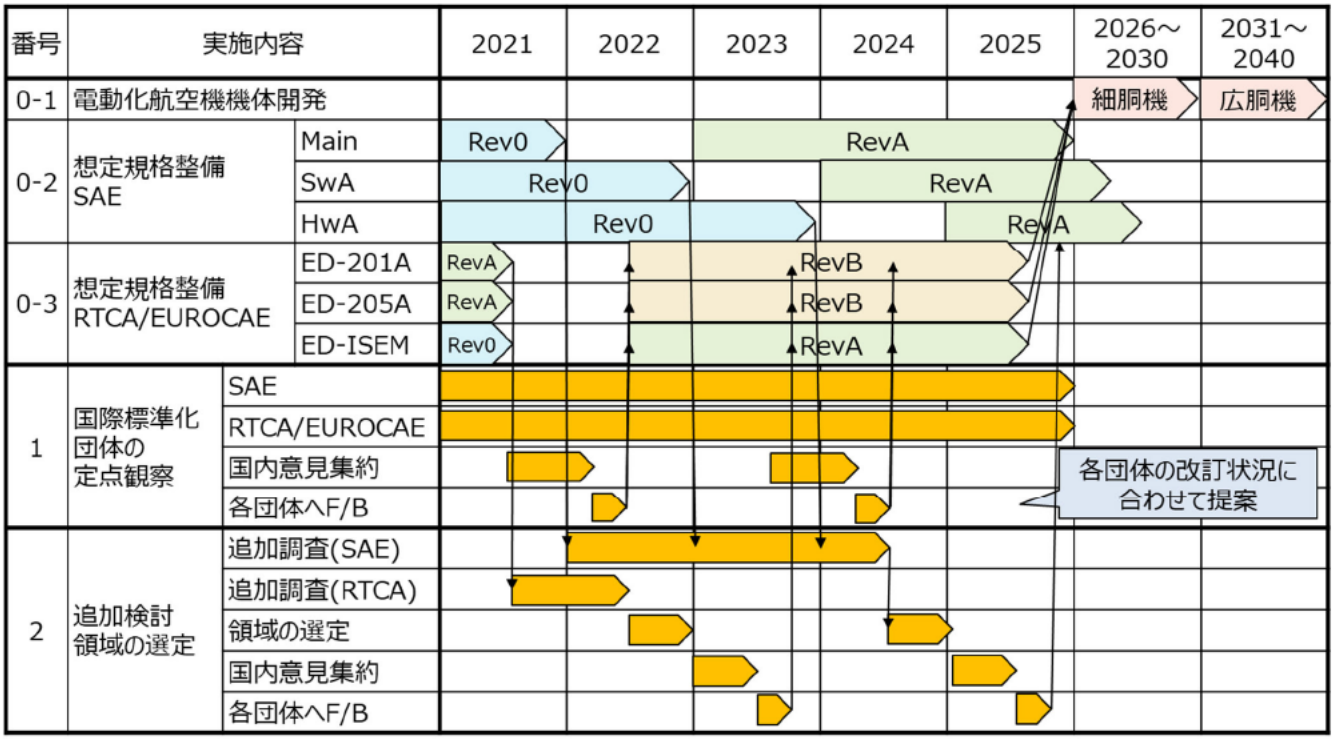
文書番号:N/A

機種	日時	場所	出席者
[redacted]		Teams 会議	[redacted]
件名	サイバーセキュリティ調査事業に関して 航空機電動化（ÉCLAIR）コンソとの意見交換		
打合資料	CS 調査事業.pdf		
目的	サイバーセキュリティ調査事業の調査状況の共有と来年度以降の活動母体に関する調整		
議事および決定事項	[redacted] SJCA で受けている NEDO の調査事業「航空機装備品，電動化分野における研究開発動向調査」においても，電動化に加えてサイバーセキュリティの検討が必要であると整理されており，ÉCLAIR の標準化ワーキンググループに入れる方向で検討するが，ÉCLAIR のステアリング会議にて議論の上決定したい。 e-Enabled 航空機に対するロードマップはどうなっているか？ 今回調査した範囲では見つけることができなかった。 電動化より進んでおり，欧米でロードマップが作成されていると思う。技術的な成立性や誰が先導しているか知りたい。 追加調査し，判明したら共有する。) 従来の航空機では制御ネットワークは外部に繋がってないため，セキュリティ対策は不要という理解で良いか？ そういう意見もあるが，制御権が本当に取られないか不明であり，不明であるから不安全という意見もある。乗っ取られた形跡があるというレポートもある。 ÉCLAIR で実施するのであれば電動化された航空機に適用した場合にどうなるかという検討となる。日本で担当できる範囲はどこになると思うか？ ネットワークにつながる装備品すべてが対象になると想定する。 喫緊の締切はいつか？ 本事業の経産省への締切は 3/22 である。ÉCLAIR に組み込むよう 3/22 の報告書には記載したい。 ÉCLAIR で受けれなかった場合，他の受け皿はあるのか？ 航空機装備品認証技術イニシアティブが来年度からコンソーシアムになると伺っており，そこが候補の1つである。ただし，電動化によりサイバー攻撃の侵入経路が増え，電動化としてしっかりと取り組んでいく必要があり，また，サイバーセキュリティを参入障壁とさせないためにも ÉCLAIR で受けていただきたいと考えている。 [redacted] AIDA を主催されており，RTCA との連携を進めている。どういうスタンスで進めるかはもう少し調査するが，電動化として入り込んでいくために整理したい。今月下旬が納期の報告書に ÉCLAIR を受け皿とすると書けるかどうかは現時点では不明であることは了承願う。 了解。) 差分調査を行い，電動航空機に適用した場合の課題抽出をするとあるが，現時点で明確な課題が見つかっているのか？) 差分の洗い出しは完了し，記述の精度に差がある等は見つかってきたが，電動航空機に対する明確な課題は見つかっていない。		

表３．３．２．１－１　電動化（ＥＣＬＡＩＲ）コンソーシアムとの議論内容（つづき）

議事および決定事項	ソフト等の他の認証と異なり，サイバーセキュリティの議論のコアを ÉCLAIR とするポイントとして，ソフトは既に制定されている規格をどう実行するかであることに対して，サイバーセキュリティは認証をとるためだけでなく，技術論が必要となってくる。サイバー攻撃を防ぐためにどういう機器が必要かを決める必要があり，自動車や IT での実績を航空にどう持ち込むかについて議論が必要。航空メーカだけでは対応できないと思う。 HW は作れても SW が苦手という話があったように，物が作れてもサイバーセキュリティが乗り越えられないという状況になることが考えられる。航空以外のプレイヤーを入れていく必要があることを理解した。 HISOL は自動車の Tier1/2 と組んで H/W 回路のコンサル等も実施している。話を聞く限り，開発のかなり上流段階でサイバーセキュリティに関して議論が必要である。 e-Enabled 航空機のもっと詳細なシステムに落として，具体的な議論が必要。要素機器は海外を使って，システムで入り込んでいくという戦略もあるが，価値が下がって安い部分でしか担当できなくなる。 欧米はそうしてくると思われるので，どうすれば防御できるか考える必要がある。 機内のルータ等をどう取っていくかの戦略が必要。 パイロット不足への対応のため，自動着陸が必要と FAA が言っている。そのため Connected なシステムが必要との議論になっている。 来年度以降定点観測等を行うための母体を探していきたい。 以上

