進化し続ける防衛装備品へ

国産装備品の競争力を支えるソフトウェア時代の制度基盤

SBOM・RMF・MOSAを「三者一体＋DevSecOps」で運用する



2026年5月

防衛技術協会
渡辺秀明

進化の系譜 — ハードウェアから「空飛ぶコンピュータ」への価値の移行

世代を追うごとに機体の価値重心は物理的構造から電子・ソフトウェアへ移行。現在はソフトウェアの統合そのものが能力向上の最大のボトルネックとなっている。

Generational X-ray Matrix



第3世代 (1960年代〜 / F-4等)

約15%

電子・ミッションシステム比率

搭載ソフトウェア規模：約1,000行

特性：価値の源泉は空力性能と推進力（ハードウェア中心）。



第4世代 (1980年代〜 / F-16等)

約30%

電子・ミッションシステム比率

搭載ソフトウェア規模：数十万行

特性：アビオニクス統合の開始。機能の約45%をソフトウェアが担う。



第5世代 (現代 / F-35)

約50%

電子・ミッションシステム比率

搭載ソフトウェア規模：800万行超

特性：アビオニクス仕様要求の90%がソフトウェアに依存する「空飛ぶコンピュータ」。

⚠ F-35の現在地：10年前の実績機と現在の課題

F-35は2015〜2016年に初期作戦能力（IOC）を獲得した「約10年前の実績機」である。現在はTR-3をはじめとする大規模なハード・ソフト統合更新フェーズにある。2024年の納入遅延（約19億ドル規模の改修）が象徴する通り、能力向上のボトルネックと開発リスクは完全にソフトウェアへ移行している。

現代の戦場 ― 無人機（UAS）におけるSoftware-Definedの常態化

近未来ではない。ウクライナ戦等で数週間サイクルのソフトウェア更新が勝敗を決する「現在進行形の現実」。
機体は価値の「容れ物」へとコモディティ化している。

ウクライナにおける戦訓

新たな航法・管制方式の有効性は約2週間でピークに達し、6〜12週間で敵の妨害・欺瞞に無効化される。ソフトウェア、通信、AIモデルを「数週間サイクルで継続更新できる組織能力」が作戦価値を直接左右する。













小型FPV・短距離消耗型

電子・システム関連費レンジ：25〜50% (基準: 40%)

機体単体は数万円規模の使い捨て部品。弾頭等を除く量産BOMにおいて、フライトコントローラーや映像伝送系が下限を規定する。

AI終末誘導・自律型の一方向攻撃機

電子・システム関連費レンジ：35〜65% (基準: 50%)

EO/IRセンサー、エッジAIアクセラレータ、耐妨害通信システムへの投資が増加し、価値が電子装備へシフト。

戦術ISR / MALE・HALE

電子・システム関連費レンジ：50〜75% (基準: 65%〜)

機体自体も高価だが、長距離広帯域データリンク、広域センサー、高度な地上管制システム（GCS）が取得費の過半を占める。

防衛調達の近代化を支える三つの基盤

常時セキュリティ確保・早期装備化・スタートアップ参入を実現する「三者一体＋DevSecOps」



三者を別々に導入するのではなく、DevSecOpsの下で一体運用することで、
「安全に、早く、開かれた防衛調達」を実現する。

MOSAとは

Weapon Open Systems Architecture（WOSA）の考え方

MODULAR OPEN ADAPTABLE FOR A STRONGER DEFENSE

“何でも自由交換”ではなく、**変更価値の高い機能のインターフェースを標準化・管理**

従来の兵器システム



WOSAの考え方

すべての部位を自由交換するのではない
作戦上変更価値の高い機能を対象に標準化・管理する



機能分離
役割ごとにモジュール化し
独立した開発・更新を可能に

重要IF標準化
変更価値の高いインターフェース
を標準化し、互換性を確保

迅速な技術挿入
新しいセンサー・アルゴリズム・
通信方式などを素早く適用

試験・競争促進
モジュール単位の試験・評価で
複数企業の参入と競争を促進

本質は“Plug and Playの万能化”ではなく、“変更しやすい設計とインターフェース管理”

AIR SUPERIORITY FOR A SAFER INDO-PACIFIC

STRONGER DETERRENCE THROUGH TECHNOLOGY AND ALLIANCE

AMRAAMの進化とWOSAの位置づけ

AAM-4B を「第1段階」に入れず、米 AMRAAM の進化を基準に整理する

第1段階：従来 AMRAAM
AIM-120C/D

買って終わり型



型式／ブロック更新が中心

- ハード・ソフトを比較的一体で改修
- 能力向上は型式／ブロック更新が中心
- WOSA ではない

従来型：大きな改修単位

第2段階：現在の中間段階
AIM-120D-3 + SIP

ハード刷新＋ソフト継続更新



F3R → D-3 → SIP-3F → SIP-4

- ✓ F3R：15 枚の回路基板を刷新
- ✓ D-3： 新しいハード基盤
- SIP-3F → SIP-4 でソフトを継続更新
- ! ただし、D-3 自体を WOSA とは断定しない

AMRAAM は「継続更新」の実例

第3段階：将来の WOSA 型兵器
標準 IF で部品単位更新

部品単位の競争・交換・更新へ



- 重要インターフェースを標準化
- サブコンポーネント単位で競争・交換・更新
- 新技術をより迅速に導入

WOSA：部品単位更新を制度化

空自への示唆 | AAM-4 → AAM-4B は「日本の型式更新例」として比較対象に置く。AMRAAM の進化段階には入れない。

注： AIM-120D-3 + SIP は「継続更新」の実例。WOSA はその先の「部品単位の競争・更新」を制度化する枠組み。

! 注：D-3 自体を WOSA 準拠と断定しない

INTEGRATED DETERRENCE FOR A STABLE REGION

A MORE SECURE TOMORROW TOGETHER

AMRAAM D-3＋SIP：WOSAではなく「継続更新」の実例

F3Rでハード基盤を刷新し、SIPでソフトを更新。その先に「部品単位で競争・交換・更新する」WOSA型兵器がある。

“買って終わり”から、ハード更新＋ソフト継続更新＋将来のサブコンポーネント競争へ

現在：AIM-120D-3



- F3R：15枚の回路基板を刷新
- 旧電子部品を更新
- ミサイル寿命全体の基盤を確保

継続的ソフト更新



能力はソフトで磨き続ける

将来：WOSA型兵器



サブコンポーネント競争	標準IFで統合	新技術を迅速挿入
複数のベンダー・新技術を選択可能	共通インターフェース（オープンアーキテクチャ）	センサー・通信・AI処理など継続的に能力向上

