令和 8 年度 2／四半期の勉強会（A）の概要について

令和 8 年 11 月 1 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 8 年度 2／四半期（7 月～9 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 4 回勉強会（A）

（1）日時：令和 8 年 7 月 23 日(木)　2000～2200

（2）発表者：齋藤英明（元電子装備研究所所長）一般財団法人 防衛技術協会 客員研究員

（3）テーマ：「**ドローン・スォーム戦闘の簡単なシミュレーション（ウクライナ迎撃戦闘を念頭に）**」＊発表資料：URL（会員に提供できるよう調整中）

（4）概要

ア　要約

本発表は、ウクライナでのドローン脅威に対する迎撃戦を念頭に、まず簡単なシミュレーションを用いて、ドローン同士の戦闘では速度や探知性能などの優位性が勝敗に大きく影響することを示した。次に、イラン製ドローン「Shahed-136」を例に、物理モデルを用いた性能分析と、その高速化版「Shahed-238」や迎撃ドローン「P-13」との戦闘シミュレーション結果が提示された。P-1 SUN は Shahed-136 には有効だ

が、Shahed-238 には対抗困難であること、またスワーム攻撃に対しては事前にドローンを周回させておくパトロール迎撃が有効であることが示された。さらに、スワーム攻撃では「単位時間あたりの攻撃密度」が本質であると指摘し、これに対抗する多層防空システム（SAM、CIWS、迎撃ドローン）の迎撃シミュレーションとコスト分析を実施した。

結論として、SAM のような高価な兵器よりも、低コストの迎撃ドローンを大量に運用する方がコスト効率に優れる可能性を提示した。質疑応答では、日本の防衛における中国のスワーム攻撃への対応、アジャイルな研究開発・調達の必要性、産官コンソーシアムによる量産体制の構築、ミサイルとドローンを組み合わせたハイブリッド攻撃への対処など、多角的な議論が交わされた。最後に、今後の勉強会やイベントの予定、関連研究の動向などが共有された。

イ　ドローンスワーム戦闘のシミュレーションと分析

➢ **ドローンスワーム戦闘の基本モデル**

- スワーム対スワームの攻防では、同数であっても速度差、攻撃パターン、探知性能差が迎撃の成否に大きく影響する。
- 簡単な数学モデルによるシミュレーションでは、迎撃側が攻撃側と同等の性能では迎撃に失敗し、2 倍の速度を持つ場合でも完全な撃破は困難であることが示された。⇒攻撃側の優位性を実証
- 事前に迎撃側が哨戒パトロールを行うことで、迎撃成功率が向上する。
- 今後の課題として、シミュレーションの高精度化や AI 導入による迎撃方法の解明が挙げられた。

➢ **攻撃ドローン（Shahed）の性能と運用モデル**

・ イラン製ドローン「Shahed-136」は、低価格の長距離巡航ミサイルとして大きな脅威であり、ロシアによって改良も進められている。

・ 物理モデルを用いた性能検討では、公開情報（航続距離 1400～2500km）を再現するには、燃料消費率や空力特性などのパラメータ調整が必要であることが示された。

・ 最適な巡航条件（約 76m/s）で飛行すれば、航続距離 2110km が達成可能と推定される。

・ 誘導方式は、コストを抑えた商用グレードの INS と GNSS のハイブリッド方式と推測され、CEP（着弾誤差）は数十から数百メートル程度で十分とされる。

➢ **スウォーム攻撃の統計的モデル**

・ スウォーム攻撃の本質は機体の総数ではなく「単位時間あたりの攻撃密度」である。

・ 発射時刻のばらつきや飛行経路差により目標への到達時間にばらつきが生じるため、これをヒストグラムでモデル化し、防空側の対処能力（MEW：単位時間あたりの最大迎撃可能機数）と比較することで飽和攻撃の成否を判定することが可能となる。