表３．４．３．４－１　活動スケジュール



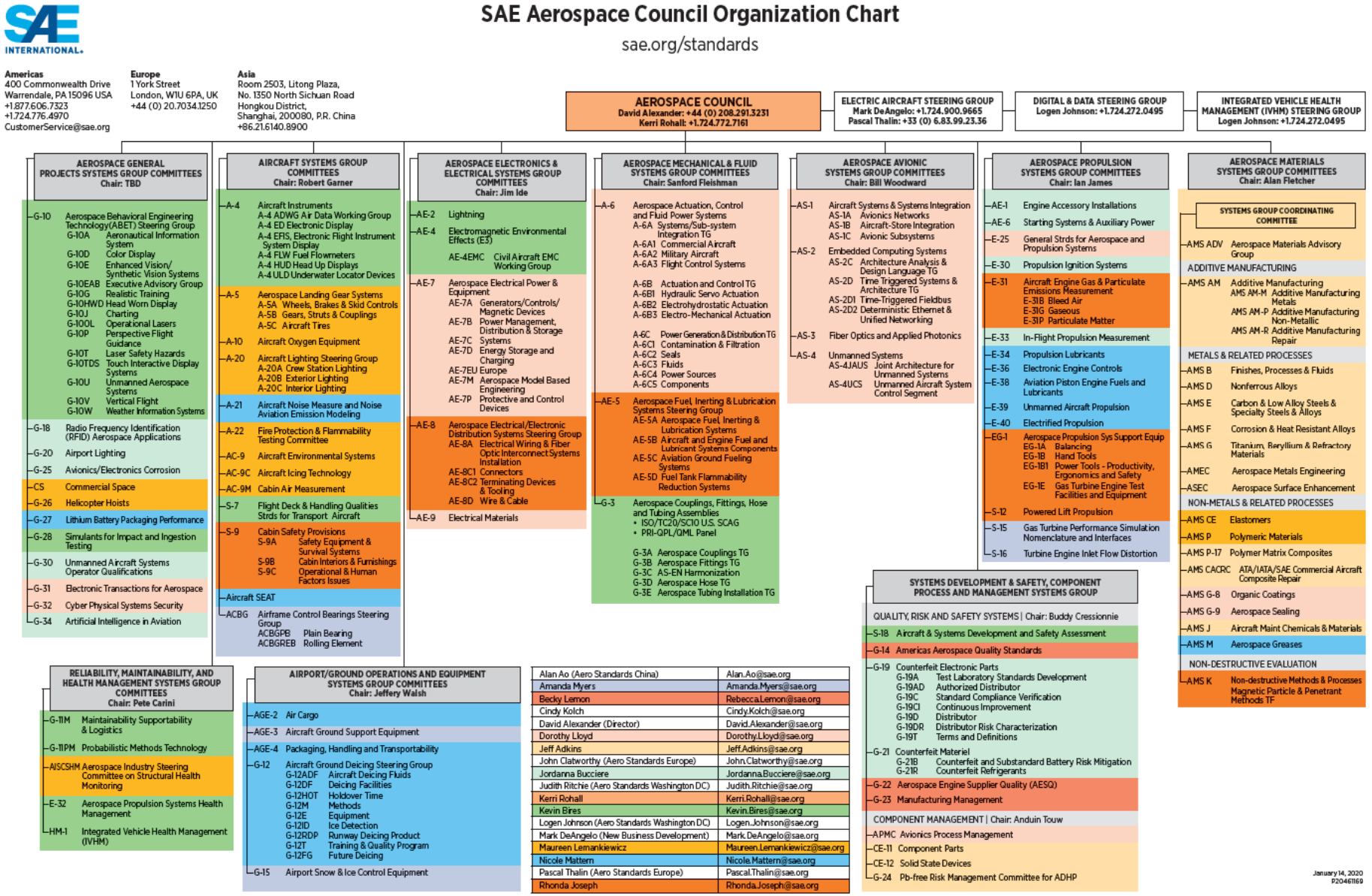


図３．１．１．１－１　ＳＡＥ航空宇宙分野コミッティ一覧

カテゴリ略称（名称）	カテゴリ英名	DO-326	DO-355	DO-356	DO全体
CPS.AM(資産管理)	CPS.AM-1				
	CPS.AM-2				
	CPS.AM-3				
	CPS.AM-4				
	CPS.AM-5				
	CPS.AM-6				
	CPS.AM-7				
CPS.BE(ビジネス環境)	CPS.BE-1				
	CPS.BE-2				
	CPS.BE-3				
CPS.GV(ガバナンス)	CPS.GV-1				
	CPS.GV-2				
	CPS.GV-3				
	CPS.GV-4				
CPS.RA (リスク評価)	CPS.RA-1				
	CPS.RA-2				
	CPS.RA-3				
	CPS.RA-4				
	CPS.RA-5				
	CPS.RA-6				
CPS.RM (リスク管理戦略)	CPS.RM-1				
	CPS.RM-2				
CPS.SC (サプライチェーン リスク管理)	CPS.SC-1				
	CPS.SC-2				
	CPS.SC-3				
	CPS.SC-4				
	CPS.SC-5				
	CPS.SC-6				
	CPS.SC-7				
	CPS.SC-8				
	CPS.SC-9				
	CPS.SC-10				
	CPS.SC-11				
CPS.AC (アイデンティティ管理、認証及びアクセス制御)	CPS.AC-1				
	CPS.AC-2				
	CPS.AC-3				
	CPS.AC-4				
	CPS.AC-5				
	CPS.AC-6				
	CPS.AC-7				
	CPS.AC-8				
	CPS.AC-9				
CPS.AT (意識向上及び トレーニング)	CPS.AT-1				
	CPS.AT-2				
	CPS.AT-3				

