短期連載

RMFシリーズ　第1回

米国の情報保証／サイバーセキュリティ確保のための枠組みの変遷とサイバーセキュリティリスク管理構造（CSRMC）について

株式会社 Japan Aerospace & Defense Consulting
株式会社 SHIFT
菅野　隆　　澤田　栄浩

本誌2026年１月号では、「防衛省自衛隊の情報システムに対するリスク管理枠組みの導入と情報デバイスを伴う既存の装備品に対する適用のポイント」を掲載しました。今回は、リスク管理枠組みRMF（Risk Management Framework）の関係者に加えて運用者も対象とし、最新のオープンソースに基づき、米国の情報保証／サイバーセキュリティ確保のための枠組みの変遷と、米国が2025年９月に導入開始を宣言したサイバーセキュリティリスク管理構造CSRMC（Cyber Security Risk Management Construct）について、時系列に沿ってできるだけ分かりやすく解説するため、RMFシリーズとして連載することにしました。RMFの現状について理解を深めて頂ければ幸いです。　（編集部）

はじめに

米国において広域コンピュータネットワークであるARPANETの技術的基盤が整い、実質的にインターネットへと進化したとされる1983年以降、同ネットワークへの接続は省庁、学術機関などに拡大しました。その後、1989年に「インターネット」と改称され民間に開放されたことで、利用者数は爆発的に増加しました。更に1990年代に入ると、大学や政府機関を対象としたサイバー攻撃（ワーム、ハッキング）[1]が初めて発生し、サイバーセキュリティ対策の必要性について米国連邦政府機関に警鐘を鳴らすこととなりました。

21世紀に入り、2001年９月11日、米国同時多発テロが発生。当時の米国ではこのイベントを「パラダイムシフト」、つまり未曽有の変化をもたらしたと認識し、その教訓を踏まえて取組を推進しました[2]。独立調査委員会の最終報告書[3]では、「冷戦型の安全保障の各種制度を見直す必要がある」と指摘した上で、新たな脅威（テロ）に対応するための国の情報組織体制や機能の強化を中心とした提言がされています。

サイバーセキュリティにおいても同様に、省庁ごとの個別対応など類似の課題が存在しており、これらの事件等を契機として、2002年12月、連邦情報セキュリティ管理法〔FISMA法（2002年電子政府法（E-Government Act of 2002）「第３編（Title Ⅲ）」〕[4]が成立しました。同法は、米国国立標準技術研究所NIST（National Institute of Standard Technology）に対し、連邦政府が同法に準拠するための取組の支援を義務付けた上で、連邦政府各機関に対して、情報および情報システムのセキュリティを強化するためのプログラムを開発、文書化、実践することを求めました。

これを受け、NISTは2003年１月に「FISMA法導入プロジェクト」を立ち上げ、連邦政府の情報セキュリティ強化に寄与するため、情報システムのセキュリティを強化し安全に運用するための様々な規格・ガイドラインを策定し公表

を開始しました[5]。

米国の情報保証／サイバーセキュリティ確保のためのプロセスの変遷（RMFまで）

(1) 国防情報技術セキュリティ認証・認定プロセス（DITSCAP）

国防省は、米軍の情報システムが運用環境において必要かつ十分なセキュリティ要件を満たしているかを、標準化した手法により評価した上で運用認証を行うため、1997年に国防省指令（DoDI5200.40）を発令し、DITSCAP（Defense Information Technology Security Certification and Accreditation Process）の実行を指示しました。

DITSCAPのプロセスは、定義、検証、妥当性確認、認定の四つのフェーズで構成されていました。システム導入当初にシステムのセキュリティを実装および評価して以降、システムが廃止または交換されるまで新たな評価は行われない仕組み[6]となっているなどの課題はありましたが、FISMA法発効以降も2006年まで運用は継続されました。

(2) 国防情報保証認証・認定プロセス（DIACAP）

2006年、国防省はDITSCAPで指摘された課題に対応するため、DIACAP（Defense Information Assurance Certification and Accreditation Process）を開始しました。

DIACAPは①文書作成の効率性 ②標準化への移行〔国防総省としての共通のセキュリティ基準（DoD8500.2）の導入〕③セキュリティ監視の継続性（脆弱性対応のパッチ適用、対マルウェア管理を継続的なプロセスととらえ、ライフサイクルを通じセキュリティを維持するといった管理の考え方の強化）が改善されました。

