

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)

株式会社 Japan Aerospace & Defense Consulting

株式会社 SHIFT

菅野 隆

澤田 栄浩

第2回では「情報システムの運用段階におけるリスク管理枠組みの『監視』フェーズについて」と題し、運用段階における管理プロセスについて、訓令に沿って細部を解説しました。今回は、米国を含む多国籍同盟である北大西洋条約機構のRMFをトピックとした、「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)をお送りします。

はじめに

北大西洋条約機構 NATO (North Atlantic Treaty Organization) には、「CIS¹⁾ 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」と呼ばれる仕組みがあり、これは DoD8510.01 (リスク管理枠組み) と同じ役割を果たしています(本稿では、以降これを NATO-RMF と呼びます)。

本稿では、公開資料を基に、NATO のサイバーセキュリティに関する歴史と現状を整理し、NATO-RMF との現状を明らかにするとともに、米国の CSRMC (後述) の今後の方向性について述べます。更に、わが国の防衛省の状況に触れたうえで、最近の関連トピックとして GCAP²⁾ について、サイバーセキュリティリスク管理の側面から考察し、今後の業務に資することを目的としています。

NATO について

NATO は、1949年4月4日に設立された西

側の集団防衛機構です。原加盟国は、米国、英国、フランス、イタリア、カナダ、ベルギー、オランダ、ルクセンブルク、デンマーク、ノルウェー、ポルトガル、アイスランドの12ヵ国で、1952年にギリシャとトルコ、1955年に西ドイツ、1982年にスペインが加盟しました。冷戦後は1999年にポーランド、チェコ、ハンガリーが加盟したのを皮切りに2004年および2009年にも中・東欧諸国が相次いで加盟し、加盟国は29ヵ国となりました(2017年時点)³⁾。

その後、2020年3月に北マケドニア、2023年にフィンランド、2024年にスウェーデンが加盟し、現在は32ヵ国体制となっています。2022年のロシアによるウクライナ侵攻以降、対ロシア抑止力は強化されていると評価できます⁴⁾。

NATO は現在、2022年版戦略概念⁵⁾ に規定されているとおり、①集団防衛②危機予防・管理③協力安全保障の三つを中核的任務としています⁶⁾。

旧ソ連が冷戦期にイデオロギーを共有していた旧ワルシャワ条約機構の東欧諸国の NATO 加盟は、徐々に進んでいきました。一般的な見方として、ロシアの視点からは、旧西側との間

の緩衝地帯が縮小・消滅してきたことを意味し、その拡大は受け入れがたい状況だと捉えている模様です。とりわけロシアによるウクライナ侵攻開始以降、関係国においてはロシア系住民をめぐる緊張が一定程度高まっているのが現状です。

サイバーセキュリティを巡る NATO の歴史

(1) 冷戦期から1990年代

冷戦期から1990年代にかけての NATO における情報セキュリティの主流は、列国と同様、情報セキュリティ Information Security (INFOSEC) でした。これは主に、暗号化 (COMSEC)、コンピュータの物理的隔離 (COMPUSEC)、電磁波漏洩対策 TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions) など、機密性 (Confidentiality) の確保に特化した静的なコンプライアンス重視のアプローチでした。

1999年1月、NATO はコソボ紛争への介入を開始しました。これに伴い、NATO 非加盟国や国際機関との情報共有の機会が増加し、情報開示基準やセキュリティ保証手続きをシステム化する必要性が高まりました。また同年3月には、冷戦期にワルシャワ条約機構に属していたポーランド、ハンガリー、チェコが NATO に加盟しました。当時、その後の大規模な拡大も予期されており、旧東側国家を同盟のシステムに統合して情報を共有するためには、情報の保護レベルを再定義し、同盟内で徹底する必要性が生じていました。

更に、同年4月下旬に開催された NATO ワシントンサミットで採択された戦略概念では、冷戦終結後の新たな安全保障環境に対応するため、従来の「集団防衛」に加え、紛争管理（危機予防）や対外パートナーシップ（協力安全保障）などの「域外任務」を重視する方針が示されました。

こうした状況の中、同年5月には NATO に

よるベオグラードの中国大使館誤爆事件が発生しました。その後の欧州連合最高司令部 SHAPE (Supreme Headquarters Allied Powers Europe) および米軍のウェブサイトは、ロシア、セルビア、中国を支援する活動家らにより、初めてサイバー攻撃（改ざん攻撃、サービス妨害攻撃）を受けることになります⁷⁾。