カテゴリ略称（名称）	カテゴリ英名	DO-326	DO-355	DO-356	DO全体
CPS.DS (データセキュリティ)	CPS.DS-1				
	CPS.DS-2				
	CPS.DS-3				
	CPS.DS-4				
	CPS.DS-5				
	CPS.DS-6				
	CPS.DS-7				
	CPS.DS-8				
	CPS.DS-9				
	CPS.DS-10				
	CPS.DS-11				
	CPS.DS-12				
	CPS.DS-13				
	CPS.DS-14				
	CPS.DS-15				
CPS.IP (情報を保護するための プロセス及び手順)	CPS.IP-1				
	CPS.IP-2				
	CPS.IP-3				
	CPS.IP-4				
	CPS.IP-5				
	CPS.IP-6				
	CPS.IP-7				
	CPS.IP-8				
	CPS.IP-9				
	CPS.IP-10				
CPS.MA (保守)	CPS.MA-1				
	CPS.MA-2				
CPS.PT (保護技術)	CPS.PT-1				
	CPS.PT-2				
	CPS.PT-3				
CPS.AE (異変とイベント)	CPS.AE-1				
	CPS.AE-2				
	CPS.AE-3				
	CPS.AE-4				
	CPS.AE-5				
CPS.CM (セキュリティの 継続的なモニタリング)	CPS.CM-1				
	CPS.CM-2				
	CPS.CM-3				
	CPS.CM-4				
	CPS.CM-6				
	CPS.CM-7				
CPS.DP (検知プロセス)	CPS.DP-1				
	CPS.DP-2				
	CPS.DP-3				
	CPS.DP-4				
CPS.RP (対応計画)	CPS.RP-1				
	CPS.RP-2				
	CPS.RP-3				
	CPS.RP-4				
CPS.CO (伝達)	CPS.CO-1				
	CPS.CO-2				
	CPS.CO-3				
CPS.AN (分析)	CPS.AN-1				
	CPS.AN-2				
	CPS.AN-3				
CPS.MI(低減)	CPS.MI-1				
CPS.IM (改善)	CPS.IM-1				
	CPS.IM-2				

