

NATO-RMF(CISセキュリティ・リスクマネジメントおよびセキュリティ認可プロセス)の経緯と現状、今後のリスク管理枠組みの行方(後編)

株式会社 Japan Aerospace & Defense Consulting
株式会社 SHIFT

菅野 隆 澤田 栄浩

前号では、米国を含む多国籍同盟である北大西洋条約機構(NATO)のRMFをトピックとし、「NATO-RMF(CISセキュリティ・リスクマネジメントおよびセキュリティ認可プロセス)の経緯と現状、今後のリスク管理枠組みの行方」(前編)をお送りしました。今回はその後編です。極めて情報が限定されている中で、米国とNATOにおけるRMFの改善に向けた取り組み、防衛省の現状について整理した上で、グローバル戦闘航空プログラム(GCAP)についても触れ、総括します。

RMFの改善

(1) 米国の状況

ア 全般

2014年にRMFが開始されて以降、そのコンプライアンス手続きは、手作業による証拠資料の収集や文書ベースの承認作業に依存していたため、負担が大きく、かつ多くの時間を要するものでした。そして、形式的な作業はセキュリティ確保に直結しないとの指摘もありました。

2019年、米国国防イノベーション委員会(Defense Innovation Board)は、その報告書「Software Is Never Done」において、ソフトウェア開発・調達速度と更新周期を最重要指針に掲げ、従来のハードウェア中心の古い調達プロセスから脱却し、ソフトウェア中心のシステムに最適化された全く新しい開発・調達システムの必要性を訴えました。そして、ソフトウェアを「(装備品を含むITシステムを)継続的に進化し続ける能力」と捉え直し、強化のための具体的ロードマップを提示、既に民間のベストプラクティスへと成長していた

DevSecOps¹⁾といった開発要領への転換を強く促しました^{2),3)}。

2022年、これらの提言などを受けDoDソフトウェア近代化戦略が署名されました。この戦略は、競争者よりも迅速に適応し優位性を維持するため、「高速で回復力のあるソフトウェア機能を提供する」という方針の下、ソフトウェア取得時間を劇的に短縮(数年かかっていたものを数分に)することを目指していました。そして、①DoDのエンタープライズクラウド環境への加速、②DoD全体のソフトウェア・エコシステムの確立、③高速で回復力あるプロセスの開発、が具体的目標として設定されました。この戦略の採用に伴い、DoDのDevSecOpsは加速することとなります⁴⁾。

DoDにおいては、運用承認ATO(Authorization to Operate)取得がボトルネックとなるステップとも認識されており、同日、併せて迅速かつ継続的なセキュリティ監視と承認プロセスの推進に向けた方針が明示されました。それは、品質とセキュリティを継続的に検証する継続運用承認cATO(Continuous Authorization to Operate)への移行を促すものでした。また、「スナップ

ショット」によるコンプライアンス文化から、「自動化」、つまりリアルタイムでの継続的監視、迅速なインシデント対応の文化に移行すべきとし、DevSecOpsによるセキュリティの自動化の採用を促し、クラウドに関しても適切なセキュリティコントロールの実装を保証することとしました。これにより、DevSecOpsパイプラインを通じたソフトウェアのリリースが、制度的に担保されました⁵⁾⁻⁷⁾。

かかる経緯を受け、2025年9月以降、RMFを上書きする形で、CSRMC (Cyber Security Risk Management Construct) への移行が宣言⁸⁾され、実現に向けた努力が継続されている状況です。

イ RMF 管理のためのツール

ア) ACAS

脆弱性管理・コンプライアンス評価ソリューション ACAS (Assured Compliance Assessment Solution) は、Tenable 社の技術を基盤とし、同社が Perspecta 社と提携して開発したソフトウェアソリューションです。

これは、DoD のネットワーク情報システムにおける脆弱性スキャンとコンプライアンス評価を自動化し、一元管理することを目的とした大規模組織向けのソフトウェア群で、国防情報システム局 DISA (Defense Information Systems Agency) が、2012年に同ソリューションを導入しています。

次世代 ACAS の RFI⁹⁾ 募集のページによると、その機能は「DoD (統合軍、各軍種、関係機関および野戦活動、戦闘支援機関、その他プログラム承認組織) に対し、資産および機器の識別と評価、ならびに国防総省システムおよびネットワークの設計、セキュリティ、コンプライアンス状況の評価を行う手段を提供」と説明されており¹⁰⁾、DoD 標準を基準とした資産の自動評価と既知の脆弱性の特定を任務としています。つまり、自動化された証跡提供システムとして機能しているものと見られます¹¹⁾。

イ) eMASS

大規模ミッション保証支援システム eMASS (Enterprise Mission Assurance Support Service) は、RMF プロセスにおけるシステム承認をサポートするために開発された、文書化および追跡の自動化機能を提供する GOTS¹²⁾ プログラムで、SaaS またはオンプレミスで提供されます。2023年頃の DISA の資料によれば、DoD によって維持・運用されているサイバーセキュリティリスク管理、RMF、評価・認証、および認定プロセスを自動化するシステムで、①プロセスの自動化と一元管理、②大規模なユーザーコミュニティと多様なフレームワーク対応、③継承機能と継続的モニタリング、④ API システム統合による DevSecOps パイプライン連携⑤ MITRE ATT&CK フレームワーク¹³⁾ の統合、の特徴があるとしており、複雑なサイバーセキュリティコンプライアンス業務を効率化するとともに、組織全体のセキュリティリスクを可視化・管理するための包括的なエンタープライズプラットフォームとして機能するとしています。ACAS を含む外部システムなどを統合し、継続的モニタリングを実現するともされています¹⁴⁾。

