

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

株式会社 Japan Aerospace & Defense Consulting

株式会社 SHIFT

菅野 隆
澤田 栄浩

はじめに

防衛省自衛隊では、省訓第26号（令和5.3.31）により「防衛省の情報保証に関する訓令」（防衛省訓令第150号）¹⁾（以下、情報保証訓令という）の改正が行われ、情報システムと、他の情報システムまたはネットワークと接続する情報システムを伴う装備品・器材は、同訓令第26条（運用承認）の規定に基づき、令和9（2027）年度末までに運用承認を受けることが必須となっています²⁾。このことは、米国政府、国防総省が採用しているリスク管理枠組み（Risk Management Framework: RMF, 以下、RMFという）の防衛省自衛隊への導入を意味しています。

本稿は、防衛装備品製造会社に RMF の概要と現状を理解頂くことを主な目的としています。まず RMF、米国の状況、防衛省自衛隊の RMF 導入の経緯と今後、対象となる情報システム、RMF プロセスについて公開されている³⁾ 情報保証訓令を踏まえて流れを解説した上で、装備品に対する RMF 適用にあたってのポイントと国の防衛力の抜本的強化の取組を踏まえ、今後に向けた認識を共有させて頂きたいと思います。防衛装備品製造会社の管理者の皆様には「RMF プロセス」を除き、担当者の皆様には全文をご覧下さい。

RMFと米国の状況

(1) RMF とは

RMF とは、情報システムの特性に応じたセキュリティ対策を実施し、最新の脅威動向を踏まえたリスク分析・評価を実施（脆弱性検査等）、セキュリティ対策の実施状況を監査（侵入試験等）するというサイクルを情報システムごとに適用・構築する考え方・枠組みのことで、これによりライフサイクルを通じて情報システムのリスクを継続的に管理し、安全に運用することが可能になります（図1）。

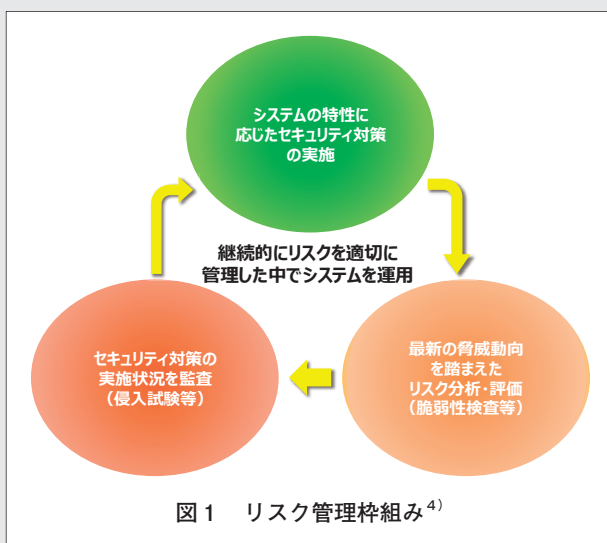


図1 リスク管理枠組み⁴⁾

表1 情報セキュリティの三要素

要素	説明
機密性 Confidentiality	権限がある人のみがアクセスできる、秘密を守ること
完全性 Integrity	情報が改ざんや破壊がされていなく正しいこと
可用性 Availability	権限を持つ人がアクセスしたいときに、いつでもアクセスできること

(2) 米国の状況

米国は2001年に起きた同時多発テロを契機とし、2002年、連邦情報セキュリティ法（Federal Information Security Management Act：FISMA 法）を発効し、情報セキュリティを強化するための企画やガイドラインを作成する役割を国立標準技術研究所 NIST（National Institute of Standards and Technology）（以下、NIST という）に正式に付与するとともに、連邦政府機関と取引を行う国内の州、地方自治体、民間企業（クラウドサービスプロバイダを含む）に対し、包括的な情報セキュリティプログラムを情報セキュリティの三要素（「機密性」「完全性」「可用性」）を重視して確立した上で（表1）、年次レビューを行うことを義務付けました。その後、2014年に同法を改正し、連邦政府の取組にあたっての国土安全保障省と行政管理予算局の監督責任を明確化しています。そして同法が関係機関、団体の情報セキュリティプログラムに準拠を求めているのが、NIST SP⁵⁾ 800-37 Rev⁶⁾2（情報システムおよび組織のためのリスクマネジメントフレームワーク）です。