AMRAAMは“継続更新”の現実例。WOSAはそれを“部品単位の競争・更新”へ進める仕組み。

注：AIM-120D-3自体をWOSA準拠と断定するものではない

注：AIM-120D-3自体をWOSA基準と断定しない。F3R＋SIPは、WOSAへ至る前段の「継続更新」モデルとして示す。

日本AAM-4Bと米AIM-120D-3の能力向上方式の違い

AIR SUPERIORITY FOR A SAFER INDO-PACIFIC

STRONGER DETERRENCE THROUGH TECHNOLOGY AND ALLIANCE

「新型化」中心か、「同一基盤の継続更新」か

日本：AAM-4 → AAM-4B



我が国の空を、
より遠く、より確実に

AAM-4 → 開発・試験 → AAM-4B

- 新しい派生型として能力向上
- ハード・ソフトを一体で改良
- 実用試験を経て更新
- 公開試料上、継続的SIP型更新は明示されていない

型式更新型

JASDF AAM-4B FOR JAPAN'S SKIES

異なるアプローチ

共通の目的

より強力な空の抑止力

米国：AIM-120D-3 + SIP



継続する進化が、
優位を保つ

F3Rハード刷新 → AIM-120D-3 → SIP-3F → SIP-4（試験中）

- 15枚の回路基板を刷新
- 同一ハード基盤を維持
- ソフトウェアで継続能力向上
- 脅威・電子防護・処理能力を順次改善

継続更新型

AMRAAM EVOLVES TO MEET TOMORROW'S THREATS

空自への示唆：「新型を開発する力」に加え、「運用中ミサイルを継続更新する力」が重要

※公開資料ベースの整理

CCA / A-GRA に見る“動き始めたMOSA”

機体とミッション自律ソフトを分離し、迅速な更新と競争を可能にする

COLLABORATIVE COMBAT AIRCRAFT FOR A MORE LETHAL AND RESILIENT FORCE

従来：機体ごとに専用ソフト

機体とソフトが一体で、独自仕様・閉鎖的

無人戦闘機 A
（例：Loyal Wingman）



専用ソフトウェア
- ミッション制御
- センサー処理
- 通信・データリンク
- ・・・

無人戦闘機 B
（別メーカーの機体）



専用ソフトウェア
- ミッション制御
- センサー処理
- 通信・データリンク
- ・・・

ベンダーロック
特定メーカーに依存

機体ごとに再開発
ソフトの使い回しが困難

更新が遅い
脅威変化への対応に時間

CCA：A-GRAを介して分離

共通アーキテクチャに多様なソフトを接続、迅速・柔軟・競争的

- **ミッション自律**：作戦行動・AI
- **センサーフュージョン**：マルチセンサー統合
- **通信**：データリンク・C2
- **EW**：電子戦・自己防護
- **航法**：測位・航法・誘導

A-GRA
（政府保有の共通アーキテクチャ）



CCA 機体 A
（例：General Atomics YFQ-42）



CCA 機体 B
（例：Anduril YFQ-44）

異なる機体 × 異なるソフトを組み合わせやすくする

機体とソフトの分離
ハードとソフトを独立に進化

迅速な更新
新機能を素早く導入

競争促進
多様なベンダーの参入・競争

将来拡張
新たな能力・機体への容易な適用

ベンダーロック抑制
政府主導の共通基盤で依存を低減

CCAは“MOSAが本当に動き始めた例”として理解しやすい

ADAPTIVE OPEN COMPETITIVE LETHAL

AUTONOMOUS COLLABORATIVE EVOLVE

ANDURIL ALTIUS 600 / 700: MOSA (WOSA) 準拠 モジュール式無人システム & 巡回型兵器

【共通基盤】モジュール式エアフレーム & パワーモジュール (MOSAコア)

- 高揚力翼 & 尾翼
- 大容量バッテリー & 電力配分
- 共通フライトコントローラー/オートパイロット (WOSA/MOSA準拠)

共通インターフェースでコンポーネントの相互運用性を確保

VENDOR A　VENDOR B　…　AFRL VALIDATION HARNESS

【迅速換装】モジュール式ペイロード (ISR, EW, 兵器)

- ミッションに応じたペイロードモジュールを field で <15 分未満に迅速換装
- 多様なベンダーのセンサー/コンポーネントを選択可能

ペイロード交換 (プラグ & プレイ)





空中発射 & 巡回型兵器ミッション

多様な運用シナリオ



1. ISR (情報収集)　2. EW (電子戦)　3. 通信中継　4. 巡回型攻撃

共通インターフェースにより、ALTIUS艦隊全体で多様なペイロードを選択可能。戦況の変化に合わせた持続的なアップデートと自律協調運用を実現。

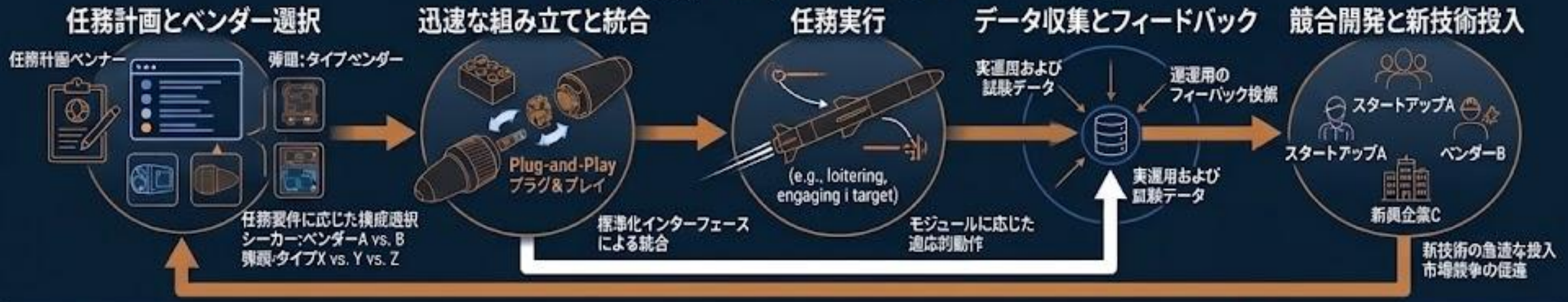
Anduril Barracuda 巡航ミサイル：各モジュールにおける複数ベンダー（スタートアップ各社）の差し替え可能性を示す