DIACAPはシステムの重要度を、任務保証カテゴリ[7]MAC（Mission Assurance Category）と機密レベル[8]CL（Confidentiality Level）という指標で分類し、この二つの指標の組み合わせで必要な管理策が決まる仕組みでした。ただし、国防省以外の連邦政府機関とインテリジェンスコミュニティは、全く異なる認証・認定プロセスと管理セットを使用していたため、これらのシステム間の相互接続は、長期にわたる調査と変換プロセスが必要であったと指摘されました[9),10)]

(3) 改正FISMA法とDoDのRMFの採用

① 改正FISMA法

2014年に改正FISMA法が成立しました。旧FISMA法では、対象システムの認証・認定にあたっては、年に1度のコンプライアンス報告が中心で、報告時点での安全性確認にとどまっていました。改正FISMA法は、こうした課題を改善するものです。

改正FISMA法は、連邦政府の機関に対して、情報および情報システムを保護するための包括的な情報セキュリティプログラムの開発、文書化、実施を義務付けることを目的としました。そして、システム毎のリスクの大きさに応じて対策の強度を変えるリスクベース・アプローチが正式に採用され、リアルタイムに近い頻度で、システムの脆弱性や脅威を監視し、動的に対応することが義務付けられました。

また旧FISMA法では、行政管理予算局OMB（Office of Management and Budget）が監視の責任を負っていた一方、サイバーセキュリティ対策の指揮系統が不明確であるといった点が指摘されていましたが、改正FISMA法では、国土安全保障省DHS（Department of Homeland Security）に連邦政府機関のセキュリティ方針を「運用・実施」する権限が付与され、インシデント発生時の対応支援や技術的指導はDHS主導で行うこととなりました。更にセキュリティインシデントが発生した際、影響を受けた機関が議会へ報告することが義務化されるとともに、重大インシデントの場合、発生から72時間以内にサイバーセキュリティ・イン

フラセキュリティ庁CISA（Cybersecurity and Infrastructure Security Agency）に報告するなどの厳格なルールが設けられました。加えて、クラウドサービスや外部ベンダーに委託している情報システムについても、政府と同等のセキュリティ基準を満たす必要があることが明確化・厳格化されました。

このように、改正FISMA法はサイバーセキュリティの実効性と迅速性の強化を目指すものでした。そして同法に取り入れられている「継続的監視」の考え方は、最新のゼロトラストアーキテクチャ導入の基盤となりました[11]。

② リスク管理枠組み（RMF）

改正FISMA法では、連邦政府全体で統一基準に基づくサイバーセキュリティ管理を行うことが求められていたため[12]、これを契機として、国防省はNISTが策定した連邦政府共通のRMFを採用するに至りました。

また「継続的監視」については、NISTが策定したRMFガイドラインに既に組み込まれており、システム変更や新たな脅威に対して動的に対応できる仕組みが整っていました。更にRMFは情報セキュリティの3要素（CIA）の重要度に応じてセキュリティ対策を選択できる柔軟な枠組みを持ち、改正法の理念であるリスクベースアプローチを既に具現化していました。

更に、政府の共通クラウドセキュリティ基準であるFedRAMPは、RMFをベースとしたものであり、RMF導入後、国防総省における民間クラウドサービスの導入や認定プロセスが、劇的にスムーズになったと言われています。

なおDIACAPからRMFへの移行期間に、「国防省全体で統一された情報源」が必要となったため、RMF Knowledge Serviceが構築され（https://rmfks.osd.mil）、RMFのプロセス、管理策、各種ガイドラインを集約した唯一の公式リポジトリとしての運用が開始されました[13]。

RMF-KSは当初、DIACAPからRMFへ移行するプログラム（システム開発プロジェクト）に対して、NISTの基準をどう兵器システムに適用するかという「読み替え」のガイドを提供することが主な目的でした[14]。

③ RMFの兵器システムへの拡大

(ア) 背景

防衛装備品は、単なるビークル（航空機、艦船、車両）や発射装置ではなく、指揮統制システムやデータリンクに接続するネットワーク機能を有する情報デバイス（コンピュータ）を伴うものがほとんどで、COTSが使用されるケースもあります。また、ソフトウェアアップデートの際や、通信リンクを通じてハッキングされる恐れがあります。

つまり、一般のPCやIoT機器と同様にサイバー攻撃を受けるリスクが存在し、仮にエアギャップが確保されていたとしても、脆弱性が増大しているのが現状です。加えて大規模な兵器システムの場合、サイバー攻撃による誤動作が物理的な大惨事につながる可能性があるため、情報システムと同等の厳格なセキュリティ管理が不可欠です。