各ツールの概要を表 1 に、具体的イメージを図 1 に¹⁵⁾示します。

ウ AI の活用

DoD が2023年に公表した「データ、アナリティクス、AI 導入戦略」¹⁶⁾ は、それまでに公表されていた AI 戦略¹⁷⁾ (2018年) とデータ戦略¹⁸⁾ (2020年) を統合・発展させ、意思決定上の優位性を確立・加速させることを目指す戦略文書で、CSRMC は同戦略の方向性に沿ったものです。

「SOAR」¹⁹⁾ 2024年1月号²⁰⁾ では、AI を活用した脆弱性の予測・検知や、自動化されたリスク管理の有用性が強調されています²¹⁾。同レポートを踏まえると、DevSecOps パイプラインを活用しながら、以下のような AI 活用を進めていると考えられます。

表1 DoD-RMF のツールの概要

サービス	説明	ツールの細部	効果
Assured Compliance Assessment Solution (ACAS)	・米国防総省 (DoD) のネットワークや情報システムにおける脆弱性スキャンとコンプライアンス (設定基準の遵守) 評価を自動化・一元管理するための、大規模組織向けソフトウェア群。国防情報システム局 (DISA) が2012年に導入したプログラム。 ・Tenable 社および Perspecta 社と提携し、Tenable 社の技術を基盤とした統合ソフトウェアソリューション。 ・専用のハードウェア機器を調達・設置する必要がなく、ソフトウェアのダウンロードのみで各部門に展開可能な柔軟で拡張性の高い脆弱性管理ソリューション。 ・全てのレベル (司令部から最前線まで) で容易に導入でき、リアルタイムなリスク評価が可能。	■ Tenable.sc (旧 SecurityCenter) 資産の発見、脆弱性の検出、コンプライアンス監査を統合する中央管理コンソール。DISA の IAVM (情報保証脆弱性管理) システムと直接連携し、新たな脆弱性アラートが出た際も即座にスキャナーに新しいポリシーを展開できるため、手作業による遅延を排除。 ■ Nessus スキャナー (能動的スキャン) 87,000以上のプラグインと38,000以上の CVE (共通脆弱性識別子) をサポートする高速かつ高精度なスキャナー。ワークステーションやサーバーなど広範な機器をチェック。 ■ Nessus Network Monitor (受動的スキャン) 従来のアクティブスキャンでは見逃されがちな、スマートフォンやクラウドサービスといった「一時的に接続されるデバイス」をリアルタイムで監視。	・手動プロセスの大幅削減。 ・米軍の各軍 (陸海空など) や情報機関 (NSA や DIA など)、沿岸警備隊を含む極めて広範で分散した組織に対して、ライセンスやコストの制限なくスキャナーを展開できる高い柔軟性と拡張性を提供。 ・これにより、DoD は単なる定期的なポイントスキャンではなく、能動的および受動的スキャンを組み合わせた「高度に自動化されたリアルタイムの継続的監視」を実現。
Enterprise Mission Assurance Support Service (eMASS)	・eMASS は、連邦政府 (国防、民間、情報機関) に対して SaaS (Software as a Service) またはオンプレミスで提供されている政府既製 (GOTS) プログラム。リスクマネジメントフレームワーク (RMF) プロセスにおけるシステムの承認 (Authorization) をサポートするための、文書化および追跡の自動化機能を提供。運用開始は2008年。 ・システム内には、サイバーセキュリティの管理とガバナンスに関連する継続的監視、RMF の記録、評価および承認の決定事項 (Assessment and authorization decisions)、システムコントロールの活動、ダッシュボードレポートなどの記録が保存。	■ WF と文章生成の自動化 - ステップ2 (選択) セキュリティコントロール選択、セキュリティ評価計画 (SAP) およびセキュリティ計画 (SP) の承認ワークフローを eMASS 上で開始。 - ステップ3 (実装) セキュリティコントロール実装のワークフローを開始。 - ステップ4 (検証) 再度 SAP ワークフローを開始し、実装した全てのセキュリティコントロールを独立検証者 (Validator) のレビュー用として eMASS 上で提出。 ■ 評価・スキャン結果の統合 eMASS には「Asset Manager」という機能があり、外部のサイバーセキュリティ評価ツールやスキャンツール (ACAS) の結果を直接システムにインポートして管理・紐付け可能。 ■ 成果物と是正措置の中央リポジ システムに関するあらゆる情報を集約する保管庫として機能。 ■ アカウントと運用責任 プロジェクトにおいて、eMASS のアカウントを取得・維持し、承認パッケージや記録を日々の業務として管理することは主に情報システムセキュリティエンジニア (ISSE) の責任。	・システムの登録から廃止に至るまで、重要なセキュリティ機能を管理するためのワークフローおよびロールベースのアクセス制御。 ・RMF ステップ (NIST 800-53 および国家安全保障システム委員会 (CNSSI) 1253 システム分類、PO&AM 管理、セキュリティ制御評価、リスクレビューの自動化) ・標準化された RMF レポートの生成、PDF へのデジタル署名、ダッシュボードおよびメトリクスの集計、およびエンタープライズ要件 (例: RMF データ要求に対する国防総省 CIO) 向けの自動レポート作成。 ・継承階層、システム間統合を可能にする API、ワークフロー用コラボレーションボード、センサデータによる運用上の継続的モニタリングサポートなどの高度な機能。

