



令和 7 年度 3／四半期の勉強会（A）の概要について

令和 8 年 1 月 18 日

ASPI 荒木(淳)

1 趣旨

本件は、ASPI が実施する勉強会（A）のフォローアップ資料並びに ASPI の広報資料として、令和 7 年度 3／四半期（10 月～12 月）における計 3 回の勉強会（A）の概要をまとめるもの。

2 第 7 回勉強会（A）

- （1）日時：令和 7 年 10 月 31 日(金) 2000～2200
- （2）発表者：荒木文博（元空幕副長）スカパー-ASAT 顧問
- （3）テーマ：「宇宙領域防衛に関する考察」

*発表資料：URL（会員に提供できるよう調整中）

- （4）概要（発表項目とポイント）

ア 宇宙空間における安全保障の動向

- ・2007 年 1 月の中国による衛星破壊実験
- ・2015 年「宇宙はサイバー空間と並び国家間における戦略的競争の鍵を握る高地」（中国国防白書「中国の軍事戦略」）
- ・2017 年「陸海空並びにサイバー空間と同様、宇宙を戦闘領域と位置付ける」ゴールドフィン米空軍参謀



総長

⇒「宇宙は戦闘領域」「宇宙を制する者が戦いを制する」→①宇宙が情報優越の鍵を握る、②戦争は宇宙から始まる可能性が高い、③「宇宙での敗北」は戦争の敗北に繋がる

イ 安全保障分野における宇宙利用（イメージ）

- ・静止軌道：通信衛星、早期警戒衛星（IR）、データ中継衛星、気象衛星
- ・中高度軌道：測位衛星
- ・低高度軌道：偵察衛星（光学、SAR、SIG 等）、通信衛星（コンステレーション）
- ・シスルナ領域

ウ 宇宙空間の混雑化（スペースデブリの状況等）

- ・スペースデブリの状況（ASAT 実験等により階段状に増加）
- ・高機能の大型衛星から低軌道小型衛星コンステレーションへの転換 + 低軌道小型衛星コンステレーションの軍事利用 ⇒ 宇宙空間が混雑化（衝突のリスク大）

エ 宇宙システムに対する脅威

- ・キネティック（物理的）対宇宙兵器（衛星を直接攻撃）
- ・ノンキネティック（非物理的）対宇宙兵器（物理的に衛星に接触することなく破壊：レーザー兵器、高出力マイクロ波兵器、電磁パルス兵器）
- ・電子的（電磁的）対宇宙兵器（データの送受信無線を妨害、欺瞞）
- ・サイバー対宇宙兵器（サイバー空間を利用し、データやシステムを破壊）



・中国の脅威：直接型 ASAT、ノンキネティック ASAT、サイバー攻撃、共軌道型 ASAT

の実績

戦略支援部隊の創設（2015 年）、軍事宇宙部隊の新編(2024 年)

・ASAT 兵器の開発・配備：中国；実践 17、実践 23、中国小型 Rendezvous Spacecraft、

ロシア：Lush-2（マトリョーシカ衛星）

・宇宙における新たな脅威：北鮮「万里鏡 1 号」、露「COSMOS2553」

オ ウクライナ戦争における宇宙関連の特徴・教訓

・特徴：①初めて宇宙領域が戦闘領域になった、②初の民間宇宙戦争（商業宇宙が重要な役割を果たした）、③GPS での精密誘導・打撃

・教訓：①古典的なインテルの宇宙利用から軍事作戦の為の宇宙利用へ、②宇宙安全保障（宇宙運用）において民間宇宙能力の活用と同盟国・同志国との協力が不可欠、③宇宙システムの脆弱性に直面

カ 米国の宇宙戦略

・オバマ政権：国家安全保障戦略（宇宙が 3 つの C）

・トランプ（# 1）政権：国家宇宙戦略(2018 年)、米宇宙軍の創設(2019 年)、国防宇宙戦略・宇宙ドクトリンの策定

・バイデン政権：商業宇宙統合戦略（DOD）、米宇宙軍商業戦略

・トランプ（# 2）政権：国際協業戦略



・米軍の商業宇宙戦略

- ・米国防省商業統合戦略：商用宇宙ソリューションを国家安全保障のミッションとアーキテクチャーに統合することでレジリエンスと抑止力を強化
- ・基本原則：バランス、インターオペラビリティ、レジリエンス、責任ある行動

・米宇宙軍の国際協業戦略

- ・宇宙における優位性を獲得するため、民間企業の革新的能力、スケーラブルな生産、迅速な技術開発を活用
- ・「今あるものを活用し、買えるものは買い、作らなければならないものだけ作る」