MULTI-VENDOR INTEROPERABILITY: MODULAR ARCHITECTURE REPLACEMENT OPTIONS

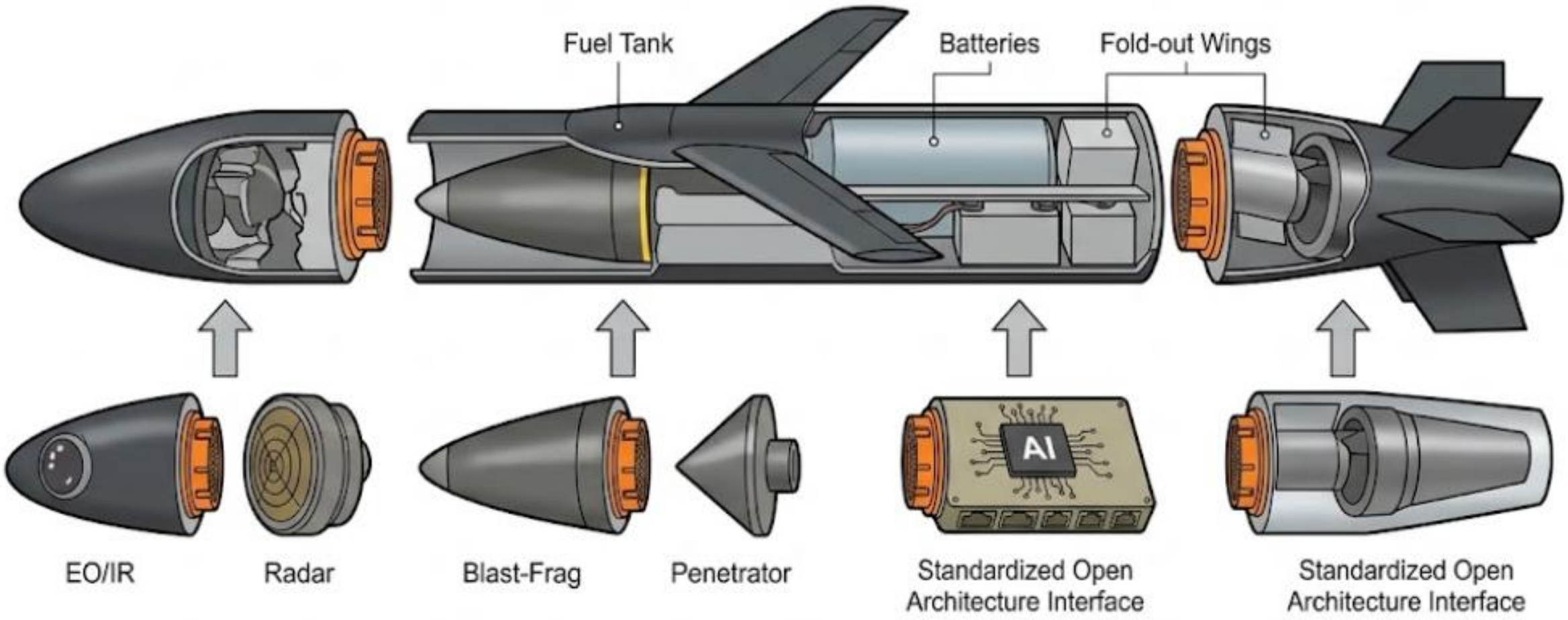


Anduril Barracuda 巡用概念図

モジュール式・複数ベンダー・プラグ＆プレイ運用



Anduril Barracuda Cruise Missile: Modular Open Architecture



Interchangeable Seeker Module
(EO/IR and Radar)

Modular Warhead Module
(Blast-Frag and Penetrator)

Interchangeable Mission Computer Module
(in autonomous "Lattice" AI core)

Modular Propulsion Module
(with turbojet engine)

A2/AD 抑止作戦空域

第21タスク部隊、作戦ID: B4550

BARRACUDA モジュール性

多ベンダー互換性

目標：脅威アセット群

TELミサイル発射機

レーダー施設群

TBM強化バンカー

スサイク投施の
特別新なパネル

ToT: 00:00:03

作戦実行結果の
フィードバック

精密打撃影響可視化



バンカー破壊（集中打撃）



TEL発射機無力化



レーダー機能停止

BARRACUDA モジュール性

多ベンダー互換性

NAVSEA & ONR MUUV(MULTI-VENDOR COMPONENT SEPLACEMENT ARCHITECTURE

NAVSEA & ONR standardized interfaces for multi-mission modular payload bay and component replacement for mission flexibility



[FUNCTIONAL SEPARATION] [COMMON IF STANDARDIZATION] [RAPID TECHNOLOGY INJECTION] [TESTING & COMPETITION]

標準インターフェースを介して、ASW、SuW、MCM、ISR、Power、Propulsionといった多様な任務対応ペイロード・ベイを、複数ベンダー(Company A, Company B等)からプラグ&プレイで選択・交換可能。
NAVSEA MUUVはオープン・アーキテクチャ設計により、迅速な機能更新と競争的調達を実現。

2025年11月

LATITUDE-CORE SPECTRUM AVIONICS Anduril A-Seeker X-Logic S-Thrust

ANDURIL ALTIUS: MOSA、SBOM/VEX、RMF 統合 DevSecOps サイクル



DevSecOps サイクル：設計・開発・テスト・配備・運用

設計・開発

テスト・評価

テスト・評価

設計・開発

三者一体＋DevSecOps：
安全で開かれた
無人システムの持続的進化

安全に、早く、開かれた
防衛調達の実現

RMF（継続的リスク管理・認可）



RMF（継続的リスク管理・認可）

ライフサイクル全体を通じた、リスクベースのセキュリティ認可と脅威の継続的監視（PIT-RMF）



MOSA（モジュール化・オープン標準）

モジュール境界の標準化による迅速な換装とマルチベンダー競争



SBOM/VEX（ソフトウェア可視化・脆弱性管理）

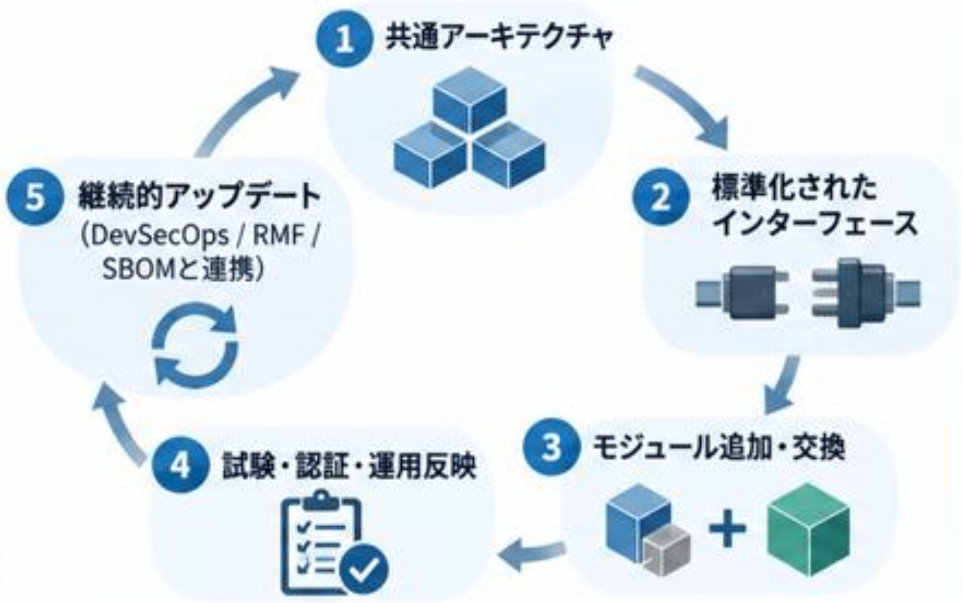
ソフトウェア構成の透明化と、脆弱性発見時の迅速な悪用可能性判断（VEX）による継続的修正