(2) 2000年代

2001年9月、NATO 加盟国である米国において同時多発テロが発生しました。NATO は、サイバー脅威への認識の高まりと、これまでに発生していたサイバー攻撃の教訓などを踏まえて、2002年のプラハサミットにおいて「サイバー防衛プログラム」の推進と能力強化を宣言し⁸⁾、サイバー攻撃を監視・検知し、インシデントに即応するための技術・運用専門機関として、サイバー事案対応能力組織 NCIRC (NATO Computer Incident Response Capability) を設立しました⁹⁾。

加えて、同年、C-M¹⁰⁾ (2002) 49 「Security within the North Atlantic Treaty Organization」を発表しました。同ドキュメントは、1955年3月2日に運用開始された旧枠組み C-M (55) 15 (Final) を刷新するものでした。なお C-M (2002) 49は、C-M (2002) 50 「Protection Measures for NATO Civil and Military Bodies, deployed NATO Forces and Installations (Assets) against Terrorist Threats」と同時に発出されていることから、同時多発テロの発生がその策定の契機の一つだったことが窺えます。

C-M (2002) 49では、情報保証の概念が導入され、暗号、ネットワーク保護、サイバー防御を含む CIS (Computer and Information System) セキュリティ (Enclosure F) および「セキュリティ認定プロセス」が確立されました。これにより、ガバナンス（予防）とオペレーション（対応）の双方にわたる基本的な態勢・体制が実装されました。

2007年4月から5月にかけて、エストニアに

対し大規模なサイバー攻撃が実施されました¹¹⁾。同事案では、政府、メディア、銀行システムなどが標的となり、現代的サイバー紛争の先駆的事例として広く認識されています。またハイブリッド脅威¹²⁾への警鐘ともなり、「サイバー攻撃は国家の安全保障を脅かす現実の脅威である」との認識がNATO全体で共有される契機となりました。

2008年のブカレストサミットにおいて、NATOは「サイバー防衛政策」を策定し、サイバー空間における同盟の基本方針を初めて打ち出しました。これにより、従来は「国家の自助努力」と位置付けられていたサイバー防衛が、「同盟全体の優先事項」へと格上げされました。同政策では、リスク管理の共通化と認可プロセスの重要性が確認されています。そして、同サミットの成果を受け、2008年には「サイバー防衛管理局」CDMA (Cyber Defense Management Authority) が設立され、サイバー運用能力の一元化が進められました。また同年5月にはエストニアにNATOサイバー防衛協力センターCCDCOE (Cooperative Cyber Defense Centre of Excellence) が設立されるに至りました¹³⁾。ブカレストサミットは、サイバーセキュリティに関するNATOの体制と方針を強化する重要な転換点であったと評価されています¹⁴⁾。

(3) 2010年代

2010年のリスボンサミットにおいて、冷戦後のNATOの役割は再定義され、サイバー脅威への対応も戦略概念に組み込まれました¹⁵⁾。

2014年には、ウクライナのクリミアおよびドンバス地域において確認されたサイバー攻撃が警鐘となり、NATOは同年9月のウェールズサミットにおいて、サイバー攻撃が武力攻撃に匹敵する深刻な影響を及ぼす場合には、北大西洋条約第5条（集団防衛）の発動対象と成り得ることを公式に宣言しました。あわせて、脅威情報の共有や技術革新促進を目的に、民間企業と

の連携強化を決定しました（NATO産業サイバーパートナーシップNISP (NATO Industry Cyber Partnership)¹⁶⁾）。

2016年2月には、NATOのサイバー事案対応能力組織 (NCIRC) とEUのサイバー緊急対応チーム (CERT-EU) の間で、情報共有や訓練、演習における協力を強化するための合意がなされました。同年7月のワルシャワサミットでは、NATOは陸・海・空に加え、「サイバー空間」を作戦領域（ドメイン）と認定し、運用することを決定しました。これは、サイバー空間において防衛任務を遂行するための法的根拠となりました。更に、各加盟国は、自国のネットワーク保護とレジリエンス能力を最優先で向上させるための「サイバー防衛の誓約」に署名し、その実装に合意しました¹⁷⁾。