キ 我が国の宇宙戦略

・我が国の宇宙安保政策

- ・1969 年 「宇宙の平和利用決議」（平和目的に限る、非軍事）
- ・2008 年 「宇宙基本法」成立（宇宙関連条約に従って宇宙利用を行う⇒安全保障の為の宇宙利用に道）
- ・2009 年 第一次「宇宙基本計画」策定
- ・2015 年 第三次「宇宙基本計画」策定⇒①宇宙空間の安定利用の確保、②宇宙を利用した我が国の安全保障能力の強化、③宇宙協力を通じた日米同盟等の強化

・我が国の宇宙安保戦略の体系

- ・戦略 3 文書と宇宙基本法／宇宙基本計画／行程表・宇宙技術戦略



を繋ぐもの⇒宇宙安全保障構想 + 宇宙領域防衛指針

・NSS/NDS における宇宙の位置づけ

・「宇宙空間の安全かつ安定した利用を可能とするため安全保障分野での取り組みを強化」（NSS）

・国全体の防衛体制の強化：宇宙領域

「宇宙領域は領域横断作戦遂行上、死活的に重要」⇒政府全体で能力強化（NDS）

・航空自衛隊を航空宇宙自衛隊へ（NDS）

・防衛力整備計画における宇宙

・「宇宙から情報を『つなぐ』、地上目標や HGV を『とらえる』、SDA を基盤としてサイバー攻撃を含む

妨害から自衛隊の宇宙利用を『まもる』」

・防衛省における宇宙防衛力整備

・つなぐ：情報通信システムの多層化・冗長化（抗たん性向上）

・とらえる：ターゲティング・コンステレーション構築、HGV 探知・追尾コンステレーション実証

・まもる：SDA 体制の構築、妨げる能力の強化、サイバーセキュリティ強化

・宇宙安全保障構想（令和 5 年 6 月 13 日）

・国家安全保障戦略に基づき宇宙安全保障の課題と政策を明らかにし、概ね 10 年を念頭に置いた

取り組みを明らかにし、宇宙基本計画に反映。

・宇宙空間の安定的利用と宇宙空間への自由なアクセスを維持すること为目标

・目標を達成するための 3 つのアプローチ：①宇宙安全保障の為の宇宙システムの利用、②宇宙空間



の安全かつ安定的な利用、③安全保障と宇宙産業発展の好循環

・宇宙領域防衛指針

- ・宇宙領域における防衛力強化の方向性：陸海空のオールドメインで防衛力の増幅
- ・迅速かつ的確な状況把握、作戦の基盤となる衛星通信の確保
- ・SDA と機能保障、民間企業・同盟国等との協力

・航空宇宙自衛隊（宇宙作戦集団）における任務領域の拡大

- ・宇宙状況把握（SSA）、宇宙領域把握（SDA）、宇宙作戦（Space Warfare）の三つのレベル
- ・ミッションの拡大、監視対象の拡大（SSA/SDA のレベル）
- ・日米共同作戦／多国間演習、宇宙作戦（抑止・対処・復旧）、マルチドメイン作戦（SW レベル）

ク 宇宙領域防衛態勢整備に関する考察

①迅速かつ的確な状況把握（とらえる）：スタンドオフ防衛（ターゲティング）及び IAMD（HGV ミサイルの探知・追尾）のための「センサー・タワー・シューターシステム」の構築

⇒宇宙領域からの広域・高頻度・高精度な目標情報の収集・分析（リアルタイムで移動目標を探知・追尾する衛星コンステレーションによるスタンドオフ防衛体制の確立（ターゲティング）＋極超音速滑空弾（HGV）を滑空段階でリアルタイムに探知・追尾するための衛星コンステレーションの構築（米軍との協力・相互運用性の確保）＋自律型 AI 並びにデジタルツインを用いた戦況の可視化



②作戦の基盤となる衛星通信の確保（つなぐ）：多層的な衛星通信網を整備、指揮統制及び戦術データ・リアルタイム共有のための「強靱な衛星通信アーキテクチャーの構築（光通信中継）」

⇒次期防衛通信衛星の整備＋重層的かつ耐傍受性、耐妨害性の高い衛星情報通信態勢（マルチ・オービット／マルチ・バンド）

③SDA 能力強化と機能保障（まもる）：宇宙利用の「持続性・強靱性」を確保し、自衛隊が行う各種任務を宇宙領域から支援・保証するための「宇宙領域把握（SDA）能力の向上」、「宇宙システム全体の機能保障強化」

⇒宇宙状況把握（SSA）：日本版 JCO 設置、民間力の活用＋宇宙領域把握（SDA）：自国の能力で自律的に監視・解析・評価・配布という SDA 活動が完結する体制を構築、電磁波望外監視体制の確立