同年、国防総省指令（DoDI8510.01）により、わが国に先行すること情報システムは約10年（兵器システムは2年）、RMF の導入が開始されています⁷⁾。

防衛省自衛隊のRMF導入の経緯と今後

令和4年（2022年）末、安保三文書が閣議決定され、「国家安全保障戦略」と「国家防衛戦

略」を実現するための中期的な防衛省の買い物計画である「防衛力整備計画」は、5年後の令和9年（2027年）までに防衛力を抜本的に強化するといった方針の下に策定されていることについては、皆様ご存知の通りです⁸⁾。そして、その際に重視する七つの能力⁹⁾が列挙され、令和5（2023）年度以降、その取組が開始されています。その中で、「領域横断作戦能力」¹⁰⁾が重視する能力の一つとされ、サイバー領域の能力は他領域（陸・海・空・宇宙・電磁波）とともにここに含まれます。

防衛省はサイバー領域の能力に関して、「能動的サイバー防御を含むサイバー安全保障分野における政府全体での取り組みと連携していく」とする一方、「重要なシステム等を中心に常時継続的にリスク管理を実施する態勢に移行」と明記しており、それがRMFに他なりません。その意義は「継続的なリスク管理の実施により、高度化・巧妙化する脅威にもより適切に対応することができ、結果、防衛省自衛隊における情報漏えいリスクの低減が可能」となる点にあるとしています¹¹⁾。

更に詳しく言うと、サイバー領域における脅威は、ロシア・ウクライナ戦争以前から日々高度化・巧妙化してきていることから、情報システム等のセキュリティ対策についても一過性の「リスク排除」から、継続的な「リスク管理」¹²⁾に考え方を転換するためにRMFを適用し、常時継続的にリスクを監視・分析・評価していくものです¹³⁾。これは、ゼロトラスト¹⁴⁾の考え方を取り込むことを企図していると見ることもできます。

日米同盟は、わが国の外交・安全保障政策の基本の一つであり、米国政府は、同国防総省、米国防衛企業と連携するわが国に対し、情報システムを介した安全な連携のため、防衛省自衛隊に同じ基準・レベルのセキュリティ対策の導入を求めてきていると言われています。更に具体的に言えば、自衛隊と米軍の情報の共有、安全な情報通信を含めたインターオペラビリティ（相互運用性）を向上させ、その連携の強化を

向上させることを通じて抑止力の最大化を目指すために、サイバー領域においても米国と同じレベルのセキュリティ基準を適用することが必須であることは、読者の皆様には理解して頂けることでしょう。

安保三文書の発出を契機とするタイミングで、今日の世界で最も厳しい安全保障環境の地域にあるわが国の平和と安全を守る防衛省自衛隊が、RMFの導入に至った背景について述べました。なお現在は、防衛省自衛隊の情報システム等にスポットが当たっていますが、国の安全を基盤的に支え、経済安全保障正面の死活的重要な社会・経済インフラでもある銀行、電力、そして情報通信などの分野についても、今後適用が求められていく可能性があると言われていきます。見方を変えたと、わが国としてRMFの適用範囲を拡大することで、米国や欧州からのサイバーセキュリティに関する最新のリスク情報のリアルタイム共有などが今後促進される可能性があるなど、大きなメリットが期待できます。

対象となる情報システム

(1) 対象となる情報システム

情報保証訓令第2条において、情報システムとは、「ハードウェア、ソフトウェア（プログラムの集合体をいう）、ネットワークまたは記憶媒体で構成されるものであって、これら全体で業務処理を行うもの」と定義され、運用承認が求められることが基本です。

そして同訓令第26条では、運用承認を要しない「別に定める情報システム」は例外とされており、別に定める情報システムについて「防衛省の情報保証に関する訓令の運用について（通達）」（防運情第9248号）に記述されています。

ここでは細部は省略しますが、これらの記述を踏まえると、他の情報システムまたはネットワークと接続する情報システムを伴う装備品・器材については、情報システムに分類され、運用承認を受ける対象と整理されました。