ウ　迎撃システムとシミュレーション

➢ **迎撃ドローンの開発と運用（ウクライナ事例）**

・ ウクライナは攻撃ドローンに対抗するため、「P-1 SUN」など極端な低コスト・高機動を特徴とする迎撃専用ドローンを大量に開発・運用している。

・ 迎撃方法は体当たりや自爆攻撃で、AI 支援による半自動化も進んでいる。

・ 攻撃ドローンの高速化（例：Shahed-238）に対応するため、ジェット推進型や空中発射型

の開発も試みられている。

➢ **シャヘドの探知と迎撃**

・ Shahed-136 は RCS が極めて小さくレーダー探知が困難なため、音響センサーや赤外線カメラ等を統合したセンサーネットワーク「デルタ」が有効活用されている。

・ P-1 SUN による迎撃シミュレーションでは、低速で直進的な Shahed-136 に対しては撃墜率 100%を達成したが、高速な Shahed-238 には追いつけず、撃墜率は 50%に留まった。

➢ **多層防空システムの迎撃シミュレーション**

・ 長距離 SAM、中・短距離 SAM、CIWS による多層防空システムをモデル化し、200 機の UAV による攻撃をシミュレーション。

・ 結果、突破機数は 9 機（突破率 4.5%）となり、多層防空は非常に効果的であることが示された。

➢ **パトロール迎撃の有効性**

・ 攻撃を受けてから迎撃ドローンを発進させるシナリオでは迎撃が間に合わず、攻撃側の 4 割が目標に到達した。

・ 事前に迎撃ドローンを目標周囲で周回（パトロール）させておくパターンでは、迎撃成功率が大幅に向上することが示された。

エ　コスト解析と多層防御のあり方

➢ **迎撃手段のコスト比較**

・ 200 機のスウォーム攻撃に対し、SAM のみでは突破率 68%、迎撃ドローンのみでは突破率 20%となった。

・ SAM と迎撃ドローンのハイブリッド運用では、突破率を 6.4%まで抑えられ、コストと効果のバランスが取れることが示された。

・ 一方、コストと突破率を最小化する数学的な最適解を求めると「SAM は不要で、全て迎撃ドローンで対処するのが最も効率的」という結果も得られた（SAM・ドローンハイブリッド運用と同予算で 16,000 機の迎撃ドローンが購入可能）。

➢ **ハイブリッド型脅威と多層防御**

・ 現実にはドローンだけでなく、弾道ミサイル（BM）や巡航ミサイル（CM）との複合攻撃が想定される。ドローンは亜音速レベルの CM まで対処可能だが、超音速以上のミサイルには対応できない。

・ ドローン対ドローンだけでなく、キネティック兵器（ミサイル等）とノンキネティック兵器（レーザー、EW）、消極防御を組み合わせた総合的な迎撃システムの構築が必要である。

・ レーザーや EW はスウォーム攻撃のような多数の目標への同時対応が困難な場合があり、**兵器特性を理解した上でのコンセプト構築が急務**である。

オ　日本の防衛への示唆と課題

➢ **日本の課題とアプローチ**

・ 日本が直面するであろう**中国によるスウォーム攻撃への対応が優先課題**であり、**固定レーダーサ**

イト等の防衛について具体的な検討が必要である。

・ 防衛装備庁が 2026 年 7 月 15 日から開始した迎撃ドローンの早期取得プログラムは評価されるが、ドローン技術の進展速度を考えると、アジャイルな研究開発・調達制度の検証と継続的な投資が不可欠である。

➢ **生産体制と産官連携**

・ 本格的なドローン戦には年間数十万台規模の生産能力が必要であり、単発の調達では産業基盤の維持が困難である。

・ 防衛省と民間企業（ベンチャー含む）がコンソーシアムを形成し、継続的な試作・生産ラインを共同で維持・発展させていくべきである。

・ 3D プリンター等を活用した安価なミサイルの大量生産も視野に入れるべきである。

➢ **ミッションエンジニアリングとデータ活用**

・ 膨大な目標を処理するターゲティングや資源配分（兵器割当）の問題に対し、民生の物流管理システム（例：日立・アマゾン）のノウハウが参考になる可能性がある。

・ キルチェーンだけでなくサプライチェーンも含め、ミッションエンジニアリングによる定量的解析を浸透させることが重要である。

（5）注目すべきポイント

〇発表者は、元電子装備研究所所長であり、退官後、MELCO において様々な装備品の開発・実装化に関与した技術者であり、幅広い知見を有する実務研究者である。その発表者がロシア・ウクライナ戦争