⇒機能保障の強化：重要衛星に自己防御機能（レーザー等）付加、宇宙システム防護衛星（ボディガード衛星）、「きらめき」「みちびき」に対する電波妨害への対処、軌道上サービス（燃料等補給）の整備、情報保全・情報保障・サイバーセキュリティの強化、即時衛星打ち上げ態勢の確立（宇宙輸送）

④相手方の指揮統制・衛星通信等の妨げ（さまたげる）：相手方の指揮統制等を麻痺させるための「妨げる能力」の強化

⇒相手方の指揮統制・情報通信を妨げる能力の充実・強化、宇宙作戦指揮統制機能の強化

⑤その他：CSPOC への参加、Operation Olympic Defender への参加、「商業宇宙戦略」の策定、



日本版 CIC の設立、人材育成・人材確保（適格性確認制度や予備自制度の見直し）

ケ 「つなぐ」衛星通信に関する将来像（作戦地域（南西域）における衛星通信（C2）アーキテクチャの強靱化）：イメージ図

コ 「とらえる」地球観測に関する将来像：イメージ図

サ 「まもる」SSA/SDA に関する将来像：イメージ図

シ 静止軌道宇宙監視ネットワーク：イメージ図

セ JCO（統合民間 SSA セル）

- ・JCO とは
- ・JCO の基本的編成と任務拡張
- ・商業能力提供プロセス
- ・主要国の JCO の事例
- ・我が国におけるスペース・オペレーションの一案

ソ まとめ

- ・「宇宙領域を守る」という概念は？ ⇔ 宇宙から国益を守る？
- ・宇宙における「抑止」の概念
 - ・宇宙空間は地上・海上・航空と全く異なる領域 ⇔ 伝統的な「拒否的抑止」、「懲罰的抑止」が機能するかどうかは不明

.



・民間企業との連携強化

・結言

(5) 注目すべきポイント

○発表者は、現役時代、要職において航空宇宙自衛隊の創設にかかる検討・構想・施策化のプロセスに関与するとともに退官後は我が国における宇宙関連事業のリーディング・カンパニーであるスカパー-ASAT 顧問として最新の技術・情報に接する立場。

○また JAAGA 理事として米空軍・宇宙軍の交換との意見交換や部隊研修を通じて米国における宇宙領域にかかる最新の取り組みなどについて深い知見を有しており、我が国／防衛省／自衛隊における宇宙領域に関わる取り組みの現状や課題について深く知る有識者の一人。

○戦略三文書の前倒し改訂にかかる検討が始められている現状において、次の三文書に盛り込まれる宇宙領域にかかる取り組みの方向性を探るには最適の資料（現在位置と課題等を網羅）と言えよう。

(6) テーマ 2 : 「JAAGA 訪米成果報告」

ア 発表者：引田 淳（元航空教育集団司令官） 三菱商事顧問

イ 概要：細部は HP で確認



3 第 8 回勉強会 (A)

- (1) 日時：令和 7 年 11 月 27 日(木) 2000～2200
- (2) 発表者：時藤和夫（元西空副司令官）日立製作所顧問
- (3) テーマ：「最近のサイバーセキュリティの動向について～サイバー紛争国際会議（Cycon2025）に参加して～」

* 発表資料：URL（会員に提供できるよう調整中）

- (4) 概要（発表項目とポイント）：

ア ウクライナのサイバー紛争における進展、運用、革新について（Day 0）

・IT 多国籍軍（IT Coalition）

- ・2023 年、ウクライナ国防省と軍の ICT 支援と戦闘能力強化の目的でスタート
- ・エストニアとルクセンブルグが主導、18 か国が参加、10 億ユーロ以上の支援を実施
- ・支援の仕組みと課題：①共通基金（ルクセンブルグ管理）又は現物支援（再供給が必要）、② NATO 調達ルールに基づく運用（時間がかかる）、③IT とサイバー分野の重要性を政治レベルに理解させる必要

・デルタ：戦闘管理システム

- ・2016 年から開発、クラウドと市販端末を活用
- ・11 のモジュール構成：地図、AI、チャット、目標管理等
- ・前線の兵士までリアルタイムの情報共有を実現



- ・デルタの先進的機能：ドローン映像と AI による目標認識と可視化、ネプチューンミサイルとの連携（モスクワ撃破）、戦果に応じた装備支援ポイント制度

・CERT-UA の脅威報告

- ・毎日平均 17 件の攻撃に対応
- ・主な脅威：ロシア、ベラルーシ、北朝鮮、中国の APT
- ・手口：偽アプリ、メール。マルウェア、スパイフィッシング等
- ・CTI の教訓と連携：デルタや軍人を狙うマルウェア攻撃多数、ROMCOM/Gamaredon/Poji 偽装攻撃事例、情報共有と連携が不可欠