MOSAの本質は“オープン化”ではなく“継続的進化”である

Geranの実戦的進化とMOSAの狙いを対比すると、共通点は“継続的に改良し続ける能力”にある

共通する核心：基本プラットフォームを維持しつつ、必要な機能を継続的に交換・改良する

MOSA（制度化された継続的進化）

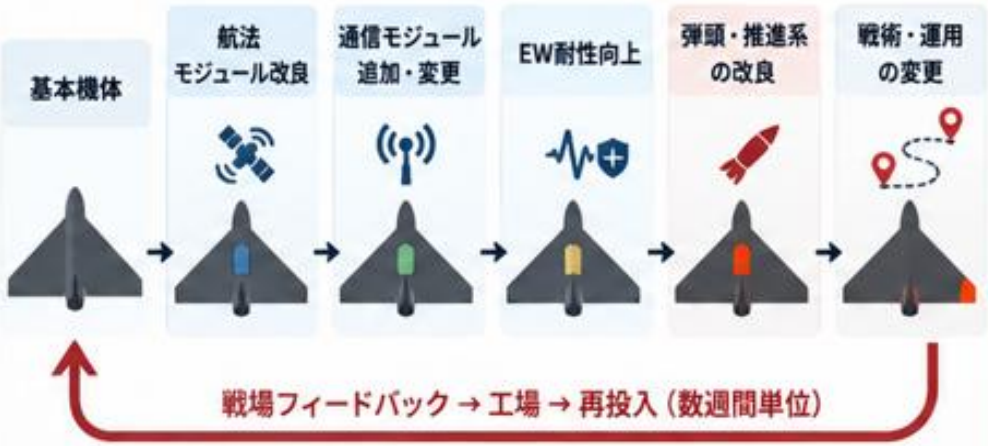


狙い： センサー、通信、AI、電子戦、防護機能を短期間で改良し、能力を持続的に向上させる

違い

公開・標準化	↔	必ずしも公開規格ではない
制度・認証を伴う	↔	まず実戦で試す
複数ベンダー参加を促進	↔	入手可能部品を即応利用
安全に進化を継続	↔	高速に進化を継続

Geran（実戦駆動の継続的進化）



特徴： 同一の基本機体を使いながら、戦場の対抗手段に応じてサブシステムを素早く改良

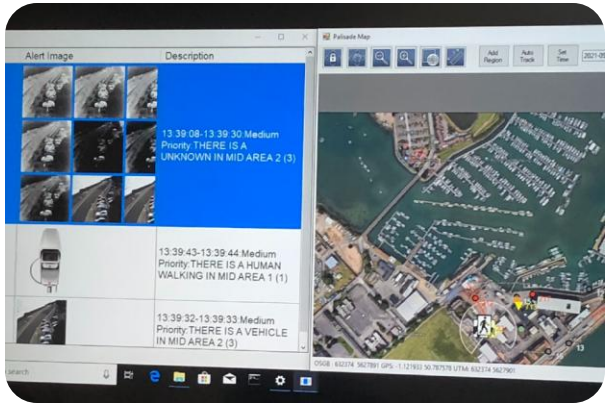
この比較から見えること

1. MOSAの本質は“モジュールを公開すること”そのものではなく、“継続的進化”を可能にすることである
2. Geranは formal MOSA ではないが、実戦では“de facto modular evolution”を実現している
3. 日本が学ぶべき点は、標準化だけで満足せず、脅威変化に追随する高速改良能力を持つこと

概念図（DoD MOSAの考え方とCSIS『From Shahed to Geran』2026の分析を踏まえた整理）

英国SAPIENT（NATO相互運用文脈）のC-UAS

センサー側で探知・分類し、共通ICDで融合・タスク・エフェクター連携



SAPIENT運用画面（Dstl / GOV.UK）

位置付け

英国MOD発

→ NATO STANREC 4869

異なる国・ベンダーの
異種ノード連接を支える推奨規格

SENSOR NODE
レーダー
エッジAI
探知・測位

SENSOR NODE
EO / IR
エッジAI
画像分類・確認

SENSOR NODE
RF・ESM
エッジAI
電波探知・識別

DECISION NODE
融合・相関・追尾
共通状況図／センサー管理／タスク生成

EFFECTOR NODE
妨害・迎撃手段
タスク受領／応答／状態報告

SAPIENT / BSI Flex 335 v2

登録 | 状態 | 探知報告 | タスク | 警報 | エラー

公開ICD・Proto・Test Harnessで、異種ノードの接続と試験を反復

要点：SAPIENTは英国起源。NATOでは単一装備ではなく、STANREC 4869による相互運用の共通語として展開。

韓国TTA Anti-Drone System FrameworkのC-UAS

探知・識別・無力化・統合管制を、参照構造と共通インターフェースで整理

標準体系

- Part 1 参照構造
- Part 2 探知
- Part 3 識別
- Part 4 無力化
- Part 5 統合管制
- Part 6 I/F・データ

DETECT
探知システム
レーダー／RF
EO・IR
検知・測位・追尾

IDENTIFY
識別システム
対象分類／属性付与
脅威判定を支援

C2
統合管制
融合／状況図／警告
タスク・運用管理

DEFEAT
無力化システム
電子・非運動・運動
効果確認・状態報告

TTAK.KO-10.1460-Part 6 共通データフレーム / Protocol Buffers

登録 | 状態報告 | 探知報告 | タスク | 脅威警告 | エラー

注意：公開TTA標準に基づく概念図。特定の実配備構成や、SAPIENTとの意味互換性を示すものではない。

米国LIDSを中心とするC-UASシステム

配備済みのFAAD C2／LIDSに、ISAとMOSAのオープン化を重ねる移行期



Project Flytrap 4.5（U.S. Army）

FIELDING + TRANSITION

配備基盤：LIDS / FAAD C2

ISA：異種システム接続
JIATF-401：MOSA・共通標準

SENSORS

KuRFS

Ku帯レーダー・追尾

SENSORS

他のセンサー

レーダー／EO・IR／RF

C2 / INTEGRATION

FAAD C2 / LIDS

共通状況図
トラック融合
射手・交戦統合

EFFECTOR

Coyote

Block 2 / 2C / 3NK

EFFECTOR

他の射手

EW／非運動／運動

ISA / standardized open-architecture data formats

Project Flytrapで多国籍・複数ベンダーを接続試験 | JIATF-401：MOSA・共通データ標準

注意：CoyoteはエフェクターでありC-UAS全体ではない。公開された米英共通データ標準発表は、SAPIENT名を明記していない。

Geranの継続的進化に対し、SAPIENTはオープン接続で継続対抗する

攻撃側はGeranを継続改良し、防御側はSAPIENTでセンサー・C2・エフェクターを接続してLayered C-UASを継続進化させる

本質：重要なのは“オープン化そのもの”ではなく、“脅威変化に応じて継続的に能力を更新できること”