つまり従来は情報保証の対象は情報システムのみでしたが、同改正により情報システムまたはネットワークと接続する情報システムを伴う装備品・器材（情報デバイスを伴う装備品等という）まで対象が拡大し、防衛省自衛隊の多くの装備品・器材が情報システムにカテゴライズされているという点に注意が必要です（免除規定があることから確認が必要）。

(2) 運用承認の時期

情報保証訓令の附則（令和5年省訓令第26号）の2項には、現に運用を開始している情報システムに関する記述がありますが、表3に該当する場合のみならず、該当しない場合も含め、基本的に全ての情報システムを対象に令和9年度末までの運用承認を求めています。

RMFプロセス

本節では、NIST SP800-37 Rev2¹⁵⁾（以下、NIST-SP800-37という）のプロセスに沿って情報保証訓令に規定される、情報システムの運用承認、リスク分析・評価、監査の手続きについて解説していきます。

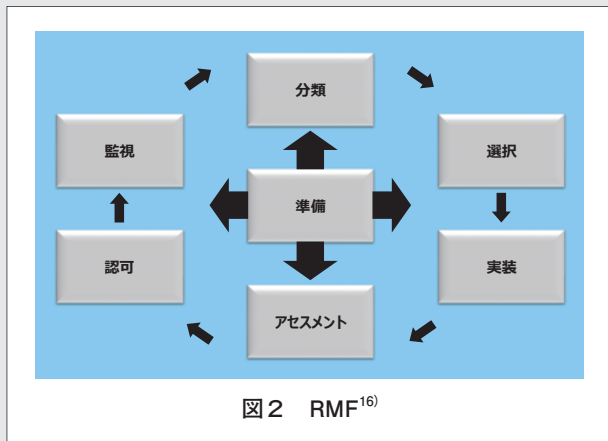
(1) 全般

NIST-SP800-37では、RMFについて次のように説明しています。

「RMFは、セキュリティ及びプライバシーのリスクを管理するための、統制がとれ、構造化された、柔軟なプロセスを提供する。このプロセスには、情報セキュリティの分類化、管理策の選択、実装及びアセスメント、システム及び共通管理策の認可、継続的監視が含まれる。RMFには、組織がこのフレームワークを適切なリスクマネジメントレベルで実行するための準備活動が含まれている（概要）」そのプロセスをイメージ化したのが図2です。

情報保証訓令は、「防衛省における情報シス

テム及び電子計算機情報に関して、総合的かつ体系的な管理の基準及び当該管理を組織的に実施するための基本的事項を定め、もって防衛省における情報保証を確保すること」を目的としており、防衛省における情報システムおよび電子計算機に関する共通の標準的で基本的なセキュリティ対策およびそれを実行するための規則の集合体といえます。



同改正において、

- － 第3章「防衛省の情報システムに係る対策」／第2節「運用承認」
- － 第9章「対策の実施状況の確認等」

の記述を加えることで、RMFを取り込む作りとなっています。

表2は、情報保証訓令に規定される手続関係者を整理したものです。確認しつつ読み進めて下さい。

じ後の説明は、申請・計画者（情報システム情報保証責任者）の立ち位置を基本として説明を進めたいと思います。

またステップの項目に、(官)、(官、民)の表示を行っています。RMF適用のための各ステップは、官が実施することが基本で、本稿では、それを前提に記述しています。しかしながら、(官)のステップは官単独で対応できる一方、(官¹⁷⁾、(民)を表示するステップは、民による技術的アドバイスが必要なステップである