(ア) 脆弱性分析

DevSecOps パイプラインから収集した大量のデータから、システムの重要性を踏まえた脆弱性の深さ、悪用可能性を考慮し、優先的に修正する脆弱性を特定 (誤検知を極力抑え、アセスメント時間を短縮)。

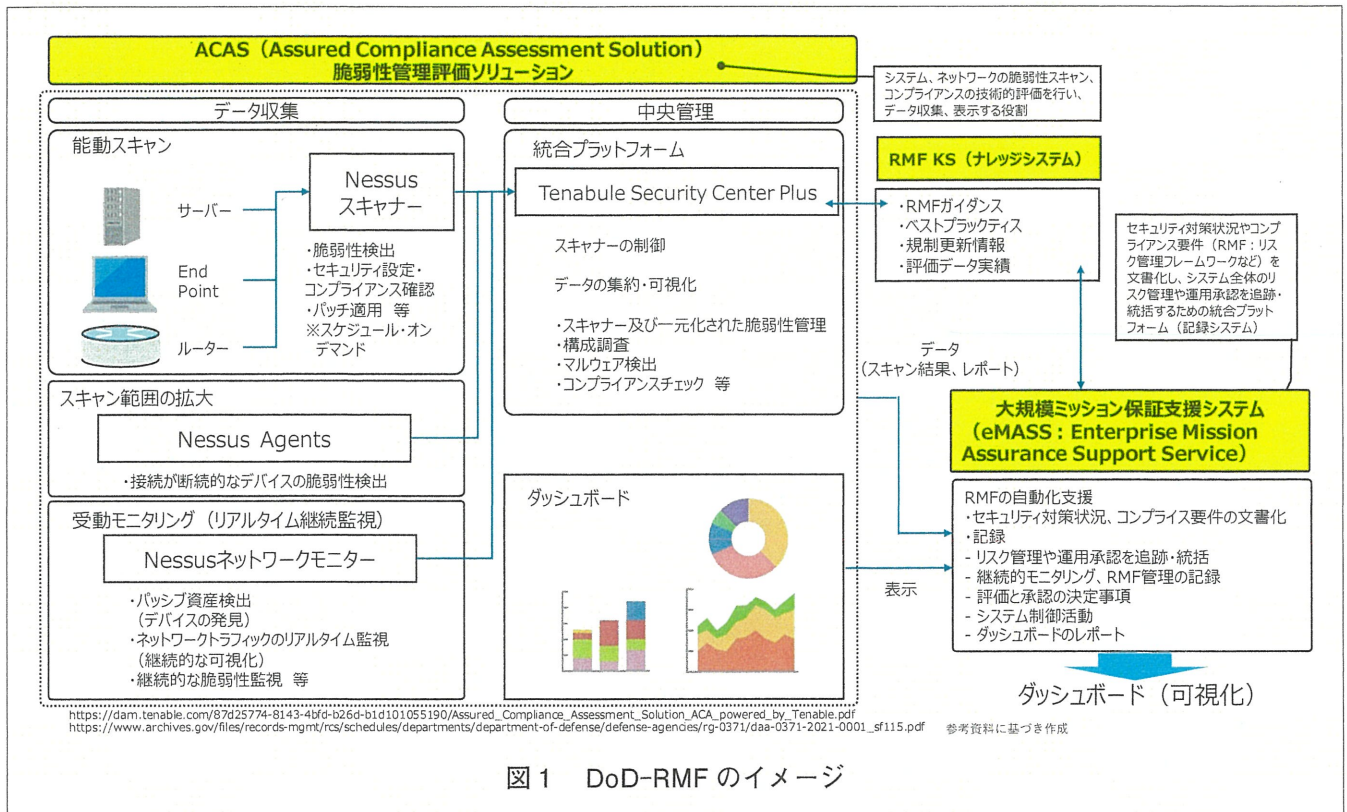
(イ) 構成ポリシー準拠の確認

システムの構成データを分析し、セキュリ

ティポリシーや STIG (セキュリティ技術実装ガイド)²²⁾ からの逸脱を検知。

(ウ) 継続監視

システムログ、ネットワークトラフィックおよびユーザー行動データを基に、「正常」な状態を学習した上で、リアルタイム分析を実施 (正常なパターンから逸脱した挙動を、未知の攻撃や内部脅威の兆候として検知)。