で着目されるドローン脅威に対する迎撃システムに関してシミュレーション基本モデルを作成し、それを通じたコスト解析の結果から、我が国におけるスウォーム攻撃に対する迎撃システムに関する示唆を提示していることの意義は極めて大きい。

○基本モデルでは、速度差、攻撃パターン、探知性能の差が迎撃成否を左右すること、同等の性能の場合、攻撃側が有利であること等が示されている。その上でイラン製ドローン「Shahed-136」と、長距離 SAM、中・短距離 SAM、CIWS による多層防空システムをモデル化したシミュレーションの結果として、多層防衛の有効性、パトロール迎撃の有効性を示していることは示唆に富む。

○また迎撃システムのコスト比較を通じて、ハイブリッド型脅威に対してはキネティック兵器（ミサイル等）とノンキネティック兵器（レーザー、EW）、消極防御を組み合わせた総合的な迎撃システムの構築の必要性と兵器特性を理解した上での**運用コンセプト構築が急務**であることを指摘している。

○最後に日本に対する示唆として、１）中国によるスウォーム攻撃への対応が優先課題であり、**固定レーダーサイト等の防衛について具体的な検討が必要**であること、２）産官学の連携と生産体制の構築の必要性、３）**データを活用したミッションエンジニアリングによる定量的解析の重要性**を指摘していることは極めて重要である。

3　第 5 回勉強会（A）

（1）日時：令和 8 年月 31 日(月)　2000～2200

（2）発表者：時藤和夫（元中空副司令官）日立製作所（株）顧問

（3）ﾃｰﾏ：「**最近のサイバーセキュリティの動向**」

＊発表資料：URL（会員に提供できるよう調整中）

（4）　概要

ア　要約

発表者が参加した 2026 年の国際会議「CyCon（サイバーコンフリクトカンファレンス）」の内容を踏まえ、最近のサイバーセキュリティ、特に AI（エージェンティック AI）の活用と現代戦におけるその役割について多角的に解説したもの。

ウクライナでの教訓を基に、サイバー作戦は単発の攻撃ではなく、偵察から戦果評価までを含む継続的なキャンペーンとして「総合戦」に統合されるべきだと強調された。その中核となるのが、ウクライナが開発した統合状況認識プラットフォーム「Delta（デルタ）」であり、本講義ではその設計思想、主要モジュール、AI 活用法、人間中心のセキュリティ設計について詳述された。

結論として、技術導入だけでは意思決定の優位性は得られず、「デジタル戦場（Digital Warfare）」「戦場認識・意思決定システム（DELTA）」「エージェント AI（Agentic AI）」という 3 要素を一つの連鎖として理解し、運用（オペレーション）面やレッドチームによる批判的評価、組織の実行速度（スピード）を重視した実践的アプローチが不可欠であると強調された。

また、AI 導入に伴うリソース不足（GPU、電力）、攻撃対象領域（アタックサーフェス）の拡大、官民連携によるエコシステム構築の必要性など、現実的な課題も論じられた。

イ　国際会議「CyCon」とサイバー作戦の最新動向

- **CyCon（サイバーコンフリクトカンファレンス）の概要:** エストニアで毎年開催される NATO CCDCOE 主催の国際会議。2026 年のテーマは「Securing tomorrow」で、ウクライナでのサイバー戦の教訓と AI 技術の活用が主要テーマとなった。
- **サイバー作戦の統合と「総合戦」アプローチ:**
  - サイバーは偵察、目標選定、作戦支援、戦果評価へ統合され、前線作戦の構成要素と認識されている。
  - 単発のサイバーストライクは効果が薄く、敵の作戦コストを恒常的に高める継続的キャンペーンが重要。
  - サイバー能力は保有するだけでは価値が劣化する「在庫ではない能力」であり、実戦・運用を通じた継続的な経験でのみ維持・向上する。
- **AI 導入と運用の重要性:** 技術導入だけでは意思決定は優位にならず、データ整備、現場での実用性、権限者の判断、安全な実行と学習といった「運用（オペレーション）」面が極めて重要。