イ AI 手法の応用について：Locked Shield 演習(Day1)

・AI の攻防の構図（攻撃側と防御側に分かれた演習：Locked Shield）

- ・自動防御 AI：SOC 自動化と即応性向上、脆弱性検出・修正、ログ・トラフィック解析、レポート作成

- ・AB2F（AI-Based Battle-Net Framework）：APT 級攻撃の自動化／持続化、攻撃経路の最適化、スウォーム知識共有、Recording Angel で学習

・攻防の対比

- ・防御 AI:ブルーチーム、SOC 全体の運用、AI 活用による設定修正・ログ要約・報告生成→防御を効率化・即応化、防御資源不足を補完
- ・攻撃 AI:レッドチーム、Kill Chain 全体、AI 活用による攻撃経路の最適化・知識共有→攻撃を高



度化・継続化、大規模・持続的攻撃

・Locked Shield における検証結果

・自動防御 AI

・成果：データ収集と自動処理部分を試験、特にログ要約・サポートチケット自動対応・レポート生成で効果を発揮、演習後実データを公開し、再現性を検証可能に。

・課題：AI モデルをそのまま使うと誤検知や「幻覚」が発生、高品質データとプロンプト設計が必要、実運用で完全に人を代替するレベルには未達

・AB2F

・成果：攻撃側の演習シナリオをより継続的、リアルに実行できることを確認、情報の外部提供も開始

・課題：データの質が攻撃 AI の成果を大きく左右、オペレーターの記録や説明が十分でない場合、AI の学習に限界あり

・成果

- ・どちらが勝ったかという軍配は現時点では存在しないとの認識
- ・レッドとブルーが勝ち負けを競うのではなく両方の仕組みをテストし改善する場
- ・短期的には攻撃型 AI（AB2F）のほうが成果が出やすい
- ・長期的には防御型 AI のほうが組織的な価値は高い

ウ 安全保障の Deep Dive：ハンティングとサプライチェーンの悪用（Day2）



・エクスプロイト（悪用）とは

・脆弱性について意図しない動作を引き起こすコード／手法

・目的例：RCE、権限昇格、情報窃取

・挙動例：添付ファイル、悪性リンク、ゼロクリック

・エクスプロイトの種類：ゼロ・クリック、添付ファイル型、ブラウザ経由、ウォーターリングホール、サプライチェーン

・可視性の 3 層構造：

・ハンティングの考え方：標的から逆算、配信段階を重点監視、オペレーショナル・セキュリティを考慮、自動化パイプラインを整備

・ハンティングの事例：WinRAR（ウィンドウズ向けの圧縮解凍ソフトウェア、世界中に普及）、Outlook
ゼロクリック（メールを受信するだけで感染）、Andoroid（どのアプリを開くかを確認せず勝手に遷移）

・ウォーターリングホール：正規サイトを改ざん＋悪性コードを挿入、日次スナップショット比較で検知、複数環境でレンダリングを差分分析

・インフラ監視：TLS 証明書／メタデータ追跡、攻撃者パネルのテンプレート解析、C2 サーバ軍の特定

・サプライ・チェーンと S-Bom：S-Bom は部品リストのみ、ネイティブでは検証不可能、Java/.NET のみ一部可

・APS (Attack Path Similarity)：IOC (Indicator of Compromise) ～複合構造へ、LLVM

IR＋類似性計算、欠落ステージ補完、クラスタリングで相関発見



・課題：環境判定や URL 有効回数制限、データの不完全性、報告形式の不一致、アーキ差、AI 制

度の限界

・**推奨アクション**

・短期：自動化パイプライン、可視性向上、挙動検知

・中期：S-Bom 拡張、中心性分析、ASP 研究

・AI は補助的に活用

・**まとめ**：IOC、S-Bom だけでは不十分ではない、過信は禁物、ゼロデイは配布段階と標的の可視性から探すのが現実的、サプライチェーンが次の主戦場、攻撃パスを複合構造で扱う、自動化・研究・検証可能な AI の導入が急務

Ⅱ 進路の変化：我々はサイバー空間で何処に向かうのか（Day3）

・脅威モデルの古さ：旧来のモデル（国家・犯罪・ハクティビスト・テロ）は無効、教会が曖昧化：国家と犯罪の融合、例：露、鮮、中の二重活動

・攻撃の巧妙さとスケール：高度な進入（Bolt Typhoon）、愛国的ハクティビズムの増加、ツール商品化に伴う参入障壁の低下

・民間企業の活用と競争の加速：I-soon リーク（中国のサイバーセキュリティ企業で、表向きは「脆弱性研究」「セキュリティサービス」を提供する民間企業）で明らかに、国家が複数企業に案件を発注、企業間で国家契約を競争