攻撃側：Geranの進化

基本プラットフォームを維持しつつ、必要なサブシステムを継続改良

Geran-2 → Geran-4 / Geran-5級

① 基本機体	② 航法改良	③ 通信追加・変更	④ EW耐性向上	⑤ 弾頭・推進改良	⑥ 高連化・戦術変更
					
基本設計を維持	GNSS耐性・慣性航法の改善	データリンク・中継・秘匿化	妨害耐性・低可知化	弾頭の多様化・推進系の改良	より高速・多様な経路・多数運用

特徴：Geranは“攻撃側の継続的進化”を体現する

脅威の進化

より高度・多様な一方向攻撃ドローン

SAPIENTの役割 = Sensor・C2・Effectorをつなぐオープンな接続基盤

対抗手段の更新

新センサー・新C2・新EW・新エフェクターの追加

SAPIENTは“MOSAそのもの”ではないが、MOSA型の継続進化を支えるオープン・インターフェース概念

防御側：SAPIENT / NATO Layered C-UAS

異なるメーカーのセンサー・C2・エフェクターを接続し、必要に応じて追加・交換

探知・追尾（センサー）	融合・識別・射撃統制（C2）	各種エフェクター（迎撃手段）
Radar RF EO/IR Acoustic	Decision / C2 • 脅威の統合認識 • 分類・優先順位付け • 迎撃手段の割当 • 他システム連接	EW（通信/GNSS妨害・ソフトキル） Gun / 近接火器（低コスト多数対処） 迎撃ドローン（低コスト・柔軟） 低コスト迎撃弾（将来追加可能）

MEROPSなどの低コストC-UASにも接続しやすい

NATOはLayered C-UASで継続更新を重視

SAPIENT = センサー+ C2 + エフェクターを統合する“system of systems”

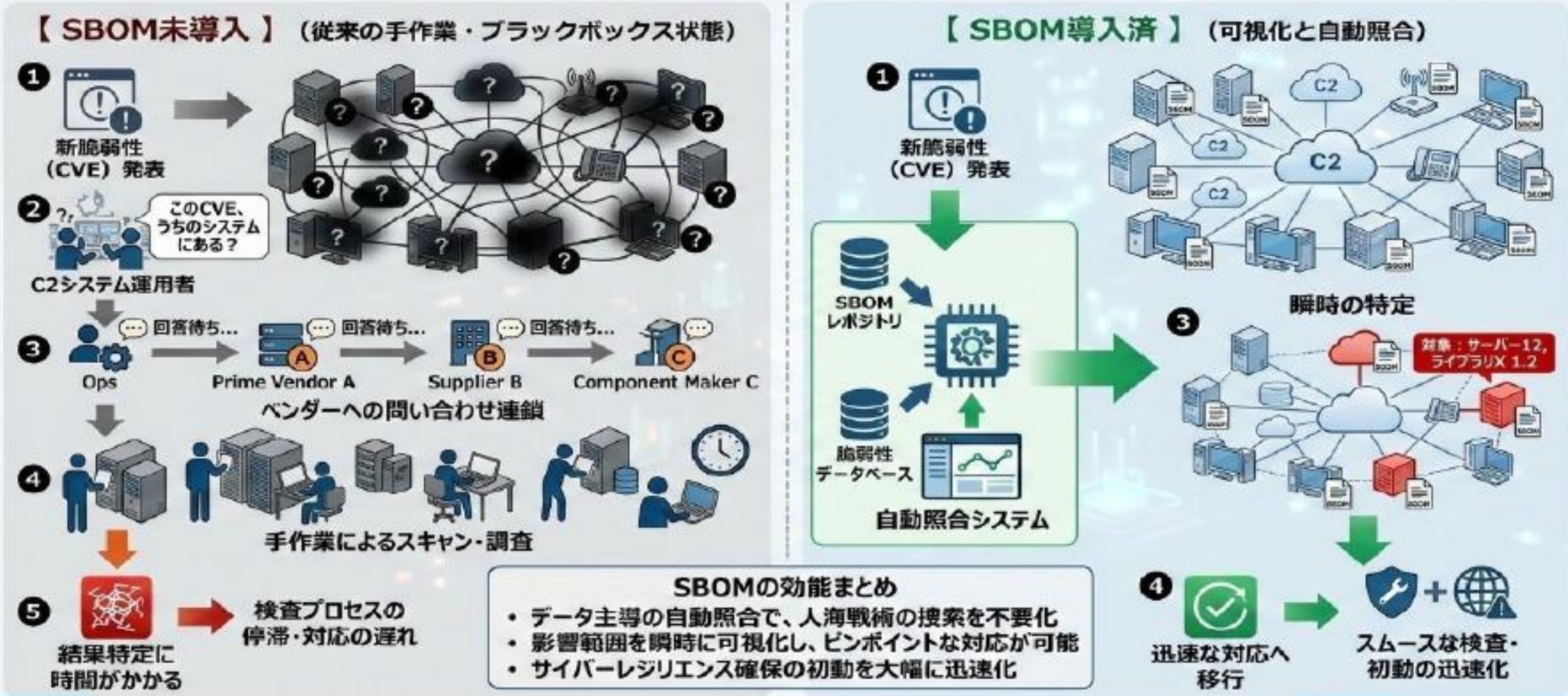
この比較から見えること

1. Geranは、基本機体を維持しながらサブシステムを継続改良する“攻撃側の進化モデル”である
2. SAPIENTは、異種のセンサー・C2・迎撃手段を接続し、NATOのLayered C-UASを継続進化させる“防御側の接続基盤”である
3. 示唆：Geranのような脅威に対抗するには、固定的な完成品ではなく、オープン接続と継続更新が不可欠である