ウ　ウクライナの統合プラットフォーム「Delta（デルタ）」

- **基本概念と設計思想:**
  - 状況認識を中心とした統合プラットフォームであり、単一システムではなく **70 以上の外部システムと連**

接する「エコシステム」として機能。

- 人間中心の設計、データ駆動型の意思決定、AI による継続的改善を統合。
- オープンソースを主体に開発され、環境適応型（その国の環境に合わせて作り込む）の導入哲学を持つ。

➢ **主要モジュールと機能:**

- 共通状況認識マップ: 戦場をデジタルマップ上に可視化。
- 映像分析・AI 画像認識モジュール: ドローン映像等から目標を自動識別。実戦映像を学習データとしており高精度。
- その他: ターゲット管理、インテリジェンス分析、ビジネスインテリジェンス等のモジュールで構成。
- これらのモジュールが閉ループ（クローズドループ）で接続されることで価値を創出する。

➢ **AI 活用と人間の役割:**

- AI は目標認識や状況分析に集中投入されるが、最終的な攻撃判断（射撃統制）は別システムに分離され、人間に委ねられている。
- 人間の認知的負荷を低減し、素早い意思決定を促す支援に重心がある。

➢ **ヒューマンセントリックセキュリティとレジリエンス:**

- **前線の極限状態にある利用者を前提**とし、安全な操作を最も簡単な操作で実現する設計を最優先。
- GPS 妨害、電子戦、物理攻撃などを組み合わせた複合脅威を前提に設計されており、高いレジリ

エンスを持つ。

- **ゲーミフィケーション事例:** 戦果を上げた部隊にポイントを付与し、新しい装備品と交換できる機能があり、兵士の士気向上に貢献している。

エ　フロンティア AI とエージェンティック AI（Agentic AI）

- **AI の進化**: 生成型 AI から、推論・行動・ツール使用・記憶・自己改善を行う「**エージェンティック AI**」へトレンドが移行。
- **エージェント運用のプロセス:** 目標設定、計画立案、ツール使用、メモリ参照、結果検証、環境変化の確認、次アクション決定といった手順を踏む。権限、承認、停止、監査、ロールバックの整理が重要。
- **オペレーショナルニーズとの関係:** 継続的キャンペーン運用や短い意思決定サイクルを支えるため、大量・異種のデータを処理する必要があり、そのバックログ解消にエージェンティック AI の活用が期待される。
- **実務的課題と人間の役割:**
  - 現状では AI に「うまく使われる」ことが多く、使いこなしには習熟と継続的改善が不可欠。
  - 人間が運用設計や業務プロセスの分割、最終責任を担い、AI を「使う」ことで意思決定を加速・質的向上をさせるハイブリッドアプローチが現実的。
  - AI のアクセス権管理（NHI: ノーティーマン ID）や、人間がいつでも介入できる仕組みの確保が重要。

オ　AI 導入に伴うリスクと対策

- **攻撃対象領域（アタックサーフェス）の拡大**:

- AI 特有の脆弱性（プロンプトインジェクション等）や AI 間連携の脆弱性が新たな脅威となる。
- OWASP は 2026 年の重大リスクとして「ゴールハイジャック」「AI サプライチェーン汚染」「人間-エージェント間の信頼乗っ取り」等を指摘。

➢ **リソース課題:** 高性能 AI の運用は、GPU の発熱や電力消費といった物理的なインフラ制約を伴う。データセンターの立地や電力供給が社会問題化する可能性もある。

➢ **対策としてのレッドチームと多層防御:**

- レッドチーム（攻撃側視点）による継続的な評価・演習を改善ループに組み込み、システムの**脆弱性を発見・修正することが不可欠。**
- AI の判断だけに依存せず、多層的な条件付けや検証措置を講じる「Defense in Depth」の考え方が重要。