・国家と犯罪のバランス：国家脅威に偏重、犯罪対応が弱い、市民・中小企業・病院が被害、法執行



機関の予算不足、提案：法執行強化、国民全体保護

・サイバー抑止力の限界：抑止は敵のリスク計算を変えず、攻撃的行動と非サイバー手段が必要、経済

制裁・ビザ制限・事業活動制限

・**中国の4つの「S」**：Sophistication（洗練性）、Scale（規模）、Stealth（秘匿性）、

Strategy（戦略性）が限界点を越えて加速中

・総括

- ・攻撃者の分類はもはや不可能
- ・サイロ的思考では主導権を失う
- ・国家手段と非サイバー手段を総合活用
- ・今こそ「共に行動」するとき

オ 防衛戦略における次の一步：AI とサイバー脅威情報（Day3）

・観測された主な方向性

- ・ゼロデイ脆弱性の悪用増加
- ・NK「DPRK IT ワーカー」作戦（北朝鮮の外貨獲得のための国家主導の IT 活動、国籍を隠して海外 IT 企業にリモートで就職）
- ・可視性のギャップを突いた攻撃（防御側が感知・検知しにくい領域を攻撃者が付く戦術）
- ・生成 AI の悪用進行中

・**AI を悪用する攻撃者達（Google の観測）**：APT（国家支援型、中国系 APT、イラン系



(APT42 等)、DPRK、ロシア系、その他、金銭目的の犯罪者、情報操作 (IO) グループ

・APT の利用実態

- ・イラン：フィッシング文案、防衛調査、レッド・チーミング
- ・中国：IP 調査、ポスト侵害スクリプト、逆解析
- ・北朝鮮：政治・核政策調査、履歴書作成、IT ワーカー作成
- ・ロシア：IO 利用が中心、偽ニュース・翻訳

・Google の防御戦略 (ディスラプション・ミッション)

⇒ 悪意ある URL や Gmail アカウントをブロック、Gdrive や C2 利用の封じ込め、IOC やプレイブック
の共有、政府・民間・学術との連携

・AI による防御側のメリット：①インシデント対応レポートの自動要約、②脅威アトリビューション支援、③
マルウェア初期解析支援、④大規模ドメイン監視とフィルタリング

・次のステップ：「知る」から「止める」へ

- ・防御側が能動的に行動し、攻撃を実際に阻止して成果を出すフェースに移行すること
- ・攻撃の実行を妨害する／インシデントを即時に抑制する／政府・民間・法執行が協働して「攻撃インフ
ラ」を潰す／AI を活用して防御効率を高め、成果を可視化する

・プラットフォーム上に整備する各種機能

- ・状況可視化機能、訓練及びミッションリハーサル機能 (AI・デジタルツイン)
- ・後方補給ネットワークシステム



・戦傷医療情報の共有システム

⇔ 人材確保、官民連携、同盟国・同志国との連携

・まとめ

・実践が理論を凌駕

・予防措置に対して、対処とその実践の重要性が増加

・対量子暗号対策（PQC）も具体的な段階

・AI 活用は必須であり、早期の戦力化が必要

（5）注目すべきポイント

○サイバーセキュリティに関する有識者の一人である発表者（時藤氏）が毎年参加しているサイバー紛争国際会議（Cycon2025：エストニア・タリンで開催）における議論のポイントなどについて説明するもの。

○Cycon は、サイバースペースとその社会への影響に関連する技術的、政策的、法律的、軍事的な最重要課題について、最新の研究を紹介し議論を促進する学際的会議であると同時にコミュニティ形成イベントとして地位を確立している。

○今回のテーマは「次の一步」。サイバー空間は武力紛争の閾値を下回る活動の舞台となり、防御的サイバー作戦と攻撃的サイバー作戦の境界線、平時、危機、紛争の境界線も曖昧になっている。活動主体はかつてないほど多様化し、その意図も大きく異なっている。ゲームのルールが常に進化している時、政治家や意思決定者、産業界、弁護士、技術的先駆者はどのように適合化していくのかが問われている状況。

○ウクライナにおける実践を通じて目まぐるしく変化・進展を遂げるサイバー領域における戦いの現状や最新



の動向を理解する上で極めて貴重な内容。

(6) テーマ 2：戦略 3 文書の見直し改訂に向けて（その 1）

ア 発表者：荒木淳一（元航空教育集団司令官）川崎重工顧問

イ 概要：細部は HP で確認



4 第 9 回勉強会 (A)