図３．２．１－１　ＣＰＳＦと海外標準文書の比較結果概要

図３．２．１－２　ＣＰＳＦと海外標準文書の比較結果概要（未調査文書の推定を含む）

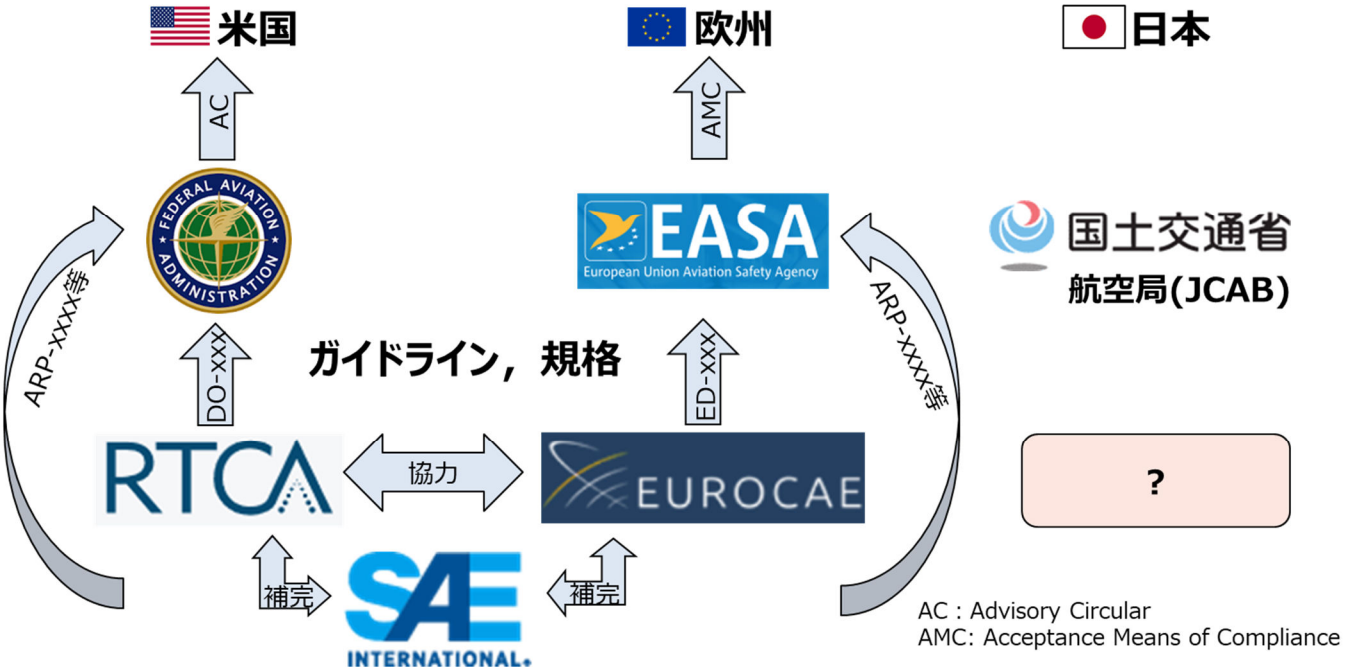


図３．４．１．１－１　欧米と日本の航空局と標準化団体の関係整理