表2 情報保証訓令に示されている組織および体制と NIST SP との関係

役 職 名	説 明	組 織 ・ 体 制	陸自の場合 (情報保証達が陸自のみ公開されているため、一例として整理)	情報保証訓令 関係条項	NIST SP での読み替え
情報保証統括責任者	省の情報保証に関する事務を統括し、情報保証に必要な取り組みを推進する責任者	整備計画局長		第4条	
情報保証監査統括責任者	省の情報保証の監査に関する事務を統括する者	サイバーセキュリティ・情報化審議官		第5条	
情報保証責任者	防衛省の各「機関等」に置かれ、当該機関の情報保証に関する事務を監督する者	別表第1 整備計画局長、防衛大学校長、 防衛医科大学校長、防衛研究所長、 統合幕僚長、陸上幕僚長、海上幕僚長、 航空幕僚長、情報本部長、防衛監察監、 地方防衛局長、防衛装備庁長官		第6条	「運用責任者」 「運用許可者」に相当
情報保証監査責任者	機関等における情報保証の監査に関する事務を行う者	情報保証責任者が設置	通信保全監査隊長	第6条の2	
情報システム情報保証責任者	情報システムの整備、維持管理、廃棄等のライフサイクル全般にわたる情報保証の確保に関する事務を行う者。各情報システム毎に置く。	情報保証責任者が設置	情報システムのライフサイクル全般にわたる情報保証の確保に係る業務を実施する部隊等の長、各部課等の長基準	第7条	「システムオーナー」に相当
情報システム運用者	情報システム情報保証責任者が作成する文書又は電磁的記録について、情報システムを利用する者の立場から情報システムの運用に関する意見を述べる者。各情報システム毎に置く。	情報保証責任者が設置	情報システム情報保証責任者が指定	第9条	
情報システム情報保証認証者	情報システム情報保証責任者が作成する文書又は電磁的記録について、総合的に評価し、情報保証責任者に対し必要な提言を行う者。防衛省の情報システム毎に置く。	情報保証責任者が設置	システム通信団長	第9条2項	
			陸上自衛隊の情報保証に関する達（陸自達61-8.19.12.17）		

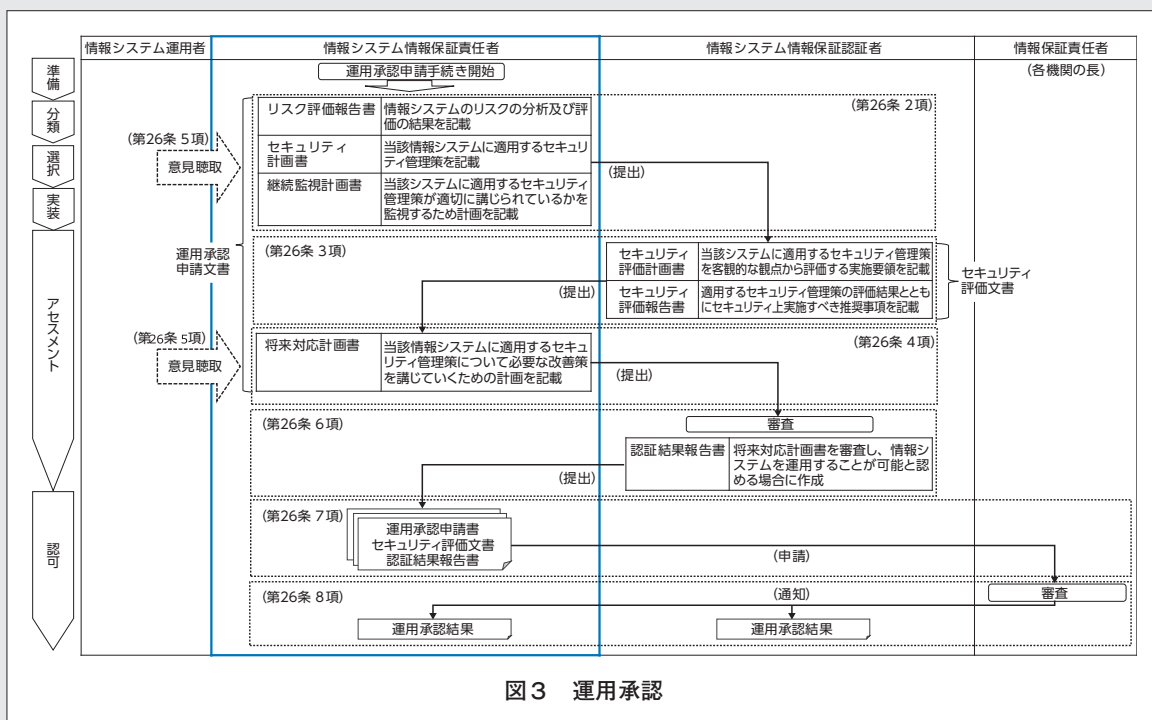


図3 運用承認

ことから、その区分を明示しているものです。

(2) 運用承認（準備、分類、選択、実装、アセスメント、認可）

ア 全般

図3は、情報保証訓令に沿った運用承認の手続きフローです。このプロセスはRMFにおける準備、分類、選択、実装、アセスメント、認可に相当します。

準備、分類、選択、実装は、情報システム情報保証責任者が、「リスク管理報告書」「セキュリティ計画書」「継続監視計画書」を作成し、情報システム情報保証認証者に提出する（第26条第2項）フェーズです。