(エ) 脅威情報の相関分析

複数の情報源から得られる脅威情報（スキャン結果、IDS/IPS²³⁾ アラート、EDR²⁴⁾ データなど）を相関分析し、攻撃の全体像を把握。

(オ) 継続運用承認

継続運用認証を実現するため、システムの状態を常時把握し、あらかじめ設定したしきい値に基づく自動化トリガーにより、脅威を監視・検知。

以上を踏まえ、DoDがRMFから段階的に移行中とされるCSRMCの全体イメージ（一例）を図2に示します。

(2) NATOの方向性と現在の状況

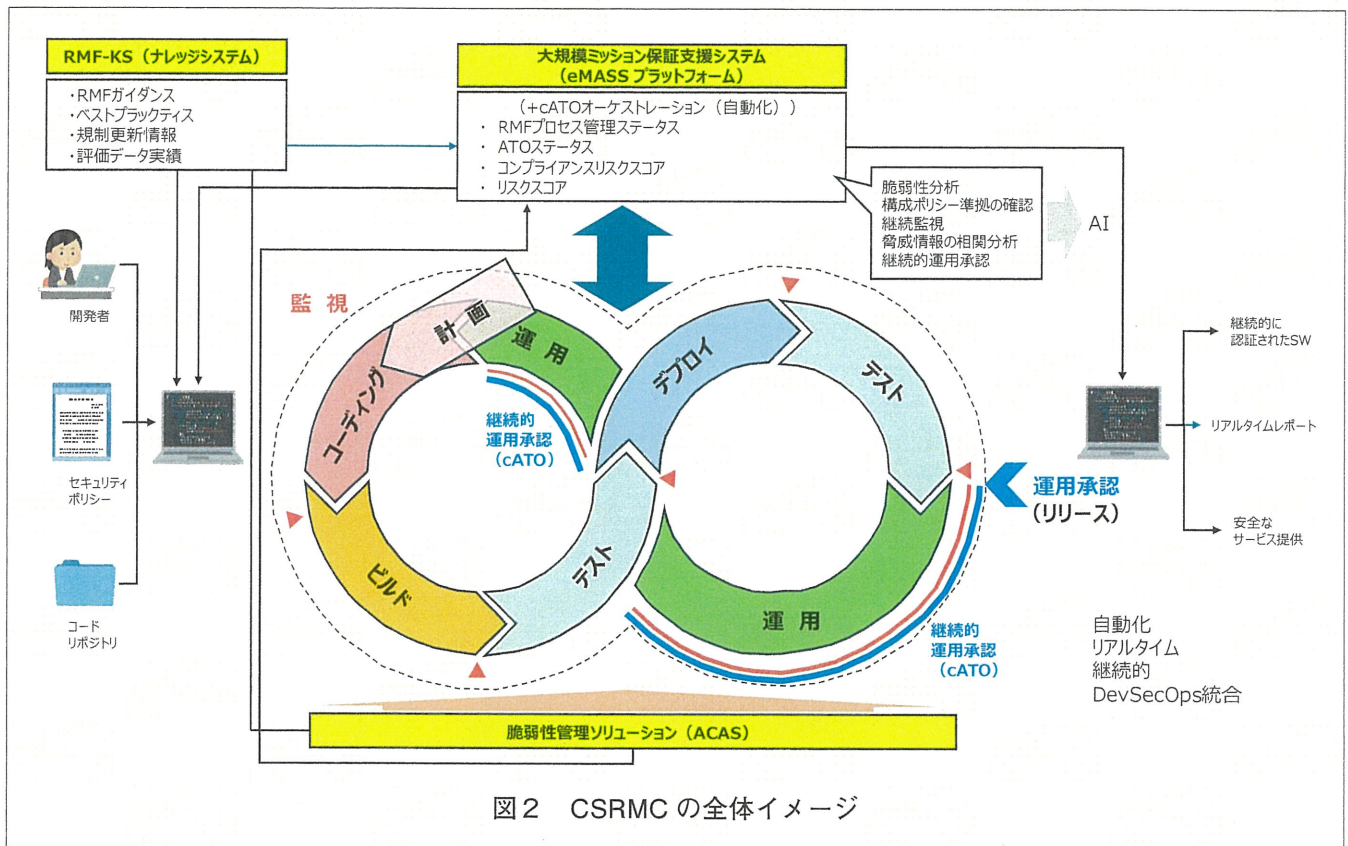
NATOでは、スペイン政府が情報システムのリスク分析と管理のために開発したMAGERIT手法²⁵⁾を基盤とする「PILAR」²⁶⁾というリスク分析・評価ソフトウェアが共通ツールとして広く活用され、相互運用性の向上に寄与しています。

NATOの現在の基本的な考え方は、2021年に提示されたNATO2030イニシアティブ²⁷⁾、

2022年の戦略構想、そして同年10月に合意されたNATOデジタル戦略ビジョン、更にその実現要領を具体化したNATOデジタル変革実施戦略²⁸⁾（2024年10月発表）といった一連の公式文書に示されています。同戦略では、戦場における優位性を確保するためには、全領域にわたる優勢の確立に加え、軍事活動の調整、非軍事活動の同期、そしてスピードの実現が必要であるとしています。