また兵器システムの部品やソフトウェアは、サプライチェーンを通じて調達されるため、チップやコードに悪意あるプログラム（バックドア）が仕込まれるリスクに対処することも必要です。製造段階からの信頼性を確保した上で、リスクを継続的に監視・管理することが求められます。

更にロシア・ウクライナ戦争の状況は、強者に対する非対称戦（非対称な手段や非物理領域での攻撃）が有効であることを示唆しました。つまり、米国の競争国は、圧倒的なキネティック火力（物理的破壊のための火力）を保持する米軍に対して、ノンキネティック火力（サイバー攻撃、電磁波攻撃など）で軍事インフラや兵器を無力化することを重視している可能性が高く、兵器そのものの「サイバー耐性（Cyber Resiliency）」を高める必要もあります。

RMFの兵器システムへの適用は、以上のよ

うな今日の状況を踏まえ、開発段階からライフサイクル全体を通じて、「サイバー攻撃によって兵器が本来の機能を喪失する」リスクを最小化することを目指しています。

㈠ 兵器システムへのRMFの適用

2014年の改正FISMA法の発効に伴い、国防省はDoDI 8500.01において「プラットフォームIT（PIT）」を定義し、「計算資源を持つものは全てサイバーセキュリティの対象である」という一貫した管理体制を敷くことで、全ての情報システム、すなわち、情報システムに加え、兵器システム、発電所、水道施設等、国防資産全体の安全性を確保しようと企図しました[15),16)]。

しかしながら、兵器システムへのRMF適用にはITとOTの不適合、適用基準の整備遅れ、レガシーシステムの壁、取得プロセスの硬直性などの要因により停滞したと言われます。米国会計検査院による度重なる辛辣なレポート、それを受けた議会による圧力により８年を経て、ようやく兵器システムを対象としたRMFの適用開始に辿り着きます。

2022年７月19日、国防省は主要なサイバーセキュリティ指針であるDoDI 8510.01（Risk Management Framework for DoD Systems）を改訂・再発行しました[17)]。その内容は、兵器システムを含む全ての情報システムに対し、設計・開発から運用・廃棄までに至る「ライフサイクル全般」でのリスク管理を改めて義務付けたものです。

そして、それまでの情報システムに対するRMFが形骸化していたことを改め、より実効的なセキュリティエンジニアリングの統合が強調されました。

また併せて、サプライチェーンの可視化が必要であることを指摘し、防衛産業へのサイバーセキュリティ基準CMMC2.0（Cybersecurity Maturity Model Certification）[18)]の普及が求められました。

更に、2022年11月には国防総省からDoDゼロトラスト戦略が発表され、兵器システムにおいても、RMFによって「ゼロトラスト」の概念を導入する取組が始動しました。そして、情報システムについては2027年、情報システムよりも実装が困難な兵器システムについては2035年が目標として掲げられています。

㈡ RMFの兵器システムへの拡大に伴う措置

RMFを兵器システムまで拡大した結果、管理策（セキュリティ対策項目）の構成や適用方法には、従来の一般的な情報システムとは異なる実戦的・物理的な変化が生じました。

(a) 「オーバーレイ（Overlay）」による最適化

兵器システムは、一般的なサーバーやPCとは動作環境（リアルタイム性、長寿命、物理的制約など）が異なります。そのため、NIST SP 800-53の標準管理策をそのまま適用するのではなく、特定の環境に合わせて調整した適用基準である「オーバーレイ」が多用されるようになりました[19)]。

国家安全保障向け（米軍、CIA、NSAなどのシステム向け）に適用されるオーバーレイとしては、CNSSI 1253が準備されています。国家安全保障に係るシステムでは、CIAの各要素をそれぞれ切り離して評価する必要がありますが、CNSSI 1253は、こうした要件を踏まえ、適用すべき管理策をピンポイントで指定する、管理策実装のためのルールブックとなっています。

(b) サプライチェーン・リスク管理の強化

兵器システムの構成部品は外部から調達され、長期にわたって運用されます。そのため、国防省によるRMF適用範囲の拡大に伴い、NIST SP 800-53 Revision 5では「サプライチェーンのリスク管理」に関する新しい管理策ファミリー（SRファミリー）を追加、チップやソフトウェアにバックドアが設置されないよう、製造工程から追跡・検証するプロセスが必須項目となりました。