カ　日本の安全保障への示唆と政策提言

➢ **米国の意思決定優位戦略**: 情報・任務の優越、全領域の即応化を目標に「スピード」を重視する戦略が潮流。

➢ **日本への提言:**

- 政策への接続: 国家防衛戦略への AI 活用明記の具体化と実装。
- 組織の処理速度向上: 技術を活用し、組織がボトルネックにならない体制を構築。
- パイロット検証: システム間連携における認知の一致や相関分析を「組織機関の検証」として実施。

（５）第 2 テーマ：四団体による令和八年度政策提言:

- 構成：陸修会、水交会、つばさ会、大遊会の自衛隊 OB 団体が共同作成。
- **提言の柱：**
  - 憲法改正：自衛権の明記や軍事司法制度の整備。
  - 軍事組織への変革と隊員の名誉・誇り：事務曹階級の新設、天皇陛下への拝謁機会の再開、英霊顕彰制度の整備。
  - 退職者（OB）の有効活用：セキュリティ・クリアランス制度を通じた現役との連携強化。
  - 防衛力のさらなる強化：太平洋正面の防衛体制整備、スタンドオフ能力の向上、弾薬のライフサイクル管理。
  - 新領域への対応：無人アセット導入のための法制度（道路交通法、航空法等）の見直しと訓練環境の確保。
  - 人的政策と処遇改善：入隊後の優遇措置、退職後の生活保障、多様な勤務形態（パートタイム制等）の導入。
  - 防衛生産技術基盤の強化：政府主導による防衛産業戦略の策定。
  - 国際協力：日米同盟の進化と、OB 団体を活用した台湾との関係構築。

（5）注目すべきポイント

〇発表者は、元統幕 J-6 部長を始め C4I、サイバー分野の要職に就いたのみならず、退職後もサイバー専門家として所属する日立製作所において、幅広く様々な立場でサイバー関連で活躍する実務者であり、研究者でもある

○ウクライナ戦争の教訓をベースにサイバー戦が総合的な戦いの一部となっていること、ウクライナで実装されている統合プラットフォーム「デルタ」の概要を紹介していること、その中で人間中心のアプローチが維持されていること等、示唆に富む。

○ウクライナの統合プラットフォームである「デルタ」の基本設計思想、主要モジュールと機能、AI 活用における人間の役割や戦闘と言う極限状態にある人間の特性を踏まえた使い方やシステム設計が行われていることは重要な指摘である。また、生成 AI からエージェンティック AI に進化しつつあること、その運用プロセスや運用要求との関係、人間の役割と実務的な課題を明らかにしている点も重要である。

○最終的に、日本の安全保障への示唆と政策提言に言及していることは、ASPI の設立趣旨に沿うものであり、現役に対しても大いに役立つ研究・報告内容となっている。

4　第 6 回勉強会（A）

（１）日時：令和 8 年 9 月 29 日(火)　2000～2200

（２）発表者：渡辺秀明（元装備庁長官）一般財団法人・防衛技術協会　理事長

（３）ﾃｰﾏ：「**進化する装備品に向けて-サイバーセキュリティ対策とアジャイル開発の両立-**」＊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　要約

防衛装備品の開発・調達における「モジュール化・オープンアーキテクチャ（MOSA）」と「サイバーセキュリティ（SBOM/RMF）」の両立が、日本の喫緊の課題であることが強調された。講演者や参加者は、米国や韓国、ウクライナの事例を基に、日本の現状の課題（官民の連携不足、国際標準からの遅れ、ベンダーロック問題など）が指摘された。解決策として、無人機分野からの段階的導入、官主導のインテグレーション、デジタルツインの活用、国際協力、そして国内の重要インフラ防衛に関する法整備と官民連携の必要性が認識・共有された。

技術的な議論を経て、防衛装備品のソフトウェア化、オープンアーキテクチャ（MOSA/WSA）化、ソフトウェア部品表（SBOM）の整備、リスクマネジメントフレームワーク（RMF）の重要性、そしてアムラーム・ミサイルの進化事例などが解説された。実戦経験がない日本での開発サイクルの確立方法や、国際標準化からの遅れと回復法、官民連携のあり方など、複数の参加者から多角的な問題提起と意見交換が行われた。