イ 準備（官、民）

- ・組織全体を対象とする組織レベルと、特定の情報システムやアプリケーションに焦点を当てたシステムレベル、この二つのレベルで共通認識と優先順位を確立し、リスクを適切に管理していくための土台作りをします（NIST-SP800-37）。
- ・リスク評価報告書には、情報システムのリス

クの分析および評価の結果を記載します（リスクの特定）。（第26条第2項）リスク評価は、情報システムの意義・位置付け・使用される環境を踏まえ、当該情報システムのライフサイクル全体を通してリスクを管理するアプローチである点、留意が必要です。

ウ 分類（官）

- ・システムに求められるセキュリティの分類を、機密性、完全性、可用性の観点でそれぞれ高、中、低に決定します（その際に参考にするものとしてFIPS 199¹⁸⁾があります）。（NIST-SP800-37）
- ・リスク評価報告書を踏まえ、情報システムを機密性、完全性、可用性の観点から高・中・低に分類（セキュリティ分類）します（情報保証訓令運用通達¹⁹⁾、運用通達という）。これは、システムの運用状況に応じて必要なレベルのセキュリティを確保する柔軟な運用を可能とする重要な手続きです。

エ 選択（官、民）

- ・セキュリティ対策とプライバシー保護策を選択していきます。情報や情報システム毎

に確認し、それぞれに合った内容の対策をカスタマイズしていきます。管理策を選択していく際は、セキュリティ管理策が記載されている NIST SP800-53（連邦政府情報システム、および連邦組織のためのセキュリティ管理策とプライバシー管理策）をベースに選択していく方法などがあります（NIST-SP800-37）。

- ・セキュリティ分類を踏まえ、情報システムに適用する管理策を決定しセキュリティ計画書を作成します（運用通達）。

ー セキュリティ管理策には、組織的管理策、人的管理策、物理的管理策、技術的管理策などの幅があり、RMF の最新の標準的な管理策は、NIST SP800-53 Rev.5（組織と情報システムのためのセキュリティおよびプライバシー管理策）にて公開されています。一方、米国防総省や防衛省自衛隊の RMF 向けのリスク管理策としては、NIST 文書をベースにして、それぞれの組織や情報システムの特성에応じて修正が加えられたものが存在しており、その点注意が必要です。

ー なお NIST-SP800-37 に相当する防衛省自衛隊のセキュリティ管理策については、情報保証統括責任者が定めることとされていますが（第19条第2項）、非公開です。

オ 実装（官、民）

- ・選択した管理策を元に、システムを設計し、管理策を実装します（実装状況の確認および機構・運用マニュアルなどを整備した上で、セキュリティ計画書に展開）（NIST-SP800-37）。
- ・情報システムの運用開始後も適用されたセキュリティ管理策が適切に講じられているかを監視するために継続監視計画を作成します（運用通達）。

カ アセスメント（官）

- ・実装したセキュリティ管理策が正しく実装されているか、意図した通りに機能してい

るか、要件を満たしているかを評価します（NIST-SP800-37）。

- ・情報システム情報保証認証者は、リスク評価報告書、セキュリティ計画書、継続監視計画書の提出を受け、「セキュリティ評価計画書」「セキュリティ評価報告書」を作成（申請システムのセキュリティ管理策の適用状況について評価）し、情報システム情報保証責任者に提出します。セキュリティ評価計画書には、情報システムに適用するセキュリティ管理策を客観的な観点から評価する実施要領を記載、セキュリティ評価報告書には、適用するセキュリティ管理策の評価結果とともに、セキュリティ上実施すべき推奨事項を記載します²⁰⁾（第26条第3項）。
- ・情報システム情報保証責任者は、セキュリティ評価文書の提出を踏まえ、情報システムに実装しているセキュリティ上の管理項目について、必要な改善策を講じていくために将来対応計画書を作成します（第26条第4項）。
- ・情報システム情報保証認証者は、将来対応計画書の提出を受け、情報システムを運用することが可能と認める場合、「認証結果報告書」を作成し、情報システム情報保証責任者に提出します（第26条第6項）。