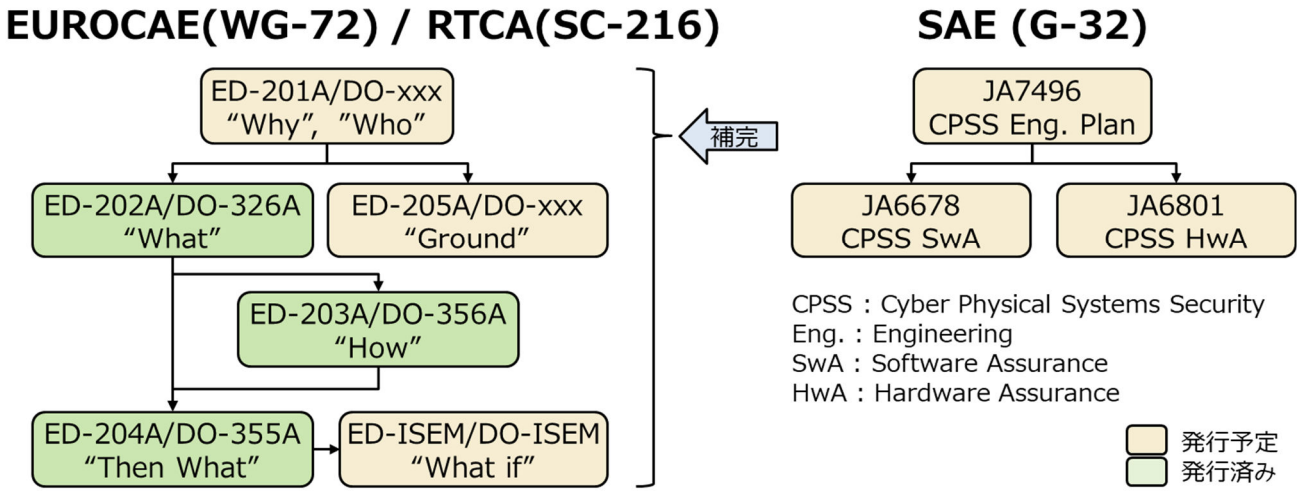
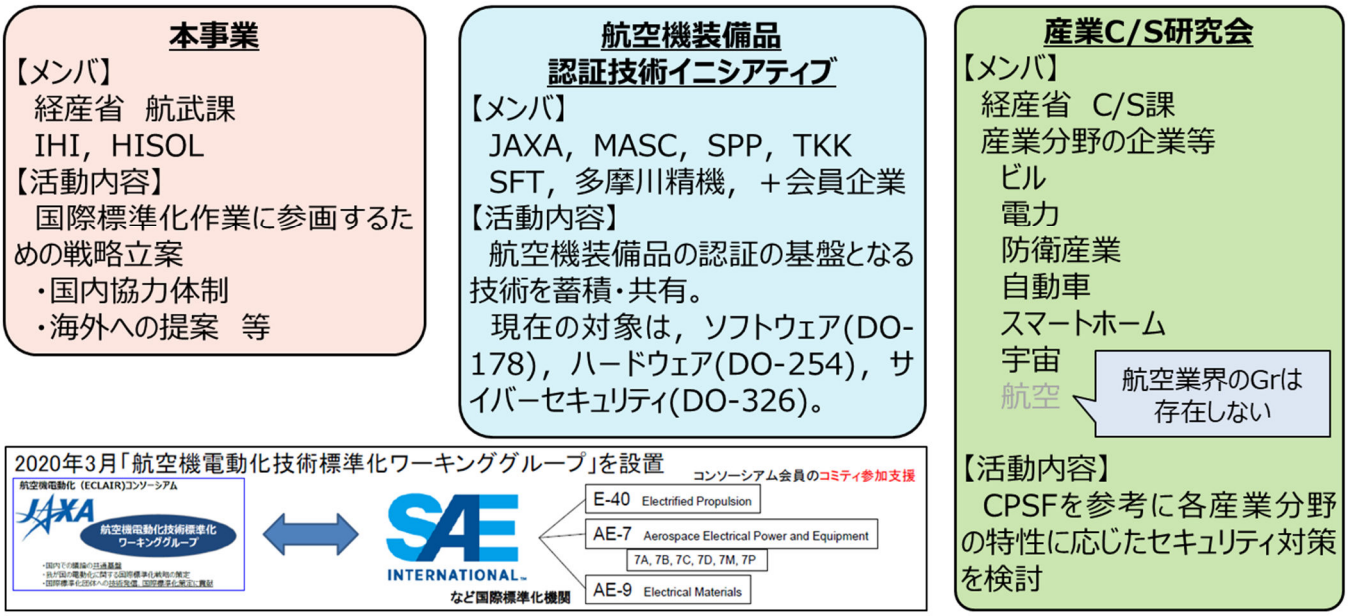
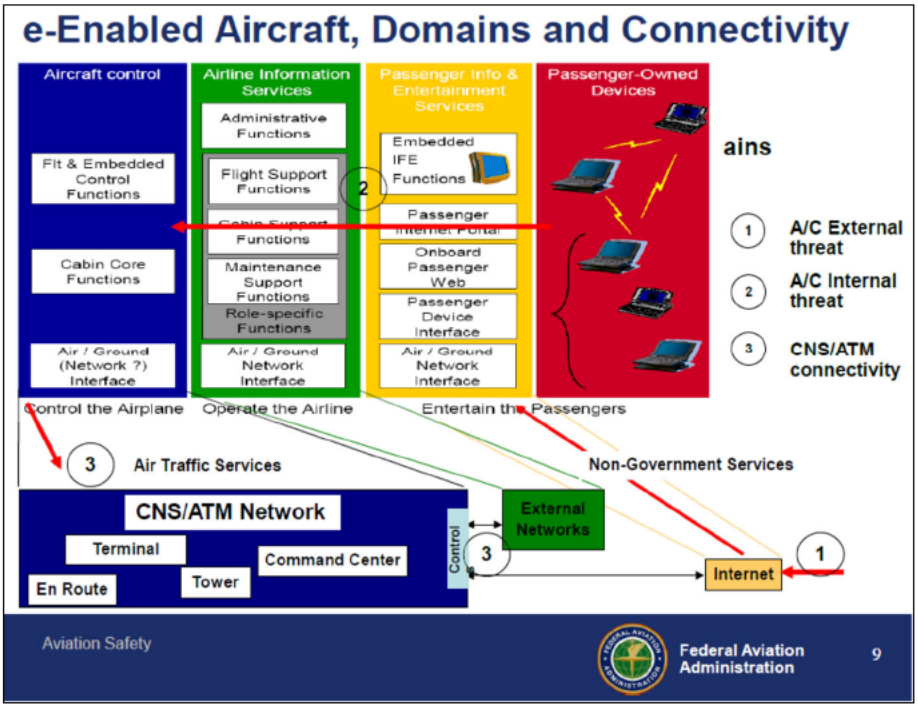