(1) 日時：令和 7 年 12 月 26 日(金) 2000～2200

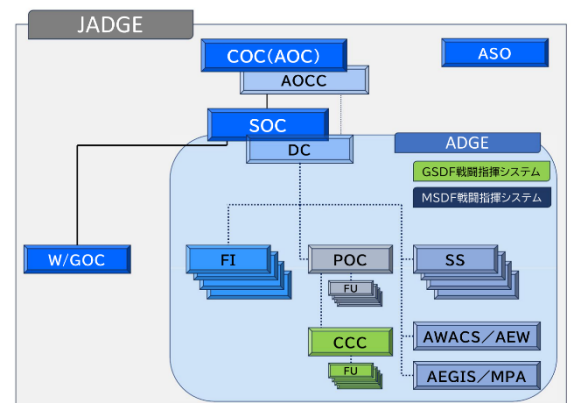
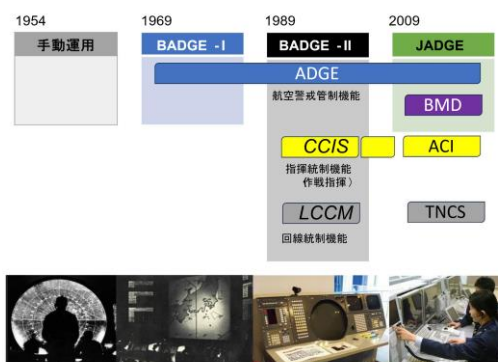
(2) 発表者：金古真一（元支援集団司令官）東芝顧問

(3) テーマ：「空自 C4 システムの変遷と一考察」

* 発表資料：URL（会員に提供できるよう調整中）

(4) 概要（発表項目とポイント）

ア 手動運用の時代から JADGE へ



JADGE における方面隊司令部以下の C2 系統

ウ 警戒管制機能（ADGE）の変遷

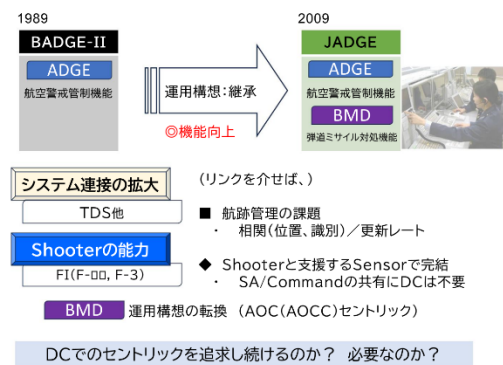
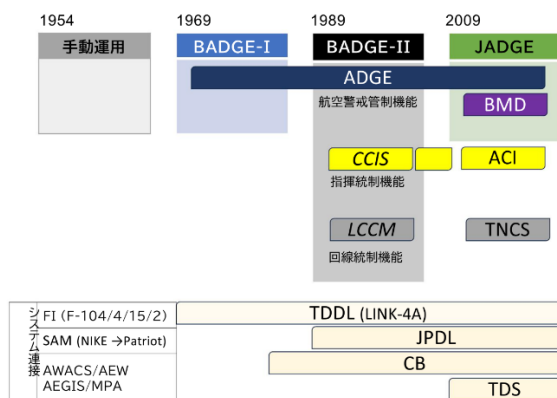
（BADGE- I ～BADGE- II）

エ 警戒管制機能（ADGE）の変遷

（手動運用～BADGE- I）



オ 警戒管制機能 (ADGE) の変遷 (BADGE-II ~ JADGE)



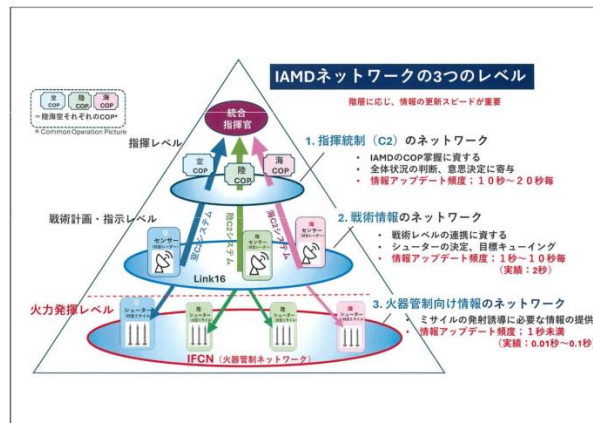
カ 次世代 JADGE (イメージ)