ランド研究所（RAND Europe）は、「NATOのデジタル能力の有効化」と題する2025年のペーパー²⁹⁾⁻³¹⁾において、調達プロセスの硬直化と非効率性、同盟国間の非対称性と優先順位の不一致、相互運用性とデジタル主権のジレンマなどの課題を指摘しています。これらはいずれも、かつて米国が認識したRMFにおける課題に加え、集団安全保障体制であるがゆえの難しさを含むものであり、険しい改革の状況が垣間見られます。

一方で、NATOで運用中のソフトウェアファクトリー³²⁾が、2026年2月にセキュリティ認証を更新したとのニュースもあり³³⁾、NATOに



においても既にソフトウェア開発、運用環境が整備・運用されている模様です³⁴⁾。

(3) 防衛省の状況

わが国の防衛省においては、令和9年度末に向けて、運用中の情報システムに対する運用承認手続きが佳境に入っています。これには、運用中のPITを伴う装備品の運用承認再取得のプロセスも含まれています。

そして、令和10年度に予定されているゼロトラスト導入や、令和11年度末に予定されている防衛省クラウド導入にあわせて、「RMF支援システム」の運用開始が計画されている模様です。脆弱性診断システムはCOTSとして一般的であることから、RMF支援システムは、eMASSにACAS（脆弱性診断システム）とRMF-KS³⁵⁾の機能を統合した機能を提供するものと考えられ、RMFに係る専門知見、セキュリティ管理策、審査文書、リスク分析・評価の実施状況、セキュリティ管理策の実施状況等を一元管理するとともに、申請、認証、監査等の

業務や関連手続きを支援することを目指している模様です³⁶⁾。

自動化、継続運用承認を実現するためには、DevSecOpsパイプライン、調達制度も含めた多くのハードルが存在しており、これらは今後の取り組む必要のある喫緊の課題です。

わが国を巡るトピック（GCAPを巡る考察）

(1) GCAPについて

GCAPはGlobal Combat Air Programの略であり、次世代戦闘機（第6世代戦闘機）を共同で開発・製造するための、日本とNATO加盟国である英国、イタリアによる国際協力プログラムであり、2035年までの配備開始を目指しています。2022年12月に参加国首脳が発出した「グローバル戦闘航空プログラムに関する共同首脳声明」により開始され、2026年4月には実務レベルの国際統合プログラムとして本格的に始動しました。

このプログラムでは、デジタル・エンジニア

リングを活用することに加え、人工知能（AI）、機械学習（ML）、ウェアラブル技術を取り入れることを始めとし、戦闘航空技術の開発と提供における新たなアプローチを推進していると言われています³⁷⁾。イタリアのレオナルド社は「この新しいシステム・オブ・システムズは、五つの領域にわたって運用され、次世代戦闘機をコアプラットフォームとして、有人および無人の周辺システムと接続される」と説明しています³⁸⁾。

英国とイタリアの間には、同盟関係に加え NATO-RMF の枠組みや STANAG³⁹⁾ といった共通基盤が存在しています。日米同盟を基盤として防衛力整備の仕組みを構築してきたわが国が、NATO 加盟国である英国とイタリアとの共同開発を進めることは、わが国のみならず、パートナー国にとってもチャレンジといえます。英 BAE システムズ社は HP にて「多様なサプライヤーによる技術的知識を活用するため、ハイテク中小企業とも提携することで技術開発を推進し、イノベーションを起こして最新スキルを GCAP にもたらす」と説明し、1,000 社以上のサプライヤーが同プログラムに参加していると発表しています。

(2) 開発基盤における情報共有にむけて

日英伊という地理的に離れた 3 カ国が、10年という限られた期間で第 6 世代戦闘機を完成させるためには、デジタル・エンジニアリングの活用が不可欠で、機体の設計から試験、製造に至るまでを仮想空間上で実施する手法を採用しているとされています。これを実現するには、日英伊の 3 カ国がネットワークで接続された協業環境を構築する必要があります。

しかし、戦闘機に関する情報は機密レベルが極めて高いため、各国からすれば「接続しなければ開発はできないが、接続すればリスクが増大する」といったジレンマが存在しています。また、国別・企業別・役職別といった粒度での緻密なアクセス制御をインフラ上に実装する必要性に加え、データ主権の課題もあり、これは

ルール形成をめぐる重要なポイントとなります。更に暗号アルゴリズムの選定、監査権限の範囲など調整課題も存在しています。

これらの認識を一致させるため、3 カ国は政府間機関である GIGO (GCAP International Government Organization) をロンドンに設立しています。更に、2025年には産業界による共同企業体である Edgewing が立ち上げられました。現在、これらの組織が中心となり、各国のセキュリティ基準の違いなどの課題を調整・吸収しつつ、統一された基準に基づくデジタル開発環境の構築に向けたすり合わせを進めている段階と推察されます。

(3) サイバーセキュリティにおけるリスク管理の観点から

今日、そして将来のソフトウェア技術および作戦環境を踏まえると、開発される戦闘機は、米国において F-35などで既に実現されている「ソフトウェアによる能力向上」の考え方が取り込まれているとみられ、継続的インテグレーション・デリバリ機能が必要です。その際、米国との相互運用性を確保するため、米国基準である DoD8510.01 (RMF) との整合が前提となります。そのため、NATO メンバーである英国、イタリアとわが国による共同開発の体制下で、cATO の仕組みをどのように構築し、いかに保持するかが共有する課題の一つであるといえます。