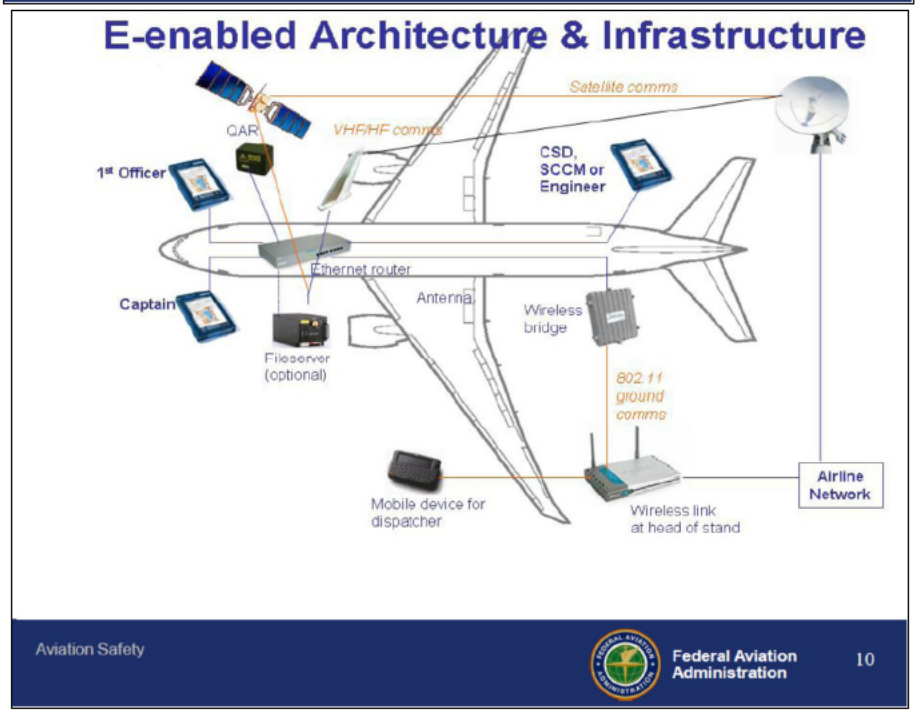
図３．４．１．２－１　航空機サイバーセキュリティに関する国際標準



第３回 航空機電動化コンソーシアム 第３回オープンフォーラム(2020/10)資料
https://www.aero.jaxa.jp/news/event/pdf/event201026/03eclair.pdf

図３．４．１．３－１　航空機サイバーセキュリティに関する国内組織





FAA Aircraft Systems Information Security Protection (ASISP) Overview、 Paper #132 2015/04
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7121273

図３．４．１．４－１　ｅ－Ｅｎａｂｌｅｄ航空機

第３回　航空機電動化コンソーシアム　第３回オープンフォーラム(2020/10)資料
https://www.aero.jaxa.jp/news/event/pdf/event201026/03eclair.pdf