(c) サイバー抗たん性の導入

兵器システム特有の要件として、攻撃を受けても任務を継続できる能力（Cyber Survivability）が評価基準に加えられました。単に「侵入を防

ぐ」だけでなく、「攻撃された状態でもミサイルを発射できるか」「機能を縮小してでも運用を維持できるか」といった、物理的なミッションの実行に直結する管理策が重視されるようになりました。

(d) 運用技術（OT）への適応

兵器は純粋なITではなく、センサやアクチュエータを制御するOT（Operational Technology）で構成されています。従来の管理策を、PLC（プログラマブルロジックコントローラ）や産業用通信プロトコルに適用可能な形へ読み替える、またはOT専用の管理策（例：物理的なアクセス制限の強化など）へ置き換える運用が標準化されました[20)-22)]。

このように、RMFの兵器システムへの拡大に伴い、管理策の「項目数」が単に増えただけでなく、「兵器のミッション継続」や「物理的な安全性」を最優先するという運用の実態に即したものとなりました。

CSRMC導入開始の宣言と現在の状況

国防省は、2025年9月にRMFを更に進化させた新しい枠組みCSRMCの導入開始を宣言

表1　CSRMC（5段階のライフサイクル）

https://media.defense.gov/2025/Sep/24/2003808112/-1/-1/1/DOD-CIO-CYBER-SECURITY-RISK-MANAGEMENT-CONSTRUCT.PDF (Accessed Nov.3 2025)

サイバーセキュリティリスク管理構造（5段階のライフサイクル）					
目的	本構造は、サイバーリスク管理を、より効果的な評価と伝達を維持しつつ、より高速になるよう再度具体化するため、文化、マインドセット、手順を創造することを意図している。この取り組みは、最終的に作戦指揮官たちに任務に関する正確なサイバーリスクを提示するにあたって、サイバー・調達専門要員の手間を減らす。				
フェーズ	内容	説明	主な活動	フェーズの効果※	RMF
フェーズ1	設計	システム開発の初期段階で必要な要件を定義	①対象システムの能力ニーズ（何のために、どのような機能を備えるべきか）の明確化 ②要件（機能、サイバーセキュリティ、サイバー生存性）の選択 ③チームの形成：ミッションオーナー、システムオーナー、PM、エンジニア、CSSP	セキュリティは最初から組み込まれており、システム アーキテクチャに回復力が組み込まれていることを保証	準備 分類 選択
フェーズ2	構築	設計された要件を実際にシステムに組み込み、ネットワークに接続する準備を行う段階	①選択された要件の実装（機能的要件、サイバーセキュリティ要件、サイバー残存性要件） ②将来的な継続的運用承認（cATO）を実現するため、情報システム継続的モニタリング（ISCM）調整システムにデータを設定 ③DODIN（国防省情報ネットワーク）への接続を低いレベルで開始	システムが初期運用能力（IOC）を達成すると、安全な設計が実装	実施
フェーズ3	テスト	システムが安全かを攻撃者の視点で攻撃して修正し、実戦投入の合格証を出す段階	①システムが担う具体的なミッションの内容に合わせて情報セキュリティ継続モニタリング（ISCM）の設定を最適化 ②高リスクシステムに対する侵入テストによる脆弱性の評価 ③自動テストレポート・ダッシュボードによりテスト結果・リスク状況をリアルタイムで分析可能な状態とするよう集約・可視化 ④脆弱性修復チームがテストで発見された弱点を修正し、再評価 ◆「実際の攻撃に対して、その任務を遂行しながら耐えられるか」を実証する品質保証のフェーズ	完全運用能力（FOC）の前に、包括的な検証とストレステストが実行	評価
フェーズ4	オンボード	運用環境への正式な導入と承認を行う段階	① CSSPのリスク管理チームが主導し、リスクレビュー、重要制度の検証、成果物の確認を実施 ②審査結果に基づき、導入を決定（完全なオンボーディング／部分的なオンボーディング） ③ DODINに対する接続が、正式な本番運用環境に引き上げ ◆ RMFの「ATO（運用許可）」を出すプロセスを、より実戦的かつ迅速に行うのがこのフェーズ	システムの可視性を維持するために、展開時に自動継続監視がアクティブ化	承認
フェーズ5	運用	実環境での運用と、継続的なリスク監視を行う段階	①システムがISCMプロセスに組み込まれ、継続的なモニタリングを通じて「継続的な運用承認（cATO）」が可能 ②運用データがISCMシステムへリダイレクトされ、常に最新の状態が可視化 ③自動ダッシュボードとアラートを用いた再現可能なプレイブックにより、リアルタイムのリスク管理を実施 ④高リスクが特定された場合、CSSPのウォッチオフィサー（当直将校）の判断により、必要によりシステムの切断などの措置 ◆ 稼働間を通じ、動的で継続的な防御を行うフェーズ	リアルタイムのダッシュボードとアラートメカニズムにより、脅威を即座に検出し、迅速に対応	監視