イ　ソフトウェア化とセキュリティの課題:

・　防衛装備品はソフトウェア比率の増大により、アジャイルな能力向上が可能になる一方、脆弱性リスクも増大。

・　セキュリティ確保には RMF（リスクマネジメントフレームワーク）と SBOM（ソフトウェア部品表）の併用が不可欠だが、日本の SBOM 導入は遅れている。

ウ　オープン化（MOSA）の重要性と課題:

・　MOSA/WSA に基づくオープンなインターフェース標準化は、モジュール単位での更新や第三者（スタートアップ等）参入を可能にし、ベンダーロックを緩和する。

・　しかし、インターフェースの統合管理が難しく、攻撃対象領域を広げるリスクもあるため、セキュリティ対策との両立が不可欠。

エ　国際動向と日本の遅れ:

・　米国はドローンのセキュリティ基準「Blue/Green UAS」を策定し、韓国や台湾は政府主導で迅速に対応しているが、日本は基準策定で後れを取り、国際市場から孤立（ガラパゴス化）する危険性が指摘されている。

・　韓国は輸出を通じて装備品の能力進化を加速させている。

オ　ウクライナ紛争の教訓:

・　ウクライナでは、戦況に応じてドローンのモジュールを数週間単位で交換・改良するアジャイルな開発が実践されており、実践駆動の継続的進化が有効であることを示している。

カ　日本の現状と進むべき道:

- 日本では官庁と企業が互いに様子見をする「待ち」の構図が停滞を生んでいる。実戦経験の不足を補うため、デジタルツインの活用、他国との共同開発・演習への参加が重要。
- まずはレガシーシステムとのしがらみがない無人機分野から国際標準に準拠した基準を導入し、官がインテグレーター役を担うべき。

キ　重要インフラ防衛の必要性:

- 自衛隊だけでなく、法整備を通じて民間企業が自らの重要インフラを防衛できる体制を整える必要があり、これは NATO などでも進む潮流である。

ク　日本の課題と具体的な進め方に関する議論（質疑応答の概要）

- 実戦経験の欠如をどう補うか: デジタルツインの活用、韓国など他国との協力、米国の訓練視察、重要インフラ防衛に関する法整備と官民連携などが解決策として提示された。
- 更新トリガーの設計: 平時が長い日本ではモジュール更新が進まない懸念が指摘され、国際的な議論や共同開発を通じて装備方針を更新していく必要性が論じられた。
- 官民の役割分担とリーダーシップ: 官がインテグレーター役を主導し、メーカー間の利害を調整する必要性を指摘。官と企業が互いに様子見をする「待ち」の構図を打破するため、政策による明確な「旗振り」が求められた。
- 技術的課題: モジュール間のインターフェース非互換がボトルネックになる懸念が示され、短期的には能力向上を優先しつつ、長期的には AI の活用も視野に入れた標準化を目指すべきとの見解が示

された。

・　総括と今後の活動：アジャイルとセキュリティの両立は可能であり、国産技術の継続的アップデートの重要性を改めて強調。クローズドな場での深い対話の意義を確認。

（5）注目すべきポイント

〇発表者は元装備庁長官であり、本テーマに関して深い知見を有する実務者であるが、最近渡米し現地で専門家と意見交換した内容について会員と共有したものである。

〇アジャイルな開発が求められる中でどのようにセキュリティを確保するか、その為の基準・標準となる制度は何かについて、現在の最新の議論に関して紹介されている。防衛装備品のソフトウェア化、オープンアーキテクチャ（MOSA/WSA）化、ソフトウェア部品表（SBOM）の整備、リスクマネジメントフレームワーク（RMF）の重要性が指摘されている。

〇ウクライナの教訓を踏まえ日本の現状と課題を提示した上で、進むべき道や重要インフラ防衛の重要性が指摘されている。

〇また、質疑応答では様々な角度からの意見が提示され、質疑応答を通じてより多角的な議論と理解に繋がったことが確認できる。