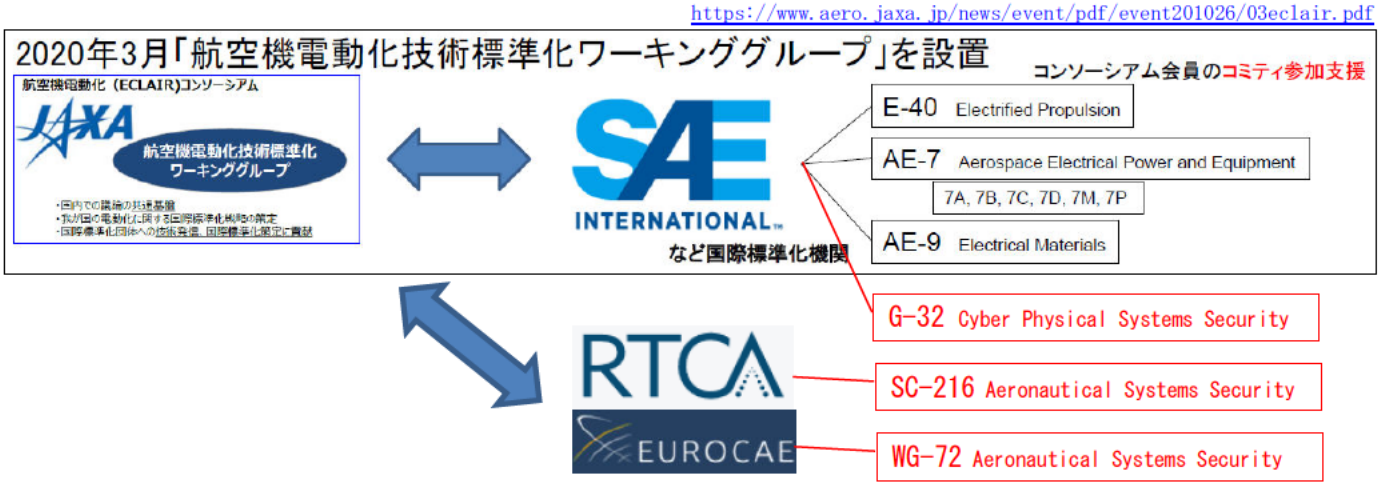


図３．４．３．３－１　来年度以降の活動体制イメージ図

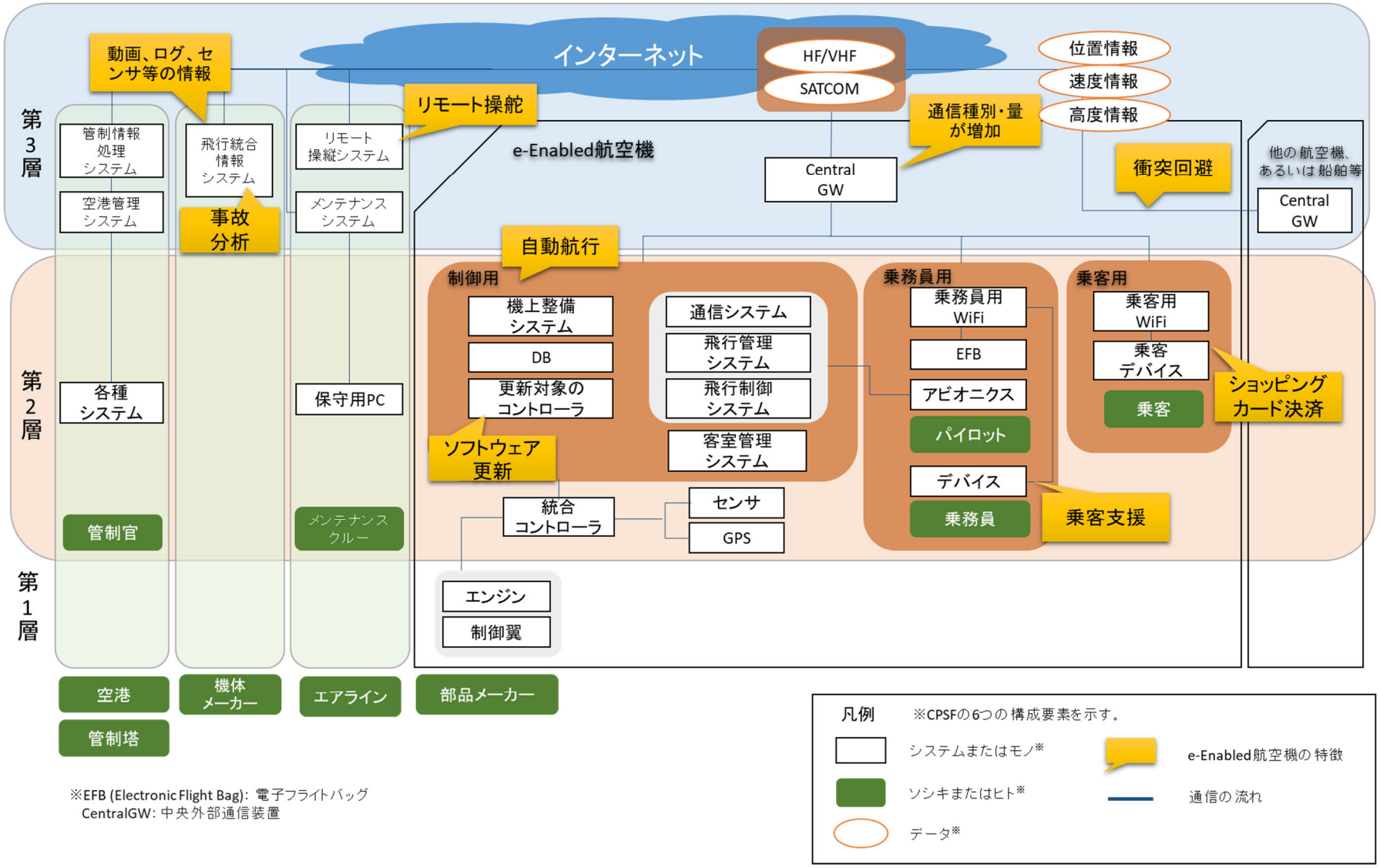


図３．４．４－１　ＣＰＳＦを適用したｅ－Ｅｎａｂｌｅｄ航空機のモデル

（様式２）

二次利用未承諾リスト

報告書の題名　令和２年度内外一体の経済成長戦略構築にかかる国際経済調査事業（民間航空機サイバーセキュリティのルール形成（国際標準化含む）戦略に係る調査研究）調査報告書

委託事業名　令和２年度内外一体の経済成長戦略構築にかかる国際経済調査事業

受注事業者名　株式会社IHI

頁	図表番号	タイトル
25	図3.1.1.1-1	ＳＡＥ航空宇宙分野コミッティ一覧
30	図3.4.1.4-1	ｅ－Ｅｎａｂｌｅｄ航空機