概念図：公開資料に基づく整理。SAPIENTはC-UASのオープン接続標準の一例、Geranは継続進化する脅威の例。

SBOM とは

SBOM導入による脆弱性検査の効率化比較：指揮統制通信システム（C2）の例



SBOMの効能まとめ

- データ主導の自動照合で、人海戦術の捜索を不要化
- 影響範囲を瞬時に可視化し、ピンポイントな対応が可能
- サイバーレジリエンス確保の初動を大幅に迅速化

欧米各国では SBOM の制度化が進展。韓国でも 2027 年から公共部門で SBOM 提出制度

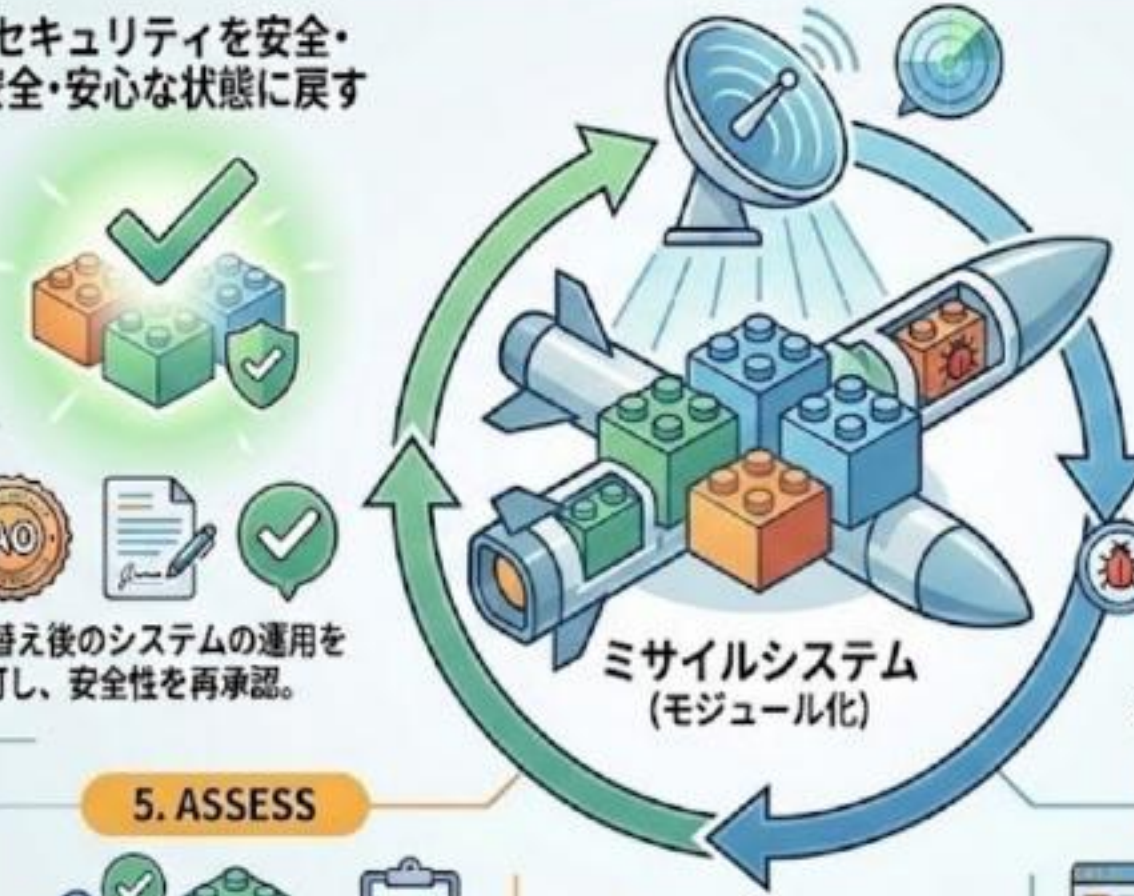
RMF とは

RMFによるミサイルシステムの継続的なセキュリティ強化プロセス：センサーモジュール脆弱性の発見と入れ替え

ミサイルシステム全体のセキュリティモニタリング

ミサイルシステムを構成する主な要素

- 通信ネットワーク (SATCOM、地上)
- ミサイルデータリンク (Link 16など)
- 誘導・統制システム センサー入力
- センサーモジュール (シーカー, GPS, レーダー)
- 発射統制装置 (コンソール)