※ https://media.defense.gov/2025/Sep/24/2003808112/-1/-1/1/DOD-CIO-CYBER-SECURITY-RISK-MANAGEMENT-CONSTRUCT.PDF (Accessed Nov.3 2025)

表２　CSRMC（10の基本原則）

https://www.compliancehub.wiki/the-end-of-rmf-understanding-the-dods-revolutionary-cyber-security-risk-management-construct-csrmc/

戦略的要領（迅速かつ効果的なサイバーリスク管理を実現するための10の柱）		
柱（原則）	説　明	要　領※
自動化（Automation）	リスク判定スピードの向上	自動化されたリスク管理により、プロセスを合理化し、人的エラーを削減し、効率を向上
重視する制御策（Critical Controls）	リスクに直結する「最も重要なセキュリティ制御」にリソースを集中	特定された重要な管理策と適応型復旧戦略に重点を置くことで、防御を強化し、業務継続性を確保
継続的監視（CONMON）、制御、および ATO	リアルタイムの監視データに基づき、運用許可（ATO）を継続的に維持	自動化された監視および制御システムを通じてリアルタイムの状況認識を可能にし、一定の ATO の態勢を実現
DevSecOps	開発初期段階からセキュリティを組み込み	継続的な開発、テスト、デプロイメントを通じてセキュリティと自動化を統合し、安全かつ迅速なサービス提供を加速
サイバー生存性（Cyber Survivability）	攻撃を受けても任務（ミッション）を継続し、迅速に復旧する能力を重視	強力な暗号化、多要素認証、継続的監視、インシデント対応計画を通じ、サイバー脅威や混乱、データ侵害からシステムを保護し、攻撃を受けたとしても任務を継続できる能力を確保
トレーニング（Training）	最新のツールやプロセスを使いこなせるよう、要員のスキルを継続的に向上	RMF の実務者向けに役割に基づいたトレーニングプログラムを強化し、一貫したパフォーマンス、サイバーセキュリティ知識、および標準の遵守の確実化
エンタープライズサービスと継承（Enterprise Services & Inheritance）	共通のクラウド基盤など（エンタープライズサービス）を利用することで、各システムがその基盤の安全性を「継承」し、個別の負担を軽減	セキュリティ制御、ポリシー、リスクを共有・継承することで、実証済みのフレームワークの採用を促進し、コンプライアンスの負担を軽減し、運用の整合性を維持
運用化（Operationalization）	サイバーセキュリティを、実際の戦闘・運用現場でのリスク判断の１つに格上げ	脅威検知、インシデント対応、コンプライアンス管理、およびプロアクティブな監視を通じて、進化する脅威に対する防御を強化し、リスク態勢をリアルタイム可視化
相互承認（Reciprocity）	承認実績のあるシステムや制御を再利用して重複する審査プロセスを排除	互いのセキュリティ評価を受け入れることで、システムリソースを再利用し、評価済みのセキュリティ態勢を共有して情報交換を促進
サイバーセキュリティ評価（Cybersecurity Assessments）	定期的かつ実戦的な評価を行い、システムの安全性を常に確認	脅威情報に基づいたテスト手法と、ミッション（任務）に整合したリスク管理プロセスを統合した、包括的なサイバーセキュリティ評価プログラムを確立

※ https://www.compliancehub.wiki/the-end-of-rmf-understanding-the-dods-revolutionary-cyber-security-risk-management-construct-csrmc/

しました。

これまでの公式発表は極めて限定的ですが、2025年９月に発表された、CSRMC の方向性を示す二つの公開資料のうち、まず「サイバーセキュリティリスク管理構造」[23] を紹介します（**表１**）。CSRMC のプロセスは RMF のプロセスを上書きした五つのフェーズ（設計、構築、テスト、オンボード、運用）から構成されています。

次に「戦略的指針（Strategic Tenet）」[24] には、迅速かつ効果的なサイバーリスク管理を実現するための10の柱（重視事項）が示されていますが（**表２**）、これらにより、速度と効率性の向上、継続的な防御、レジリエンスと運用の統合、基盤の強化を達成するとしています。