キ 認可（官）

- ・システムオーナーが対象システムの運用やセキュリティ管理策について、システムの運用責任者へ申請を提出、運用認可者は確認し、該当システムの運用で生じるリスクを受容できることを明示し、運用を認可します（NIST-SP800-37）。
- ・情報システム情報保証責任者は、「運用承認申請文書」²¹⁾に「セキュリティ評価文書」²²⁾と認証結果報告書を添えて、情報保証責任者に対して運用承認を申請します（第26条第7項）。
- ・情報保証責任者は、申請の内容について審

査し、情報システムを運用することが可能と認める場合には、情報システムの運用承認を行い、その結果を情報システム情報保証責任者および情報システム情報保証認証者に通知します（第26条第8項）。

(3) リスクの分析・評価（監視）（官、民） （監視 共通）

- ・対象システムのセキュリティ管理策の有効性を、システム所有者または共通管理策を策定した者、セキュリティやプライバシーの責任者などが継続的に評価していきます。運用認可の申請と許可も継続的に行っていきます（NIST-SP800-37）。
- ・情報保証訓令における承認後の組織的な監視については「リスクの分析・評価」「監査」があります。

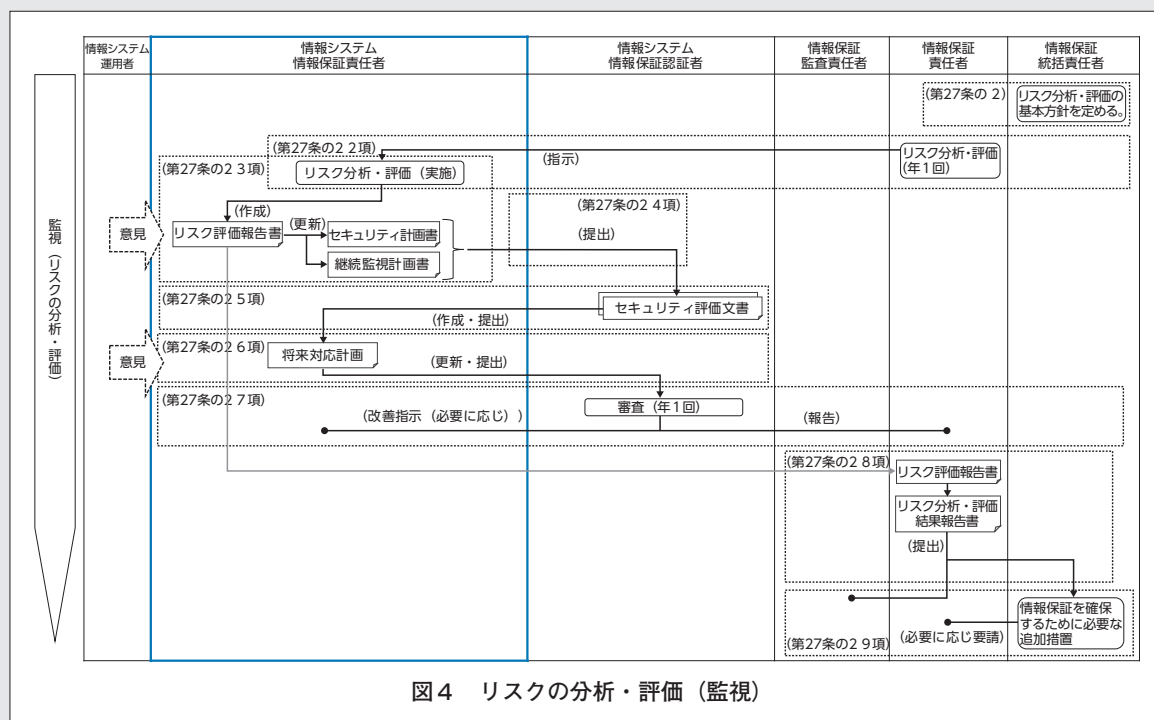
（第27条関連）

リスクの分析・評価（監視）

図4は、情報保証訓令に沿ったリスクの分析・評価（監視）の手続きフローです。リスク分析・評価には脆弱性検査が伴うことが基

本となります。

- ・情報保証統括責任者が、リスク分析・評価を行うに当たっての基本方針を定めます（第27条の2第2項）。
- ・情報保証責任者は、情報システム情報保証責任者に対して毎年度1回以上リスク分析・評価を実施させることが義務付けられています（第27条の2）。
- ・情報システム情報保証責任者は、リスク分析・評価を実施し、その結果を記載したリスク評価報告書を作成、その結果を踏まえて、セキュリティ計画書および継続監視計画書を更新し、情報システム情報保証認証者に提出します（第27条の2第2項）。
- ・情報システム情報保証認証者は、リスク評価報告書、セキュリティ計画書および継続監視計画書の提出を受け、セキュリティ評価文書を新たに作成し、情報システム情報保証責任者に提出します（第27条の2第5項）。
- ・情報システム情報保証責任者は、セキュリティ評価文書の提出を受け、これを踏まえて将来対応計画を更新し、情報システム



情報保証認証者に提出します（第27条の2第6項）。

- ・情報システム情報保証認証者は、毎年度1回以上、更新された将来対応計画書を審査し、情報保証責任者に報告、必要に応じて、情報システム保証責任者に改善指示等を行います（第27条の2第7項）。
- ・情報保証責任者は、リスク評価報告書を踏まえ、毎年度、リスク分析・評価の実績を記載したリスク分析・評価結果報告書を作成し、情報保証統括責任者および情報保証監査責任者に提出します（第27条の2第8項）。
- ・情報保証統括責任者は、リスク分析・評価結果報告書を踏まえ、必要に応じて、情報保証責任者に対して情報保証を確保するために必要な追加措置等を求めることができます（第27条の2第9項）。