2018年7月のブリュッセルサミットでは、サイバー領域を加盟国の防衛に効果的に組み込むため、サイバー作戦センター (Cyber Operations Centre) の設立が決定されました¹⁸⁾。

(4) 2020年以降

2021年、ブリュッセルサミットにおいて、NATOは三つの中核任務と、同盟全体の抑止・防衛態勢を支援するための新たな包括的ポリシーを承認しました。加盟国はNATOの防衛的権限を再確認するとともに、サイバー脅威に対しては集団的対応を含め、あらゆる能力を駆使して積極的に抑止・防衛するとのコミットメントを発表しました¹⁹⁾。

2022年6月のマドリードサミットで採択された戦略概念には、サイバー空間が「絶えず争われる領域」であることが明記されました。またサイバー攻撃が北大西洋条約第5条の発動要件になり得ることが再確認され、仮想サイバーインシデント支援能力部隊VCISC (Virtual Cyber Incident Support Capability) の設置が合意されました²⁰⁾。

2023年7月のヴィリニウスサミットでは、新たなサイバー防衛強化コンセプトが承認され、

各国が保有するサイバー作戦能力を同盟全体の集団防衛や軍事作戦にいかに関与するかが焦点となりました。また民間インフラの脆弱性が軍事作戦に影響を及ぼさないよう、軍民連携を強化する方針が確認されました²¹⁾。

2024年7月のワシントンサミットでは、NATO 統合サイバー防衛センターNICDC (NATO Integrated Cyber Defense Centre) の設立が合意されました。同センターは、サイバー領域を作戦ドメインとして統合的に指揮する中核機関となることが期待されています²²⁾。

2025年6月のハーグサミットでは、ウクライナ情勢の長期化とハイブリッド脅威への対応を背景として、加盟国の国防費目標がGDP比2%から5%に引き上げられました。このうち1.5%相当分は、重要インフラの保護、デジタルネットワークの防衛および市民のレジリエンス強化に充てられることとされており、注目すべき動向となっています^{23), 24)}。

NATO-RMF の概要、進化過程と課題

(1) NATO-RMF の概要

ア 根拠となるドキュメント

NATO Security Policy (NATO セキュリティポリシー) は、NATO 理事会により承認される最高位のセキュリティ方針です。

その下位規定である Directive on CIS Security (CIS セキュリティに関する指令) は、セキュリティ方針のうち、特に NATO 加盟国やパート

ナー国との間で機密情報を安全に処理・保存・伝送するための通信情報システムを保護することを目的としています。同指令は、IT システムおよびネットワークの保護に特化し、より具体的な実装手順や要件を定めた文書です。そして、この指令の中核をなすのが、セキュリティ認可プロセスです。

イ 基本指針

AC²⁵⁾/35-D/2004-REV3 “Primary Directive on CIS Security”²⁶⁾ の第7章は、CIS のセキュリティ認可プロセスおよびライフサイクル (The Security Accreditation Process and The Security Life Cycle of a CIS) を規定するものであり、NATO-RMF を定義する実務上最も重要なセクションです。同章は、その概念と基本原則を明確化するとともに、ネットワークやシステムの運用開始に先立つ認可に関する法的・手続き的な枠組みを定めています。セキュリティ認可プロセスは、CIA トライアド²⁷⁾を確保することを目的として、システムのライフサイクル全体を通じた継続的プロセスとして整理されています。基本構成は、①定義②リスク評価③設計・実装④評価⑤認可の五つのフェーズからなっています。

ウ 管理指針

AC/35-D/2005-REV3 “Management Directive on CIS Security”²⁸⁾ の第5章では、認可当局 SAA (Security Accreditation Authority) が認可 SSA (System Security Authorization) を行うにあたり、システムの開発・運用部門が提出

表1 セキュリティ認可を得るために開発、運用サイドが提出する資料

ドキュメント名	説明
SSRS (System-specific Security Requirements Statement: システム固有セキュリティ要件書)	対象となるシステムが、NATO の全体的なセキュリティポリシーに沿って「何を、どのように守るべきか」を具体的に定義した仕様書
ST&E Plan and Report (Security Test and Verification Plan and Report: セキュリティテスト・検証計画および報告書)	SSRS で定められたセキュリティ要件や対策が、実際のシステム上で正しく実装され、機能しているかを検証(テスト)するための計画と、その客観的な結果を示す証拠となる報告書
SecOps (Security Operating Procedures: セキュリティ運用手順書)	システムの日常運用において、セキュリティをどのように維持し、ユーザーがどう振る舞うべきか、またインシデント発生時にどのような手順で対応するかを定めた詳細な運用マニュアル