CSRMC は、「文書ベースの認定」から「自動化された継続的監視」へと管理策の運用をシフトさせるものであり、兵器システムが戦場でリアルタイムにサイバー脅威に晒されている状況をダッシュボードで可視化し、常に「運用許可（ATO）」の状態を維持する「Constant ATO」を目指しています。CSRMC は、これらの10の重視事項を踏まえつつ、五つのプロセスを実現することとなりますが、AI 活用はいずれの柱においても必要不可欠な技術になると考えられます。

これまでの公式発表では、CSRMC の10の柱（重視事項）を踏まえてシステムが具体化された際のイメージが、RMF よりも優れていると評価されています。つまり RMF は制度と実績で評価され、CSRMC は目標とする構造のイメージで評価されています。制度面は未だ明らかになっておらず、今後の米国の動向を冷静に注視していく必要があります。

総　括

米国の情報保証／サイバーセキュリティ確保

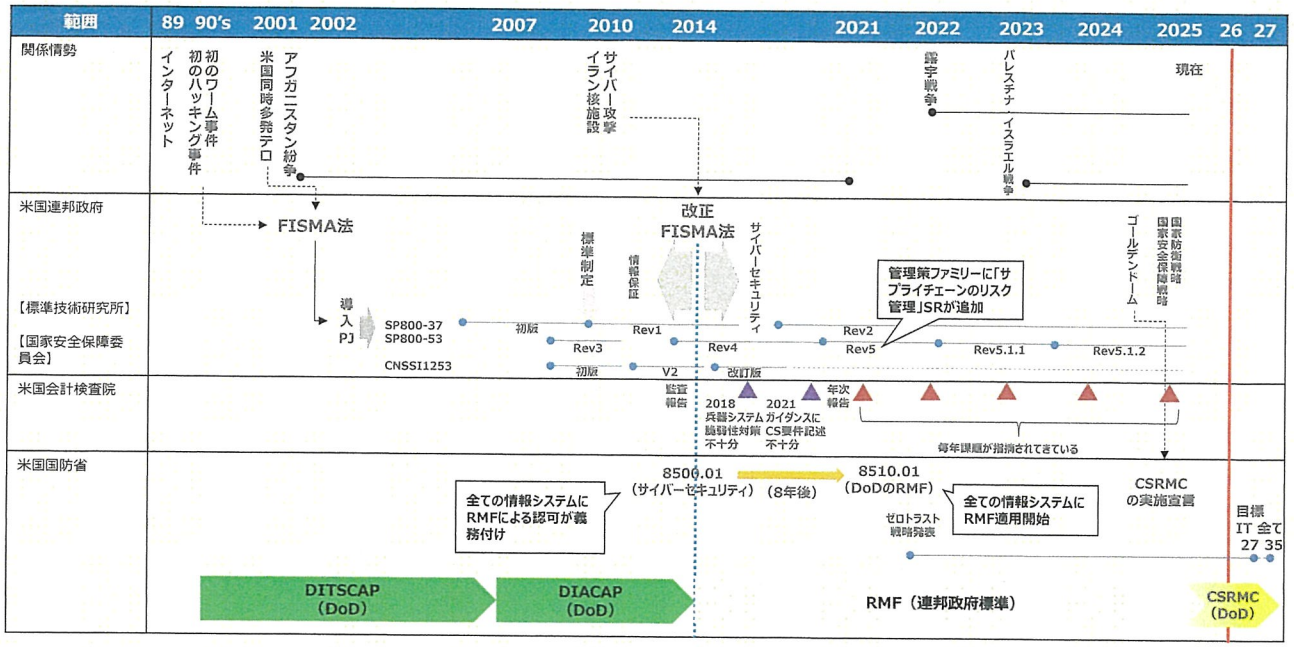

図１　米国の情報保証／サイバーセキュリティ確保のための枠組みの変遷（年表）

表３　米国の情報保証／サイバーセキュリティ確保のための枠組みの変遷

項目	DITSCAP	DIACAP	RMF	CSRMC（構想段階）
正式名称	DoD Information Technology Security Certification and Accreditation Process	DoD Information Assurance Certification and Accreditation Process	Risk Management Framework	Cyber Security Risk Management Constract
運用年代	1997年～2007年	2007年～2014年	2014年～2025年	2025年以降（最新）
主な目標	「C&A（認定と認証）」の確立とITシステムのセキュリティ標準化	「情報保証（IA）」への移行と、DoD全体での一元管理・可視化	リスク管理の統合と連邦政府標準（NIST）との整合性確保	認証の自動化・高速化と「常時接続・常時監視」の実現
アプローチ	静的・サイト別 特定の場所・時点でのシステム構成を物理的に確認・承認する。	静的・管理策ベース DoD固有の「IAコントロール」を用いた管理。Webツール（eMASS等）の初期導入。	ライフサイクル・リスクベース システム開発から廃棄までの全工程でリスクを評価。	動的・継続的監視 DevSecOpsと統合し、開発・運用の中でリアルタイムにリスクを許容
構成要素／フェーズ	4フェーズ Definition, Verification, Validation, Post-Accreditation	5アクティビティ Initiate, Implement, Validate, Make Decision, Maintain	6ステップ Categorize, Select, Implement, Assess, Authorize, Monitor	5フェーズ Design, Build, Test, Onboard, Operations
認証の性質	Snapshot（スナップショット） 認定時の状態のみを保証。紙ベースの膨大なマニュアル作業。3年毎再認証	← DIACAPスコアカードによる定量的評価を試行。3年更新。	← 「ATO（稼働権限）」の発行がゴール。3年更新	Constant ATO（常時ATO） 継続的なデータ監視により、再認証プロセスを不要化・自動化することを目指す。
特長	「個々のコンピュータを守る」	「ネットワーク全体で情報を保証」「可視化・管理」	「連邦政府標準（NIST）への統合」	「文書ベースの認定から、自動化された継続モニタリングへ」
	定性的評価	定量的評価、機械的判断 コンプライアンス（管理策）ベース	人間（AO）による判断 リスクベース	