また多国籍多数の防衛ベンダーが参画するプロジェクトであるがゆえの課題として、厳格なソフトウェアのサプライチェーンリスク管理が必要であることから、SBOM⁴⁰⁾の仕組みの活用による、ライフサイクルにわたる構成要素の透明性の確保・管理が必要になると考えられます。

更にハードウェアの切り口で、将来の能力向上のためには MOSA⁴¹⁾の仕組み採用の公算が高く、モジュール交換にあたって、サイバーセキュリティのリスク管理に対する影響を局所化するためのモジュール設計とリスク評価の要領

の検討が必要になる可能性があります。

おわりに

わが国の安全保障は、これまで日米同盟を基軸としてきていますが、近年の国際環境の変化の影響を受け、2026年4月に防衛装備品移転における5類型が撤廃され、米国のみならず、NATOやAUKUS、東南アジア諸国をはじめとする同志国との連携の取組も、かつてないほど活発化しています。共同訓練に加え、わが国隊員のNATO司令部への派遣、装備品等の共同開発や移転など、その範囲は拡大し、内容も質・量ともに拡大していることが見てとれます。

マルチドメイン作戦、領域横断作戦の目指すところは、陸、海、空、宇宙、サイバーの複数の領域において競争相手（国）に対する優位性を確保するとともに、意思決定のスピードを加速させ、その相乗効果を通じて競争相手（国）にジレンマを与え、作戦上優越し勝利することです。その能力を保持する上で、領域の一つであると同時に死活的に重要な連携の基盤的機能

を提供するサイバー領域の安全を確保するサイバーセキュリティの管理の態勢は、その重要性を増しています。

また装備品等に関しても、ソフトウェア開発に関してはDevSepOpsパイプライン上での開発が一般的となり、防衛装備品の開発環境のトレンドはこれまでにないフェーズへと移行している状況であり、開発・調達には、「スピード」が必須の時代になっています。

わが国は、これまで米国とのバイラテラルな関係を基軸に抑止力を維持してきたことから、RMFをはじめとする諸制度についても米国の枠組みを参考にしています。一方で、近年の周辺の安全保障環境と不透明な国際情勢を踏まえると、平和と安全を確保するための選択肢を増やす必要があると考えられ、かかる視点から、GCAPの取組は大きな試金石の一つであり、併せてNATO-RMFの動向も今後の仕組みや制度を考える上で大変参考になるものと思われます。引き続き、これらの動向に注目していきたいと思います。

(2026年6月10日記)

参考文献・注

- 1) システム、ソフトウェア開発 (Development) から運用 (Operations) までの一連のプロセスに、セキュリティ (Security) を初期段階から統合させる開発手法のこと。
- 2) Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage Defense Innovation Board 2019, https://www.dmi-ida.org/download-pdf/pdf/SOFTWAREISNEVERDONE_REFACTORINGTHEACQUISITIONCODEFORCOMPETITIVEADVANTAGE_FINALSWAP.REPORT.PDF (Accessed on April 5, 2026)
- 3) DoD Enterprise DevSecOps Reference Design, Department of Defense (DoD) Chief Information Officer 2019, [https://dodcio.defense.gov/Portals/0/Documents/DoD Enterprise DevSecOps Reference Design v1.0_Public Release.pdf](https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf) (Accessed on April 5, 2026)
- 4) Department of Defense Software Modernization, Memorandum, DEPUTY SECRETARY OF DEFENSE 2022, <https://media.defense.gov/2022/feb/03/2002932833/-1/-1/1/departments-of-defense-software-modernization-strategy.pdf> (Accessed on April 5, 2026)
- 5) Continuous Authorization To Operate (cATO), Memorandum, OFFICE OF THE SECRETARY OF DEFENSE <https://media.defense.gov/2022/Feb/03/2002932852/-1/-1/0/CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF> (Accessed on April 5, 2026)
- 6) <https://dodcio.defense.gov/Portals/0/Documents/Library/cATO-EvaluationCriteria.pdf> (Accessed on April 5, 2026)
- 7) NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST 2011, <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf> (Accessed on April 5, 2026)
- 8) Immediate Release, Department of War Announces New Cybersecurity Risk Management Construct, U.S Department of War Sep. 24, 2025, <https://www.war.gov/News/Releases/Release/Article/4314411/departments-of-war-announces-new-cybersecurity-risk-management-construct/> (Accessed on April 5, 2026)
- 9) Request for Information 情報提供依頼
- 10) RFI - Next Generation of the Assured Compliance Assessment Solution (ACAS), <https://sam.gov/opp/f466c15e54de4ff590a8438cd1aef0c4/view> (Accessed on April 5, 2026)