センサーモジュールの脆弱性を探索

脆弱性のあるモジュールを入れ替え

センサーモジュール → 新しいセンサーモジュール

OUT / IN

古いセンサーモジュールの取り外し

新しいセンサーモジュールの取り付け

4. IMPLEMENT

セキュリティ要件と新しいセンサーモジュールの実装。

C2インター統合テスト

5. ASSESS

セキュリティコントロール新センサーモジュールの検証

コードレビューツール

RED TEAM

セキュリティを安全・安全・安心な状態に戻す

入れ替え後のシステムの運用を許可し、安全性を再承認。

ミサイルシステムでのRMFの利点

- 脆弱性の迅速な排除と無力化
- 安全な誘導データの保護
- ミサイル運用(命中率)の信頼性向上
- ミサイルシステム機能の継続と安全性の復帰

背景と課題 — なぜ今、制度基盤が必要か

安全保障環境の変化と技術の進展により、ソフトウェアライフサイクルを支える制度基盤が不可欠

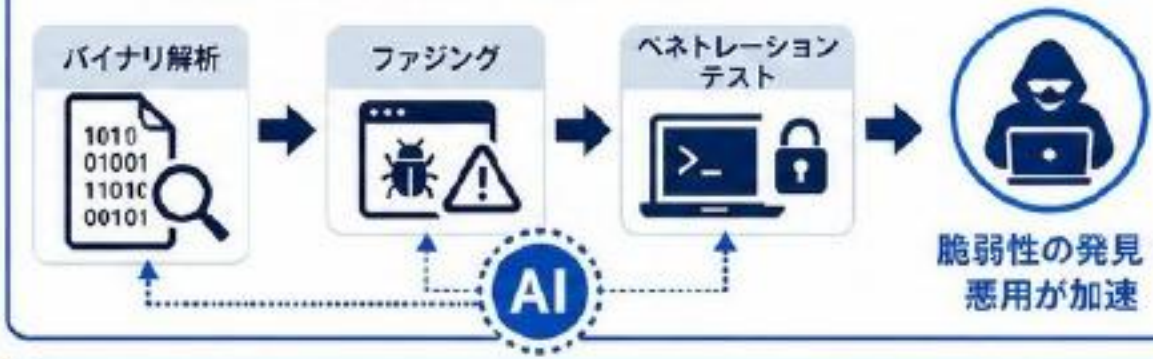
1 ソフトウェアが性能を決める時代

戦闘力・運用能力の多くが
ソフトウェアに依存



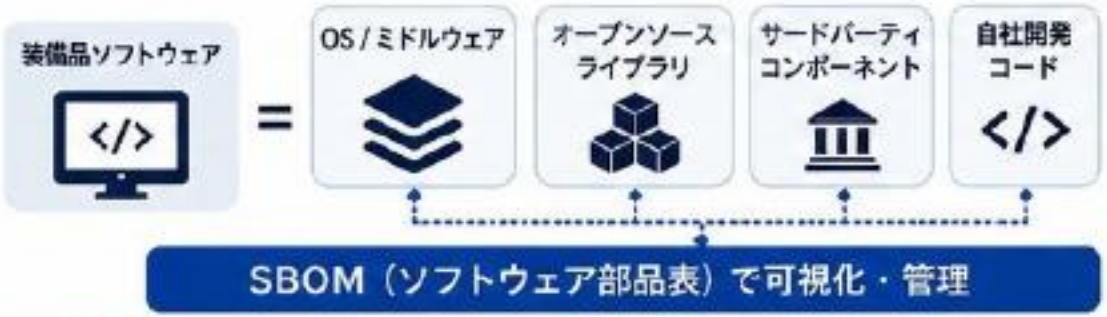
2 生成AIで脆弱性発見が加速

AI支援により解析・検証の精度とスピードが飛躍的に向上
脆弱性の発見・悪用がより速く・容易に



3 オープンソース利用拡大で構成把握が不可欠

ソフトウェアの大部分がオープンソースで構成
構成の可視化とライセンス・脆弱性管理が必須



4 スタートアップの民生技術を迅速に取り込む必要

AI・ドローン・センサー等、民生技術の進展は速く、
既存のクローズドー体設計では迅速な採用が困難



装備品の「ソフトウェア化」に対応するには、可視化・継続管理・モジュール化を制度として整える必要がある

DevSecOpsサイクル — 三者一体はこう回る

MOSA → SBOM → RMF → 更新・再配備の循環で、セキュリティ・早期装備化・スタートアップ参入を同時に実現



常時セキュリティ確保

RMF の継続監視とSBOMで影響を即座に把握し、MOSAで迅速に修正・更新。リスクを最小化し、安全性を常に確保。

1 MOSA：新技術をモジュールとして接続

モジュール化で新技術を取り込み、スタートアップもモジュール単位で参加可能。全体システムを見直さず部分更新できる。

2 SBOM：構成を可視化し影響範囲を特定

新モジュールを登録し部品表で構成を透明化。脆弱性発覚時に影響モジュールと範囲を即座に特定。国際標準（米国・EU）でサプライチェーン要件化。

3 RMF：リスク評価・認可・継続監視

リスクに基づく評価で認可を与え、継続的に監視・確認。脆弱性があればMOSAで該当モジュールを差し替え。CMMC（SP800-171）等に準拠。

4 更新：脆弱モジュールのみ交換し再配備

脆弱性のあるモジュールだけを差し替え、検証後に再配備。迅速にセキュリティを回復し、運用を継続できる。

DevSecOpsサイクル

三者一体の連携で継続的に強化

早期装備化

MOSAでモジュール単位のアジャイル開発を実現。SBOMとRMFの自動連携で評価・認可を迅速化し、早く導入し、運用しながら性能を向上。

スタートアップ参入

MOSAのオープンなモジュール標準で、非伝統的事業者もモジュール単位で参入しやすく、イノベーションを加速。

DevSecOpsは独立した第四制度ではなく、三者を設計・開発・試験・配備・運用の中で継続的に回す運用基盤である。

三者一体がもたらす政策的・戦略的効果

① 早期装備化とアジャイル開発



MOSAにより、成熟したモジュールを段階的に組み込み、迅速なアップグレードを実現。

② スタートアップ参入促進



標準インターフェースにより、非伝統的企業が防衛市場に参入できる環境を創出。

③ 新技術の迅速な導入



AI・無人システム・センサー・ソフトウェア等をモジュールとして既存システムに統合。

④ 国際装備移転と相互運用性



標準インターフェース、SBOM、RMFが、同盟国等とのコンポーネントレベルの協力の基盤を形成。

『作って終わり』から『運用しながら進化』へ──
制度基盤が競争力そのものになる。

敵は必ず脆弱性を見つける ― 問われるのは防御側の対応力

国家レベルの脅威アクターは、あらゆるシステムに侵入テストを仕掛ける

従来の一体型・閉鎖型

敵	時間はかかるが突破可能	
味方	内部が見えず、部分修正できない	 ブラックボックス
結果	脆弱なまま運用	

受動的で、修復も遅く、継続的にリスクを抱える

MOSAだけ先行

敵	公開IFから攻撃面が拡大	
味方	認証基準や監視体制が未整備	
結果	最も危険	

可視性不十分なまま攻撃面だけ増大

MOSA＋SBOM＋PIT RMF

敵	侵入は困難	
味方	発見→特定→交換が可能	 発見 特定 交換
結果	能動的に防御	

可視化・標準化・監視により能動的に防御

敵（攻撃側）の特性

探すことにコストをかけ続ける
必ず脆弱性を見つけるまで諦めない

非対称性（アシンメトリー）

時間は敵の味方

見つける負荷は小さい

味方（防御側）の特性

完璧を作ることはできない
しかし、見つけて直すことはできる

セキュリティの本質は「見つからないこと」ではなく、「見つけた後に直せること」である。

透明性・標準化・継続的監視により、脆弱性を「管理可能なリスク」に変える

無人機を起点とした導入戦略

安全に、早く、開かれた防衛調達を実現するために無人機を起点として制度を先行運用する

① なぜ無人機から始めるのか



「更地」から
出発できる
グリーンフィールド

レガシーのしがらみが少ない
新規設計の装備品から制度を最適化

予算規模と緊急性が高い
SHIELD構築など重点分野で
制度導入の必要性が高い

国際的な整合性が得やすい
韓国もK-MOSAを「国防無人体系」に設定し、
国際的にも同じ論理が進展

② 無人機固有のリスク

歯護リスク
有事・遭遇時の
機体・データ保護

改ざんリスク
物理的改ざん・
サプライチェーン攻撃

通信リスク
通信妨害・乗っ取り・
リンク切断

暗号リスク
暗号強度・管理・
アップデート脆弱性

PIT RMFを設計初期から組み込み必須
→ 後回しにすると再設計が必要となり、
コスト・期間が大幅に増大

③ 日本の強みと機会

センサー技術
光学・赤外・レーダー等の
世界トップクラスの技術力

GaN半導体
高出力・高効率デバイスで
無人機の性能向上に貢献

炭素繊維・複合材
軽量・高強度で航続距離・
積載性能を向上

ロボティクス技術
自律制御・協調運用・整備性で
優位性を発揮

海洋無人システム
USV・UUVを含む海洋領域で
標準化・事業化の主導権を獲得

SHIELD構築の進展、DICASとの接続、K-MOSAの動きにより、今が制度導入の好機

米国・韓国の PIT への取組み ― 国際的な参照点 ）（要調査）

米国

PIT-RMF と IS-RMF を制度的に区別（ NIST SP 800-37 / DoD RMF ）

- Blue UAS （国防総省） NDAA ・ ITAR ・ CPI ・ FMS 管理が強く、外国は完全コピー困難。
- Green UAS （ AUVSI ） 商用・公共向けのサイバー／サプライチェーン認証（ SBOM/HBOM 等）。
- ITAR の壁
  FMS だけでなく DCS にも ITAR/AECA/DDTC 。ソース・詳細 SBOM ・暗号・耐タンパー・ CPI は非開示。

韓国

K-MOSA ・ K-RMF ・ SBOM を整備（ 2027 年～公共部門で SBOM 提出制度）

- 国防無人体系 無人機を国家体系に位置づけ、国内 UAS に K-RMF/K-MOSA/SBOM を直接要求。
- 輸入 UAS は契約要件化 米 FMS/ITAR ・イスラエル・トルコ・欧州製は SBOM ・脆弱性通知・更新保証・ C2 接続評価・残余リスクを要求。
- 自国主導 PIT を強化 輸入依存のブラックボックス・リスクを認識し、国産 PIT 体系を拡大。

共通の教訓 ― 輸入装備にはブラックボックスが残る。だからこそ「自国主導で PIT 可能な無人機体系」を整備する。

米国「戦時取得システム（WAS）」メモ — MOSAを調達制度の中核原理へ

2025年11月7日、ヘグセス国防長官が発出。米国はMOSAを「適時性の速度を加速する主要なテコ（primary lever for accelerating the speed of relevance）」と明確に位置づけた。

メモの骨子 DAS → WAS

- 国防取得システム（DAS）を「戦時取得システム（WAS）」へ改称し、取得を戦時態勢（wartime footing）に置く
- 大統領令14265を法的起点とし、取得改革戦略（五本柱）と三本のメモを同時公表
- MOSAの最大活用を直接の任務に位置づけ

MOSAへの指示 速度のテコ

- モジュラーシステムの提供を積極的に優先せよ
- ベンダーロックの打破と競争の促進
- サプライチェーン強靭性の確保
- 迅速かつ漸進的な技術的優位の維持

結論 — 米国においてMOSAは、防衛調達制度の中核原理として位置づけられるに至っている。

出典：米国防省「Transforming the Warfighting Acquisition System」メモ及び取得改革戦略（2025.11.7, National War College）／10 U.S.C. §4401／FY2026予算資料