適用ガイドライン （主な準拠基準）	DoD 8510.1-M （DITSCAP Application Manual） DoD 5200.40	DoD 8510.01（2007版） DoD 8500.2 （別紙　IA Implementation / IA Controls）→管理策カタログ	NIST SP 800-37（プロセス） NIST SP 800-53（管理策） CNSSI 1253（オーバーレイ） …公開、NSS向けにカスタマイズされた管理策実装のルールブック	DoD cATO Memo （Continuous Authorization to Operate） DoD Enterprise DevSecOps Reference Design ※NIST 800-53を自動化ツールで検証

※ https://www.compliancehub.wiki/the-end-of-rmf-understanding-the-dods-revolutionary-cyber-security-risk-management-construct-csrmc/

のための枠組みの変遷とサイバーセキュリティリスク管理構造（CSRMC）について述べました。米国の情報保証／サイバーセキュリティ確保のための枠組みの変遷（年表）を**図1**に、米国の情報保証／サイバーセキュリティ確保のための枠組みの変遷を**表3**に示します。

CSRMCの導入開始の宣言以降、国防省から更なる発表は行われていません。また、わが国の防衛省・自衛隊においても、現時点ではCSRMCの導入開始宣言や、これらの動きを受けたRMF関係の発表など、米国に連動した対応は確認されていません。そのため、当面は現行の情報保証訓令の手続きに沿った対応が引き続き求められていくことになると考えられます。

一方で、動的・継続監視、cATOなどの自動化やセキュリティエンジニアリングの取り込み、そのためのAI活用は時代の要請であり、今後はこれらの技術動向に注目していく必要があると思料します。

参考文献

1）Morris Worm事件（1988.11）https://www.fbi.gov/history/famous-cases/morris-worm, NASAへのハッキング事件（1999年8～10月）https://www.skillsoft.com/blog/a-history-of-the-worst-cyberattacks, FBIおよび陸軍コンピュータへのハッキング事件（1990）https://www.quora.com/What-are-the-most-significant-security-breaches-in-US-government-history

2）西半球に位置し、ユーラシア大陸から離隔したアメリカ合衆国において独立以降国土が戦場となったのは、内戦である南北戦争（1861～1865）が最後。冷戦時代を含め、米国同時多発テロの発生まで、外部からの大規模な攻撃を受けた経験はありませんでした。

3）宮田智之「【短信：アメリカ】同時多発テロ事件に関する独立調査委員会の最終報告書」，外国の立法，222（2004.11）国立国会図書館HP https://dl.ndl.go.jp/view/download/digidepo_1000428_po_022208.pdf（Accessed Feb. 02, 2026）

4）「HR2458-2002年電子政府法　第107回議会（2001-2002年）」米国議会 https://www.congress.gov/bill/107th-congress/house-bill/2458 （Accessed Jan. 27, 2026）

5）「情報セキュリティ向上のための米国の取組」独立行政法人情報処理推進機構 セキュリティセンター（2006.5）https://www.ipa.go.jp/security/reports/oversea/nist/fisma.html （Accessed Jan. 27, 2026）