- 11) ASSURED COMPLIANCE ASSESSMENT SOLUTION (ACAS), POWERED BY TENABLE, Tenable HP, https://www.tenable.com/sites/default/files/uploads/documents/whitepapers/Whitepaper-Assured_Compliance_Assessment_Solution_ACAS_Powered_by_Tenable.pdf (Accessed on April 5, 2026)
- 12) Government Off-The-Shelf の略。政府機関が自ら開発・所有する製品を指す。
- 13) MITRE ATT&CK とは、「現実世界の観測に基づいた、攻撃者の戦術と技術に関するグローバルにアクセス可能な知識ベース。ATT&CK 知識ベースは、民間企業、政府機関、サイバーセキュリティ製品・サービス業界において、特定の脅威モデルや手法を開発するための基盤として活用可能」とある。<https://attack.mitre.org/> (Accessed on April 5, 2026)
- 14) Enterprise Mission Assurance Support Service (eMASS), Request for Records Disposition Authority, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION HP, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/departments-of-defense/defense-agencies/rg-0371/daa-0371-2021-0001_sfl15.pdf (Accessed on April 13, 2026)
- 15) Assured Compliance Assessment Solution (ACAS), powered by Tenable, Tenable HP, https://dam.tenable.com/87d25774-8143-4bfd-b26d-b1d101055190/Assured_Compliance_Assessment_Solution_ACA_powered_by_Tenable.pdf (Accessed on 26 Apr. 2026)
- 16) DEPARTMENT OF DEFENSE “Data, Analytics, and Artificial Intelligence Adoption Strategy. Accelerating Decision Advantage” Office of Prepublication and Security Review, DoD 2023, https://media.defense.gov/2023/nov/02/2003333300/-1/-1/1/dod_data_analytics_ai_adoption_strategy.pdf (Accessed on Apr. 6 2026)
- 17) SUMMARY OF THE 2018 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY Harnessing AI to Advance Our Security and Prosperity, US Gov. HP, 2019, <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF> (Accessed on April 13, 2026)
- 18) Executive Summary: DoD Data Strategy Unleashing Data to Advance the National Defense Strategy, US Gov. HP, 2020, <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF> (Accessed on April 13, 2026)
- 19) Statst-of-the-Art Report の略。DoD の技術情報センター (DTIC) の下部組織である情報分析センター IAC (Information Analysis Centers)、特にサイバーセキュリティ分野を担当する CSIAC などが定期的に発行する、特定の技術分野に関する最も権威ある包括的な調査レポート。
- 20) Abdul Rahman, “Applications Of Artificial Intelligence (AI) for Protecting Software Supply Chains (SSCS) in The Defense Industrial Base (DIB)”, CSIAC-BCO-2023-499, CSIAC Jan.2024, https://csiac.dtic.mil/wp-content/uploads/2024/02/SOAR_CSIAC_Applications-of-Artificial-Intelligence-AI-for-Protecting-Software-Supply-Chains-SSCs-in-the-Defense-Industrial-Base-DIB_032724-contract.pdf (Accessed on Apr. 6 2026)
- 21) 同ドキュメントは、米国国立標準技術研究所 (NIST) のサイバーセキュリティ・フレームワークとの整合性や、SBOM (ソフトウェア部品構成表) を用いた透明性の確保について詳述するとともに、ブロックチェーンと AI の統合による改ざん防止や、DevSecOps パイプライン内でのコード信頼性向上など、革新的な技術アプローチを提示している。また AI 駆動のモニタリングが防衛ネットワークのコンプライアンス維持と迅速なインシデント対応に不可欠であることを結論付けている。
- 22) Security Technical Implementation Guides (STIGs), DoD Cyber Exchange Public, <https://www.cyber.mil/stigs/> (Accessed on Apr. 20 2026)
- 23) Intrusion Detection System の略。侵入検知システムは侵入を検知、通知を行うシステム。Intrusion Prevention System (侵入防御システム) は侵入を検知、自動遮断まで行うシステム。
- 24) Endpoint Detection and Response の略。端末を常時監視し、侵入や不審な挙動をリアルタイムで検知・分析し迅速に対処する仕組み。
- 25) Portal de la ADMINISTRACION Electronica, https://administracionelectronica.gob.es/pae_Home/dam/jcr:80b16a91-75b1-432d-ab23-844a12aab5fc/MAGERIT_v_3_book_1_method_PDF_NIPO_630-14-162-0.pdf (Accessed on April 14, 2026)
- 26) EAE/PILAR HP, <https://www.pilar-tools.com/en/> (Accessed on April 13, 2026)
- 27) <https://www.nato.int/en/news-and-events/events/transcripts/2021/06/04/nato-2030-a-transatlantic-agenda-for-the-future> (Accessed on April 14, 2026)
- 28) <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/17/natos-digital-transformation-implementation-strategy> (Accessed on April 14, 2026)
- 29) Judith Huismans, et al., 2025
- 30) Rebecca Lucas, et. Al, “Effective digital capability development, Enabling NATO digital capabilities series: Paper 1”, RAND Europe. 2025, https://www.rand.org/content/dam/rand/pubs/research_reports/RR43800/RR43831-2/RAND_RRA3831-2.pdf (Accessed on April 14, 2026)
- 31) Judith Huismans, et. Al, “Interoperability in the digital environment: opportunities and challenges, Enabling NATO digital capabilities series: Paper 1”, RAND Europe. 2025, https://www.rand.org/content/dam/rand/pubs/research_reports/RR43800/RR43831-3/RAND_RRA3831-3.infographic.pdf (Accessed on April 14, 2026)
- 32) 2022年に初回認証を受けた、ソフトウェアのセキュリティ確保、構築、テスト、移行、配信のための標準化された環境を提供するクラウド型 GOTS プラットフォーム。NATO は、同基盤は同盟国、産業界、学術界のパートナーとの緊密な連携とイノベーションの活用を可能とするものとしている。
- 33) “NATO Software Factory revalidated as trusted platform for secure digital delivery (Mar 27 2026)”, NATO-HP 2026, <https://www.ncia.nato.int/newsroom/news/nato-software-factory-revalidated-as-trusted-platform-for-secure-digital-delivery> (Accessed on April 14, 2026)
- 34) SAGE : Sonatype Air Gap Environment, <https://www.sonatype.com/sonatype-air-gapped-environment-overview> (Accessed on April 14, 2026)
- 35) RMF Knowledge Service の略。RMF の実施、計画、実行をサポートするための動的なオンライン知識データベース。セキュリティ制御ベースライン、オーバーレイ、個別のセキュリティ制御、実施ガイダンス、および評価手順にアクセス可能。