表2 認可にあたり求められる管理要件

管理要件	細部事項
1. セキュリティ運用手順 (SecOPs) の策定と順守	・セキュリティの管理および組織体制 (連絡先を含む) ・人的セキュリティ、物理的セキュリティ、情報セキュリティの規定 ・CISセキュリティの規定 ・インシデントおよび緊急時の対応手順 ・構成管理 ・利用規程
2. アカウントおよびアクセス権の実務管理	・権限の確認と記録 ・パスワード管理 ・職務の分離
3. 日常的な監視とインシデント・事業継続対応	・ログの監視 ・インシデント管理 ・事業継続とバックアップ
4. 記憶媒体および機器の実務的統制	・記録媒体の厳格な管理 ・私物機器の利用禁止
5. セキュリティ実装と構成の管理 (変更管理)	・変更時の影響レビュー ・自動化ツールによる継続的評価

表3 CIS セキュリティにおける中核的な三つの運用コンセプト

運用コンセプト	説明	規定先
多層防御 (Defense-in-Depth)	NATO のシステム設計における「根本的なアーキテクチャ原則」。単一のセキュリティ対策 (例: ファイアウォールのみ) に依存せず、ネットワーク境界、システムホスト、アプリケーション、データレベルで複数の防御層を重ねるという戦略的方针。	AC/35-D/2004-REV3 "Primary Directive on CIS Security"
暗号化製品の統制 (Control of Cryptographic Products)	NATO 機密情報 (NATO Classified Information) を電子的に処理・伝送するためには、NATO によって公式に承認された暗号化製品 (SECAN 等による承認) のみを使用しなければならないというポリシー。これはシステム認可における前提条件 (トラストの根幹)。	
継続的な構成管理と再認可 (Continuous Configuration Management and Re-accreditation)	システム稼働後の「変更管理」と「認可状態の維持」という、日々の実務・運用管理に関するプロセス。 システムの構成が変更された場合 (パッチ適用、機器の追加、ネットワークの変更など) にセキュリティ態勢をどう維持するか、また、どのような重大な変更が加えられた場合に SAA (認可当局) による「再認可 (Re-accreditation)」の手続きを踏まなければならないのかといった実務的な管理要件の規定を包含。	AC/35-D/2005-REV3 "Management Directive on CIS Security"

すべき文書 (表1)、求められる管理要件などについて定めています (表2)。

以上の2文書は、NIST SP800-37のドキュメントに相当します。これらの規定が重視する中核的な三つの運用コンセプトを表3に示します。

エ RMF の比較

DoD の RMF は、米国 NIST (国立標準技術研究所) のガイドライン (SP 800-37等) をベースにしているのに対し、NATO-RMF の包括的な仕組みは、加盟国間で合意された前述の独自のセキュリティ指令に基づいています。

なお、わが国の防衛省の RMF 導入については2022年12月に閣議決定された安保三文書 (防衛力整備計画) において宣言されていますが、その背景には、近年の周辺地域の緊張の高まりとそれに連動したサイバー脅威の高まり、それらに対応するための日米間の相互運用性や、情報共有態勢を確保するための必要性があると考えられます。