6）“Definition of Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)”, Ignyte HP, https://www.ignyteplatform.com/glossary/department-of-defense-information-technology-security-certification-and-accreditation-process-ditscap/ （Accessed Jan. 27, 2026）

7）3段階　MAC Ⅰ：任務に不可欠　MAC Ⅱ：任務に重要　MAC Ⅲ：任務に必要

8）3段階　機密（Classified）、センシティブ（Sensitive）、公開（Public）

9）pts-ben, “Transitioning from DIACAP to RMF”, Phoenix TS HP, 2013 https://phoenixts.com/blog/diacap-vs-rmf/（Accessed Jan. 27, 2026）

10）Dominic Richardson, “Tech History: The Transition from DIACAP to RMF” 2021, Medium HP, https://medium.com/@Dominic.Richardson01/tech-history-the-transition-from-diacap-to-rmf-arts-tribune-8c91a90f4aa7 （Accessed Jan. 27, 2026）

11）Public Law 133-283官報，米国議会　https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf（Accessed Feb. 02, 2026）

12）これにより省庁間の互換性が向上し、コスト（経費、時間）が大幅に削減されるといったメリットがありました。

13）Lon Berman, “Ask Dr. RMF–Getting into the Knowledge Service”, BAI Information Security HP, 2023, https://rmf.org/ask-dr-rmf-knowledge-service/（Accessed Jan. 27, 2026）

14）2026年現在、RMF KSは単なる文書置き場ではなく、AI技術の適用（AI RMF）や、RMFの後継とされる新フレームワークCSRMC（Cybersecurity Risk Management Construct）への移行を支えるプラットフォームとして進化を続けている模様です。（なお、このサービスはCAC保持者等の軍関係者専用となっており、一般公開はされていません）

15）DoDI 8500.01, March 14,2014　https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf（Accessed Jan. 27, 2026）

16）DoDI 8530.01, PP.2, March 7, 2016　“c. Applies to the DODIN. The DODIN includes DoD information technology (IT) (e.g., DoD-owned or DoD-controlled information systems (ISs), platform information technology (PIT) systems, IT products and services) as defined in DoDI 8500.01 (Reference (h)) and control systems and industrial control systems (ICSs) as defined in National Institute (NIST) Special Publication (SP) 800-82 (Reference (i)) that are owned or operated by or on behalf of DoD Components.”,（Industrial Control Systems (ICS) とは、工場、発電所、水道施設、ビル管理、あるいは兵器システムなどの「物理的なプロセス」を自動で監視・制御するためのハードウェアとソフトウェアの総称）https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf

17）DoDI 8510.01, July 19, 2022 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf
18）戦争省が請負および下請負業者と共有する機密ではない機微な情報を保護することを目的とし、情報の種類と機密性に応じ、段階的なサイバーセキュリティ基準の導入を義務付けている認証制度。３段階のレベルが存在し、NIST SP 800-171/172などに準拠。レベル２はNIST SP 800-171に準拠しており、防衛省の保護情報特約に相当しますが、設定第三者審査機関 C3PAO（Certified Third-Party Assessment Organization）によるに認証が必要となる点が異なります。
19）例えば、航空機のフライト制御システムでは、可用性（システムが止まらないこと）が機密性よりも圧倒的に重視されるため、可用性に特化した管理策セットが選択されます。
20）「情報システムと組織の管理ベースライン」NIST CSRC（Sep. 2020.9）https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final
21）「NIST SP 800-82 改訂３ 運用技術（OT）セキュリティガイド」NIST CSRC（Sep. 2023.9）https://csrc.nist.gov/pubs/sp/800/82/r3/final（Accessed Feb.3 2026）
22）「（エグゼクティブサマリー）OT 運用技術のためのゼロトラスト」Department of Defense Office of Prepublication and Security Review（Nov 18, 2025）https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes.pdf（Accessed Feb.3 2026）
23）「サイバーセキュリティリスク管理構造」DoD CIO（Sep.24 2025）https://media.defense.gov/2025/Sep/24/2003808112/-1/-1/1/DOD-CIO-CYBER-SECURITY-RISK-MANAGEMENT-CONSTRUCT.PDF（Accessed Nov.3 2025）
24）「戦略的指針（Strategic Tenet）」DoD CIO（Sep.24 2025）https://media.defense.gov/2025/Sep/24/2003808111/-1/-1/1/DOD-CIO-CYBER-SECURITY-RISK-MANAGEMENT-CONSTRUCT-STRATEGIC-TENETS.PDF（Accessed Nov.3 2025）

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

発売中

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応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