防衛調達の近代化を支える三つの基盤

常時セキュリティ確保・早期装備化・スタートアップ参入を実現する「三者一体＋DevSecOps」



三者を別々に導入するのではなく、DevSecOpsの下で一体運用することで、
「安全に、早く、開かれた防衛調達」を実現する。

現代のドローン戦におけるモジュールベースの OA の必然性

～ウクライナ実戦が示す更新周期の非対称性～

2026 年 7 月



付録　資料



第 1 段階：手動 FPV と一体型設計の限界（2023 年）

■ **[Deployment]**

安価な手動 FPV を大量投入。全機能が機体に固定の一体型。

■ **[Limitation]**

命中率は技量依存。新人約 20%、熟練 70 ～ 80% 。

■ **[Bottleneck]**

戦力は熟練操縦者の数で頭打ち。



第 2 段階：ロシア電子戦の激化 (2024 年)

■ [Jamming]

妨害電波・ GNSS 欺瞞を前線へ大量配備。

■ [Blind]

目標直前で映像が途絶、盲目のまま墜落。

■ [Crisis]

更新が追いつかず、命中率 20 ～ 30% 以下へ半減。



第 3 段階：通信・航法モジュールの高速交換（2025 年以降）

■ **[Module Shift]**

妨害に合わせ、無線を数週間単位で交換。

■ **[Countermeasure]**

光ファイバー (35 社超) や画像航法で成功率を回復。

■ **[Agility]**

交換可能な設計だけが追従できた。

※AI 誘導 (次頁) と並行進展。





第 4 段階 :AI 終末誘導の利用（2025 後半以降？）

■ [Upgrade]

150 ドル未満の後付け AI(例 :TFL-1)。コスト増 1 ～ 2 割。

■ [Autonomy]

終末 400 ～ 500m を機械視覚で自律追尾。

■ [Lethality]

命中率約 80% へ (企業・ Brave1 公表値)。



第５段階：スウォーム OSで「１人Ｎ機」管制

■ [Software]

共通スウォームOSを複数機に搭載。

■ [Operation]

ソフトが航法・編隊・回避を担い、１人Ｎ機へ。

■ [Milestone]

26年1月、米試験で１人３機・３目標打撃。実戦投入はこれから。

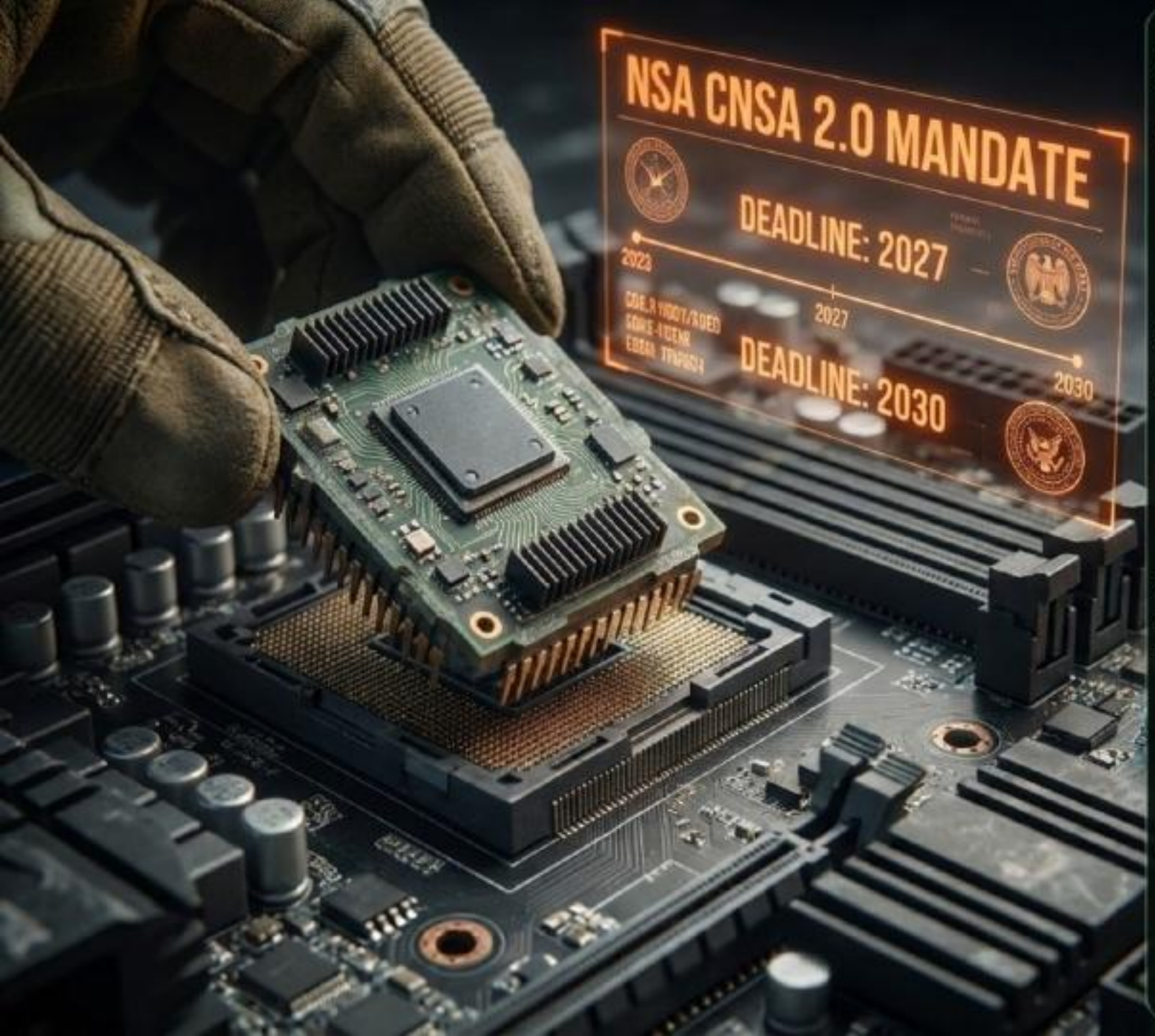
MOSA の構造的必然性 :5 系統の更新非対称性



■ **[Asymmetry]**
駆動要因が独立→更新も独立に到来。

■ **[Bottleneck]**
一体型は毎回全体再設計。最速周期に追従不能。

■ **[Necessity]**
速い機能を機体から切り離す MOSA が必然。



規制の圧力：暗号 (CNSA 2.0)

■ **[Gate 2027]**

2027 年～新規調達は耐量子暗号が必須。

■ **[Retire 2030]**

2030 年末までに非対応機器は退役。31 年～義務化。

■ **[Crypto-Agility]**

暗号を抜き差しできる設計が生死を分ける。



結論 :MOSA と継続的リスク管理 (CSRMC) の不可分性

- **[Limitation]** 交換のたびに SBOM が変化。全体再認証は不可能。
- **[Process]** 継続的リスク管理 (CSRMC) の導入が必須。
- **[Goal]** CSRMC と MOSA は表裏一体の戦略。



世界の潮流：共通 OS — Auterion

■ **[Foundation]**

PX4 等の公開標準を土台に米・NATO ・台湾で採用拡大。

■ **[Paradigm Shift]**

機体とソフトを分離、 AI を後付けで迅速更新。

■ **[Caveat]**

企業主導のデファクト標準。依存リスクに留意。