図1に NATO-RMF の文書体系、サイクル、ガバナンスを、図2に DoD-RMF を、図3に防衛省-RMF をそれぞれ整理します。

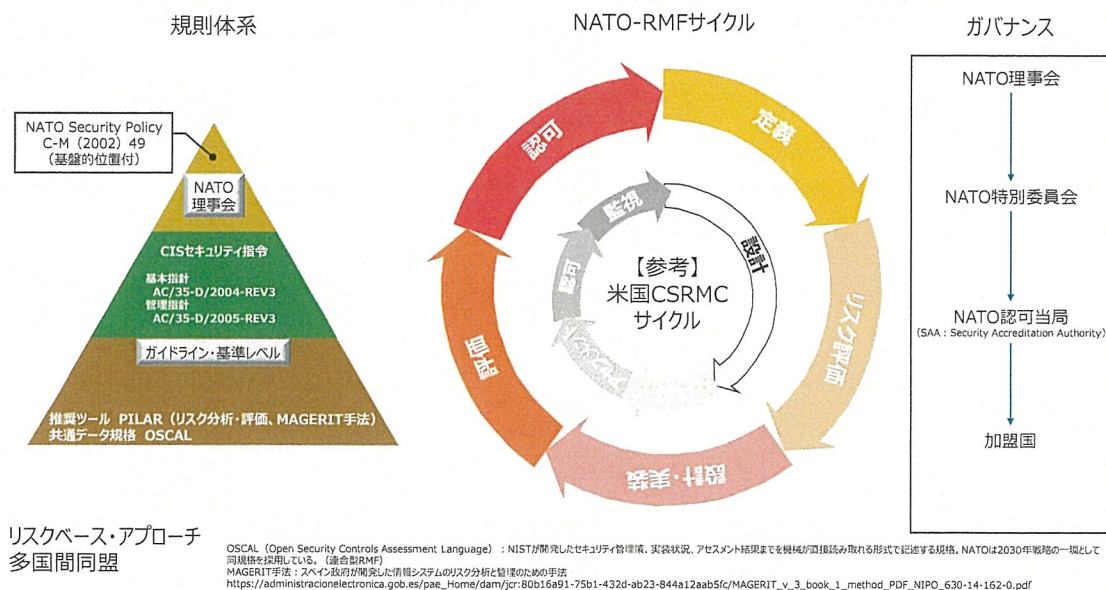


図1 NATO-RMFの文書体系、サイクル、ガバナンス

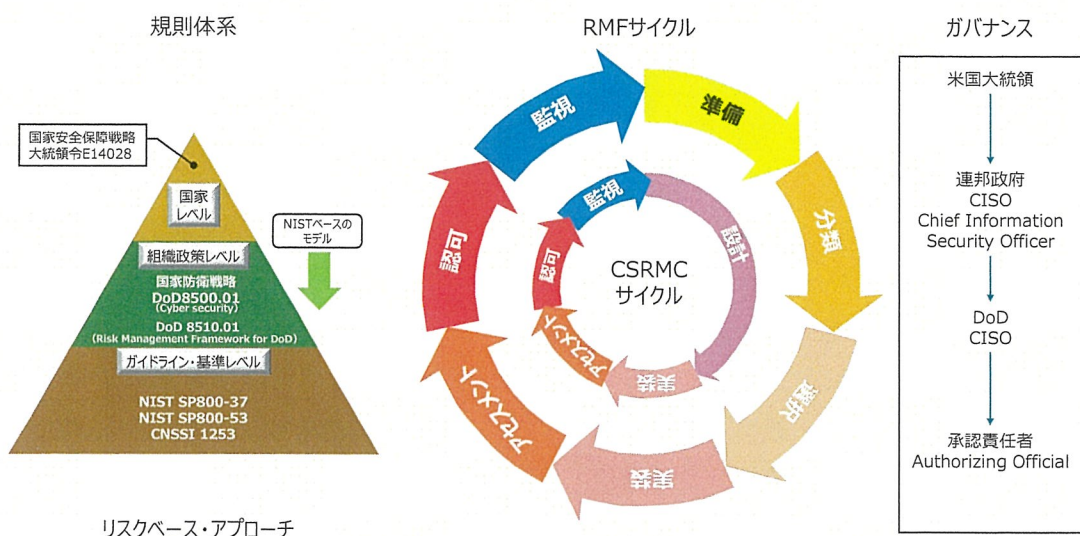


図2 米国 RMF の文書体系、サイクル、ガバナンス

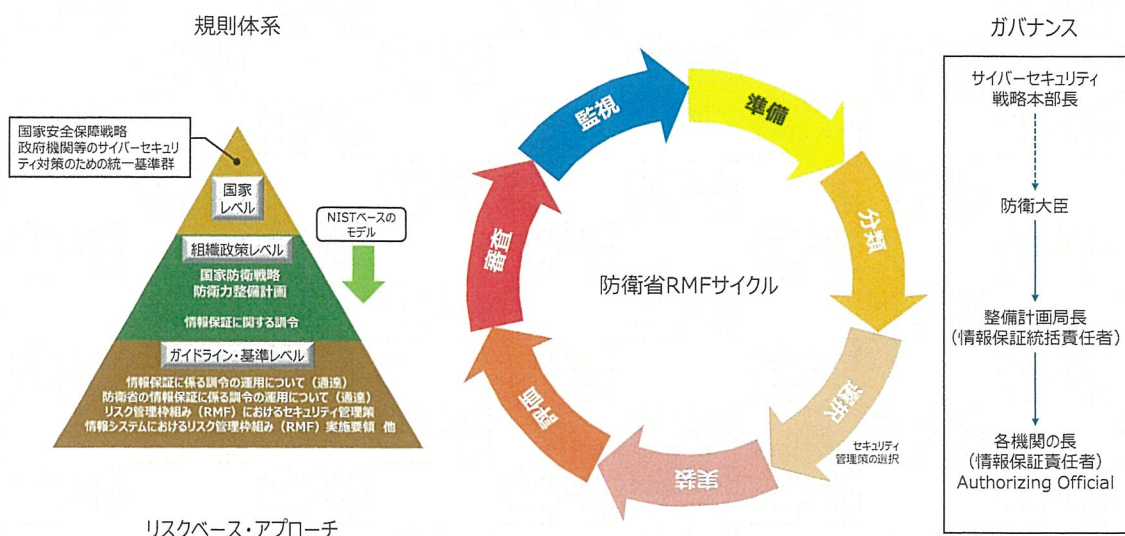


図3 防衛省 RMF の文書体系、サイクル、ガバナンス

(2) NATO-RMF の進化過程

前節の「サイバーセキュリティを巡る NATO の歴史」において、NATO のサイバーセキュリティにかかる大きな流れを概観しましたが、ここでは NATO-RMF に焦点を絞ります。NATO は、概ね以下の三つのフェーズを経て、兵器システムを NATO-RMF の対象に取り込むに至りました。

ア フェーズ 1：CIS 防衛の時代（2002～2016年）

NATO-RMF は2002年に公表され、CIS を対象として取組みを開始しました。兵器システムについては独立した「クローズドなシステム」と見なされ、RMF の対象からは除外されていました。

イ フェーズ 2：作戦ドメインとしての認識（2016～2021年）

2016年のワルシャワサミットにおいて、サイバー空間が作戦ドメインとして認定されたことにより、CIS のみならず、作戦に直接関わる軍事システム全体（PIT を伴う兵器を含む）についてもリスク管理が必要であるとの認識が強まりました。このフェーズでは、加盟国間でサイバー脅威情報を共有するための規格や手続きの検討が開始され、手続き的相互運用性の基盤整備が進められました。