(4) 監査（監視）（官）

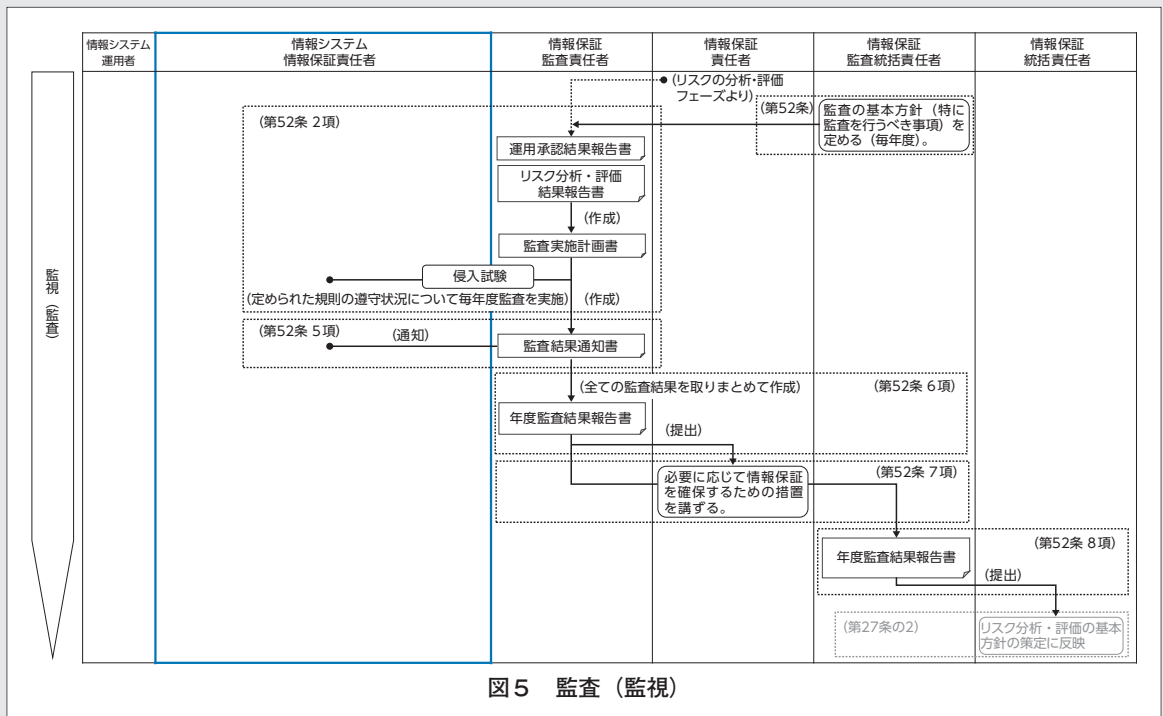
（第52条関連）

図5は、情報保証訓令に沿った監査（監視）の手続きフローです。

- ・情報保証監査統括責任者は、毎年度監査の基本方針を定めます（第52条）。
- ・情報保証監査責任者は、年度の監査の基本方針を踏まえ、対象となる情報システムの運用承認結果報告書およびリスク分析・評価結果報告書に基づき監査実施計画書を作成し（第52条第2項）、定められた規則の遵守状況について毎年度監査を実施して監査結果通知書を作成、情報システム情報保証責任者に対して監査結果を通知します。（第52条第5項）

なお監査計画書には、監査の対象（侵入試験の対象となる情報システムを含む）、監査の項目、その他必要な事項を記述することとされており、監査において侵入試験の実施は前提となっています。

- ・また情報保証監査責任者は、年度で実施した全ての監査結果を取りまとめ年度監査結果報告書を作成、情報保証責任者と情報保証監査統括責任者に提出します（第52条第6項）。
- ・情報保証責任者は、年度監査結果報告書を踏まえ、必要に応じて組織全体の情報保証を確



保するための措置を講じます（第52条第7項）。

- ・情報保証監査統括責任者は年度監査結果報告書を取りまとめ、情報保証統括責任者に提出します。それを受け、情報保証統括責任者は次年度のリスク分析・評価の基本方針の検討に反映します（第27条第2項）。

装備品製造会社のRMF適用のポイント

前述の通り、情報保証訓令は、防衛省自衛隊の内部（官）に向けた命令・指示であることから、組織内の手続きですが、適用にあたっては、省内事務手続きの知見を基礎として、同装備品の運用要領や運用を想定する環境、保管状況などに係る現場を知る運用者知見と、情報デバイスを伴う装備品等の製造会社（ベンダー）知見、そしてサイバーセキュリティ、RMFに係る基本的な知見が必要です。

令和9（2027）年度末までの運用承認取得を必成目標として、官側が手続きを推進する中で、令和6（2023）年以降の運用承認（第5章 RMF プロセス／(2) 運用承認）手続きに対する技術のご支援を通じた気づきのポイントについて示します。