キ IAMD ネットワークと3つのレベル

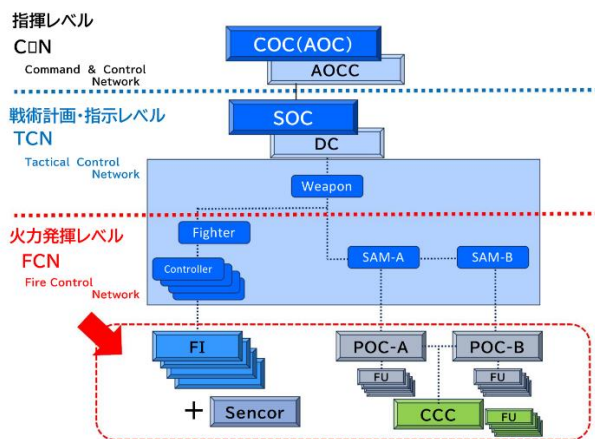


次世代JADGE(仮称) (イメージ)

防衛力抜本的強化の進捗と予算・令和0年度概算要求の概要ー



ク 総隊 (COC) 以下の C2 系統



ケ 作戦現況図の管理と作戦思想の統一

分散 = フラットな関係 “No Organaizer”
→ AI “For What?”

SA (Common Picture+Action (Detect, L/O, Shoot, KILL))共有
+ 戦闘(射撃)協調だけで十分なのか?

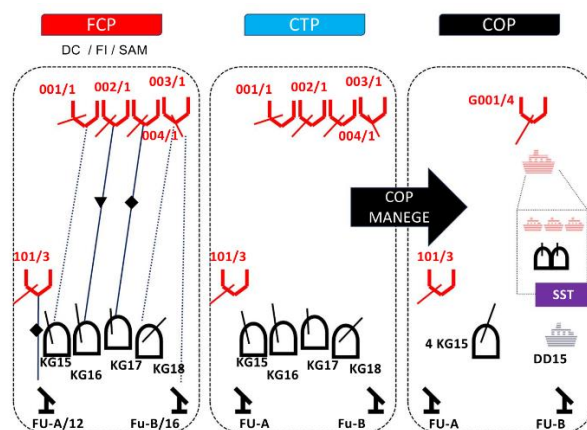
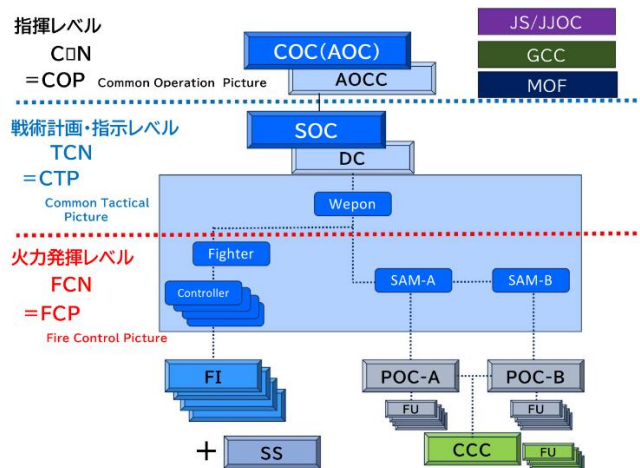
作戦現況図の管理

- 航路管理のコンフリクト
 - 許容する → Double Assign
 - 識別はShooterのみ
- 共有図
 - CTP/COPとはなり得ない? (情報量過多→not for 指揮官)