ウ フェーズ 3：兵器システムのレジリエンスと統合の時代（2022年～現在）

NATO がサイバーセキュリティリスク管理の対象として、兵器システムや PIT を明確かつ包括的に取り込み始めた背景には、2022年の戦略概念の採択があります。同概念では、兵器システムを含む全ドメインの軍事能力のサイバーレジリエンス確保が最優先事項の一つと位置づけられ、これが大きな転換点となりました。

また加盟国の兵器システムにおける脆弱性は、同盟全体の作戦遂行を損なうリスクとなり得ることから、多国籍統合に向けた標準化が不可欠となりました。このため NATO は、加盟国に対し、自国の兵器システムに対するアセス

メント結果を共通データ規格（OSCAL²⁹⁾など）で提出することを、継続的監視（ISCM³⁰⁾の一環として求め始めています。

(3) RMF による負担増加の顕在化

NATO が RMF における現場の疲弊を顕著な問題として明確に認識し、その対策へと大きく舵を切ったのは、DoD とほぼ同時期である2020年代初頭、特に2021年から2022年にかけてとされています。この時期、NATO の主要な戦略文書や技術文書において、RMF プロセスがもたらす「過度な負担」と「作戦スピードとの乖離」が指摘されるようになりました。

その限界は、「紙ベースの手動作業による疲弊」、NATO 特有の「多国籍環境における互換性の欠如」という二つの側面で顕在化しました。従来の静的な RMF は、現場にとって終わりのない書類作業となり、DoD と同様に迅速な能力配備を阻害するボトルネックとなっていることが明らかになりました。他方で、クラウドや DevSecOps（開発・セキュリティ・運用の統合）の普及により、兵器システムや CIS システムにおけるソフトウェア更新の頻度が技術的には「数年単位」から「数日～数時間単位」へと大幅に短縮しており、両者のギャップは拡大していました³¹⁾。