DoD のパブリックキーインフラストラクチャ (PKI) 証明書 (例: 共通アクセスカード) を持つ個人、または DoD スポンサーシップを持つ外部認証機関の証明書を持つ個人がアクセス可能。

DoD Instruction 8510.01: Risk Management Framework (RMF) for DoD Systems, July 19 2022, DoD HP, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf> (Accessed on April 15, 2026)

RMF KS のウェブサイト: <https://rmfks.osd.mil> (Accessed on April 15, 2026)

36) 公告 RMF 支援システムの技術支援役務, 防衛省HP, <https://www.mod.go.jp/j/budget/chotatsu/naikyoku/nyuusatu/2026/0204d.pdf> (Accessed on April 14, 2026)

37) Global Combat Air Program, BAE Systems HP, <https://www.baesystems.com/en-uk/product/global-combat-air-programme> (Accessed on April 14, 2026)

38) Global Combat Air Program (GCAP), Leonardo HP, <https://www.leonardo.com/en/business/gcap> (Accessed on April 14, 2026)

39) Standardization Agreement の略。NATO の加盟国間で、相互運用性を確保するために合意された技術仕様から運用手順までの多岐の分野にわたる軍事標準化規格。

40) Software Bill of Materials の略。オープンソースソフトウェア (OSS) が一般化する環境下において、ソフトウェアコンポーネントとその依存関係、コンポーネントに関する情報、およびそれらの階層的な関係性を正式かつ機械可読な形式で記録した目録でソフトウェアを構成する「部品のリスト (入れ子構造の目録)」として機能。機械可読であることから、大規模なデータを自動的に管理・処理することが可能。米国主導の規格。 <https://www.cisa.gov/sites/default/files/2024-10/SBOMFramingSoftwareComponentTransparency2024.pdf> (Accessed on 4 Jun. 2026)

(参考事項) NIST SP 800-53 (RMF セキュリティ管理策) Rev. 5 に管理策の一部として組み込み済

41) Modular Open System Approach の略。システムライフサイクル全体にわたって競争力のある、かつ費用対効果の高い調達と維持を実現するための、統合的なビジネスおよび技術戦略。オープンスタンダードを採用し、モジュール式、疎結合かつ高度に凝集したシステム構造をサポートする技術アーキテクチャからなる調達および設計戦略を取っている。また、モジュール設計を採用し、適合性を検証可能な標準規格に準拠したシステムインターフェースを含むシステム構成が可能となる。以上により、調達ライフサイクル全体を通してシステムコンポーネントの追加、変更、交換、削除が可能。 <https://www.cto.mil/sea/mosa/> (Accessed on 4 Jun. 2026)

米国においては2017年、国防権限法 (FY17 NDAA) 805条で法制化済、 <https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf> (Accessed on 4 Jun. 2026)

発売中

本誌に連載の「イラストでよむQ&A」が単行本になりました

防衛技術のジョーシキ!?

防衛技術ジャーナル編集部 編

・A5判 ・208頁 ・定価 (本体2,500円+税)

「火薬と爆薬の違いは？」と聞かれてすぐに答えられますか？
「どちらも爆発する怖い化学物質だし…」と考えている人は多いと思いますが誤解です。火薬はそれ自体で爆発しません。燃焼するだけなのです。一方の爆薬はダイナマイトに代表されるように、火薬の70万倍ものスピードで燃焼し爆轟します。このように何となくわいた疑問に答えるために多くの事例を集めてみました。本書のタイトルが『いまさら聞けない 防衛技術のジョーシキ!?』とあるように、防衛技術の研究者にとっても改めて参考になること請け合いなので、ぜひ座右に一冊置いてみてはいかがでしょうか。 (まえがき より)



一般財団法人 防衛技術協会

〒113-0033 東京都文京区本郷3-23-14 ショウエイビル9F TEL 03(5941)7620 FAX 03(5941)7651
<https://www.defense-tech.or.jp>