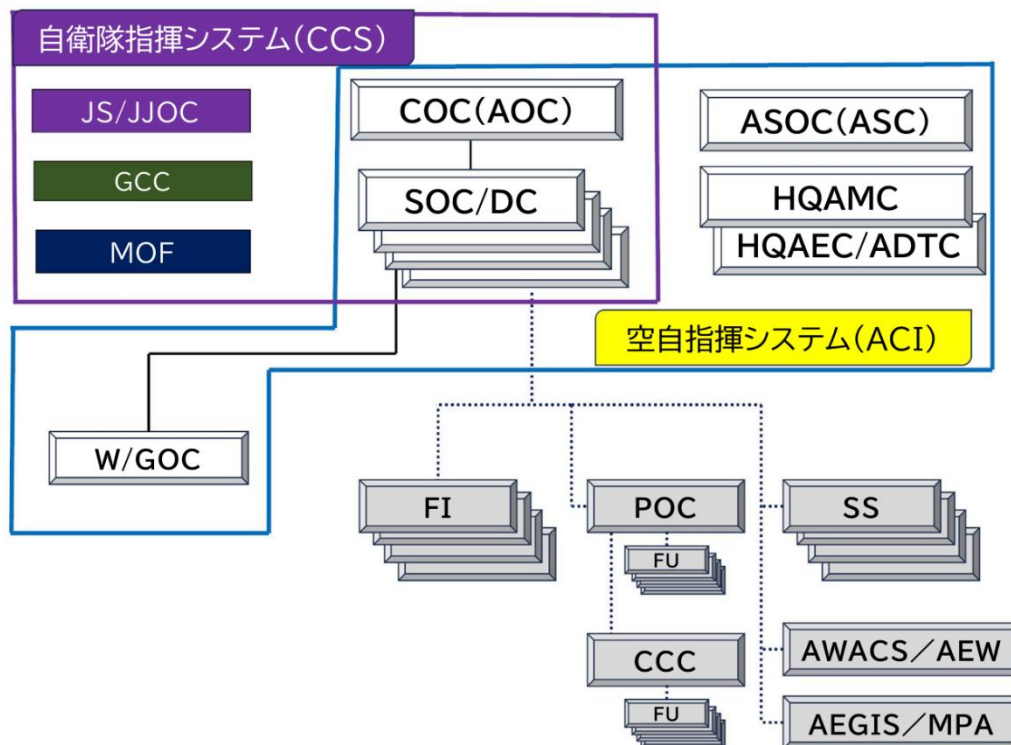
作戦(not戦術)思想の統一

- 作戦全体のデザインは、誰が? AIがCommander?
 - AIの活用は、
 - ・ 戦術面での優先度判断(◎)
 - ・ Shooter同士の協調(◎)
 - 作戦指揮(システムを含む)との関係は?

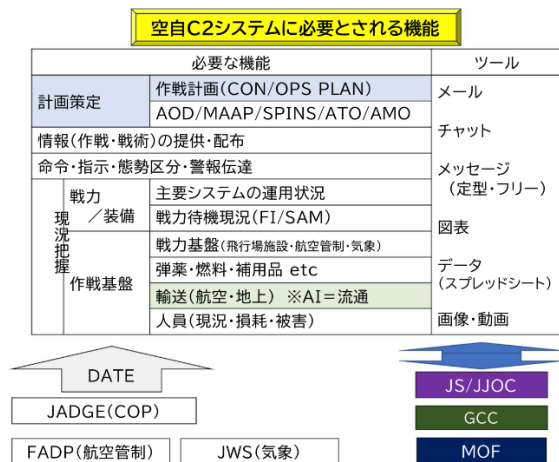
コ 火力発揮／戦術計画・指示／作戦指揮



サ 自衛隊指揮システム（CCS）と空自指揮システム（ACI）の関係



シ 空自 C2 システムに必要とされる機能 ス 計画・命令作成に AI（生成）の活用



計画・命令作成へのAI(生成)活用

■ 各種計画・命令策定プロセス

- ➔ 指揮官と幕僚のコミュニケーション
- ➔ 指揮官は、意図・企図を幕僚に言語で伝え、プロダクト(計画・命令)を文字化、図式化
- ➔ コミュニケーションでは、作戦関連の共通の言語(認識)使用



- 生成AIに作戦計画に関連する共通のTERM(軍事用語・略語)、繰り返し考えさせれば(プロンプト必須)
文字化・図式化された作戦計画・命令を作成できるのでは
「幕僚を PowerPoint Ranger」から解放する」

(5) 注目すべきポイント

○要撃管制幹部として空自の作戦運用の現場レベルを経験してきた発表者（金古氏）が、その後の方面隊司令官、総隊副司令官、航空支援集団司令官等の要職における経験を通じて、空自の指揮統制の基本的な考え方について BADGE や JADGE というシステムの変遷を辿りながら総括したもの。

○防衛力の抜本的強化の 7 つの柱である「領域横断作戦能力」「指揮統制・情報関連機能」のあり方について考える上で、防空作戦を中心に構築されてきた空自の C2 系統の基本的な考え方を整理・理解することは極めて重要。

○今回の内容を、第 5 回勉強会（A）「統合防空ミサイル防空（IAMD）」、第 6 回勉強会（A）「AI による意思決定支援システムー 防衛省 IAMD 構想と米国 JADC2 の概要と MSS—Japan の開発提言」と併せて再読することも、IAMD 構想における C2 系統のあり方や日米共同における新たな C2 系統のあり方を考える上で有益。

(6) テーマ 2：下里水路観測所研修(衛星の軌道精密計測にかかる情報提供



ア 紹介者：斎藤英明

イ 概要：細部は HP で確認

(7) テーマ 3：戦略 3 文書の見直し改訂に向けて（その 2）

ア 発表者：荒木淳一（元教育集団司令官）川崎重工顧問

イ 概要：細部は H P で確認