2016年のワルシャワサミットで、NATO がサイバー空間を作戦ドメインと認識したことを受け、加盟国間でのサイバー脅威情報の共有が本格化しました。しかし、各国はそれぞれ独自の RMF 規格（例：フランス ANSSI、ドイツ BSI、米国 NIST）を採用しているため、「どのリスク情報が重要か」を相互に翻訳・調整する作業に膨大な負担が生じ、現場は混乱と疲弊に直面したといわれています。このことは、多国籍間での相互運用性の欠如という構造的課題を浮き彫りにしました。

更に、2022年のマドリッドサミットで採択された戦略概念では、「マルチドメインにおける軍事能力のレジリエンス」が強調され、各国は負

表4 NATO のサイバーセキュリティ・リスク管理枠組みに係る年表

[illegible]

担増大への対応も求められるようになりました。

これまで説明した経緯を、表4に整理します。

(つづく)

参考文献

- 1) NATO Standard AJP-6, ALLIED JOINT DOCTRINE FOR COMMUNICATIONS AND INFORMATION SYSTEMS, Edition A Version, Feb. 2017, https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDA_V1_E_2525.pdf (Accessed on March 30, 2026)
通信システムとは「情報の伝達（転送）を達成するために組織された機器、方法、手順および必要に応じた人員の集合体」、情報システムとは「情報の処理機能を達成するために組織された機器、方法、手順及び必要に応じた人員の集合体」を指す。CISは、これら通信システムおよび情報システムを合わせた総称。日本国内では、防衛省の情報システム（ハードウェア、インフラ）に、それを運用する要員を含めたものを「システム」と定義している。
- 2) Global Combat Air Program の略。日、英、伊による第6世代戦闘機共同開発プログラム。
- 3) 小笠原高雪 他「国際関係・安全保障用語辞典（第2版）」P.65, ミネルヴァ書房, 2017より、以下引用。
「本部はブリュッセル、最高意思決定機関は北大西洋理事会で、その下に統合軍事機構を擁す。冷戦期の脅威はソ連を盟主とするワルシャワ条約機構であり、その主な任務は集団防衛であった。冷戦後は3度の戦略概念の改訂を経て、テロ、大量破壊兵器の拡散、民族紛争、組織的犯罪等を主要な脅威とし、集団防衛のほか、危機管理と協調的安全保障を主任務とする地域機構へと変容。（中略）なお、2014年のウクライナ危機以降は、対ロシア抑止のための戦力編成、前方展開プロセスなどを通じ、集団防衛機能見直しの動きもみられている。」
- 4) 「北大西洋条約機構（NATO）について」外務省欧州局政策課, 令和8年1月, 外務省 HP, <https://www.mofa.go.jp/mofaj/files/100156880.pdf> (Accessed on March 30, 2026)
- 5) NATO の「戦略概念」は通常約10年ごとに更新される最重要指針。現時点での最新版は2022年6月に採択された「2022年版戦略概念（2022 Strategic Concept）」。
- 6) The North Atlantic Alliance (NATO), Federal Foreign Office HP <https://www.auswaertiges-amt.de/en/aussenpolitik/internationale-organisationen/nato-node/north-atlantic-alliance-218796> (Accessed on April 3, 2026) (Accessed on April 13, 2026)
- 7) Melia Pfannenstiel, Dan Cox, “NATO’s Cyber Era (1999–2024) Implications for Multidomain Operations”, Military Review, Army University Press, 2024, <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/NATOs-Cyber-Era-UA/> (Accessed on April 13, 2026)
- 8) Prague Summit Declaration, North Atlantic Council in Prague HP, 2002, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/21/prague-summit-declaration> (Accessed on April 3, 2026)
- 9) Jason Healey and Leendert van Bochoven, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.” Issue Brief, Atlantic Council HP, Feb. 27, 2012, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/natos-cyber-capabilities-yesterday-today-and-tomorrow/> (Accessed on April 3, 2026)

- 10) 「C-M」は NATO 文書コード、北太平洋理事会 (NAC) が発行する「Council Memorandum (理事会メモランダム)」を指す。政策策定や決定通知に使われる包括的な公式文書シリーズ。
- 11) 2007 cyber-attacks on Estonia, NATO Strategic Communications Center of Excellence, https://stratcomcoe.org/uploads/pfiles/cyber_attacks_estonia.pdf (Accessed on April 13, 2026)
- 12) ハイブリッド戦の脅威を指す。
「ハイブリッド戦：軍事と非軍事の境界を意図的に曖昧にした現状変更の手法。相手方に軍事面にとどまらない複雑な対応を強いる。例えば、国籍を隠した不明部隊を用いた作戦、サイバー攻撃による通信・重要インフラの妨害、インターネットやメディアを通じた偽情報の流布などによる影響工作を複合的に用いた手法が、「ハイブリッド戦」に該当。」
引用元：令和元年版防衛白書、防衛省 HP http://www.clearing.mod.go.jp/hakusho_data/2019/html/nc007000.html (Accessed on April 14, 2026)
- 13) NATO opens new center of excellence on cyber defense, NATO HP, 14 May 2008 <https://www.nato.int/en/news-and-events/articles/news/2008/05/14/nato-opens-new-centre-of-excellence-on-cyber-defence> (Accessed on April 13, 2026)
- 14) Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008, NATO HP, 03 April 2008, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2008/04/03/bucharest-summit-declaration> (Accessed on April 13, 2026)
- 15) Active Engagement, Modern Defense Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon, NATO HP, 19 November 2010, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2010/11/19/active-engagement-modern-defence> (Accessed on April 13, 2026)
- 16) Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, NATO HP, 05 September 2014, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration> (Accessed on April 13, 2026)
- 17) Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, NATO HP, 09 July 2016, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique>
- 18) David A. Wemer, “Behind the din over defense spending, NATO was hard at work in 2018.” NATOat70, Atlantic Council HP, March 21, 2019, <https://www.atlanticcouncil.org/blogs/new-atlanticist/behind-the-din-over-defense-spending-nato-was-hard-at-work-in-2018/>
- 19) Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, NATO HP, 14 June 2021, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communique>
- 20) NATO 2022 Strategic Concept, NATO HP, Updated: 03 March 2023, <https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept> (Accessed on April 13, 2026)
- 21) Vilnius Summit Communiqué Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023, NATO HP, 11 July 2023, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique> (Accessed on April 13, 2026)
- 22) Washington Summit Declaration Issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. 10 July 2024, NATO HP, 10 July 2024 <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration> (Accessed on April 13, 2026)
- 23) Key decisions, Overview-2025 NATO Summit in The Hague, NATO HP, 2025, <https://www.nato.int/en/news-and-events/events/2025/6/overview---2025-nato-summit-in-the-hague> (Accessed on April 13, 2026)
- 24) The Hague Summit Declaration issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in The Hague 25 June 2025, NATO HP, 25 June 2025 <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration> (Accessed on April 13, 2026)
- 25) Ad Hoc Committee の略。特別委員会 / 臨時委員会。
- 26) Security Committee Primary Directive on CIS Security Noted by the Chairman, 15 Nov. 2013, Nato Atlantic Council, <https://nbu.gov.cz/download/pravni-predpisy---nato/container-nodeid-819/ac35-d2004-rev3.pdf> (Accessed on April 3, 2026)
- 27) CIA Triad の略。情報セキュリティの 3 原則〔機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability)] を指す。
- 28) Security Committee Management Directive on CIS Security Noted by the Chairman, 12 Oct. 2015, Nato Atlantic Council, https://archives.nato.int/uploads/r/nato-archives-online/b/e/9/be9006a3ba28928df0b75e4f24fac7ad694b6f68edf464dca90ddf83f5399cd7/AC_35-D_2005-REV3_ENG_NHQR17300.pdf (Accessed on April 13, 2026)
- 29) Open Security Controls Assessment Language の略。NIST が開発したセキュリティ管理策、実装状況、アセスメント結果までを機械が直接読み取れる形式で記述する規格。NATO は 2030 年戦略の一環として同規格を採用している。
- 30) Information Security Continuous Monitoring の略。システムの認可 (ATO) を維持するために、あらかじめ定義されたセキュリティ管理策が正しく機能しているかを常に確認すること (NIST SP 800-137)。
- 31) Judith Huismans, et Al, “Conceptualising digital Capability, Enabling NATO digital capabilities series: Paper 1”, RAND Europe. 2025, https://www.rand.org/content/dam/rand/pubs/research_reports/ RRA3800/RAA3831-1/RAND_RRA3831-1.pdf (Accessed on April 14, 2026)