- ・RMFの適用を求められている装備品数は未だかなり残されており、限られた人的資源（官民間問わず）での対応により、運用承認を期限内〔令和9（2027）年度末〕に完了させるためには、一刻の猶予も許されない段階に入っています。
- ・ベンダー側から支援する装備品の担当者が、RMFやサイバーセキュリティに関する基礎知識が十分でない場合、官との調整開始の段階において、工数見積を円滑に進められない等、必要以上に時間を要するケースが見られます。官（申請者）側を支援するベンダー側が、この点認識し、これらに関する最低限の知見を事前に準備すれば、この課題を解決することが可能となります。

おわりに

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にあたっての装備品会社様に対するポイントを説明しました。更に留意する点について書きとめます。

○ドローンなど新規にCOTSとして官が取得を予定している情報システムを伴う装備品に関しては、運用要領の検討にあたり、IT技術やAIの活用などによる運用の可能性を最大限確保するため、情報システムに接続する可能性が極めて高く、この場合、RMFの適用が必要となります。つまりベンダーは、納入した後も、運用承認を取得するまでの間、支援が必要になると考えられます。

○装備品移転にあたっては、移転先でRMFを適用して現地国で運用承認を受けることを想定し、他国のRMFの対応状況についても、アンテナを張っておく必要があります。

政府は、令和4（2022）年末に閣議決定された「国家防衛戦略」と「防衛力整備計画」について、最近の安全保障環境の急激な悪化を踏まえ、前倒しで改正する方向で検討に入ったとメディアは伝えています²³⁾。加えて、小泉防衛大臣は着任式の訓示において、安保三文書の見直しの検討の必要性の認識を示しました²⁴⁾。

装備品製造会社の皆様におかれましては、材料費の高騰等の厳しき折ではありますが、わが国の国益に資するため、防衛省自衛隊による防衛力の抜本的強化に向けた取り組みの重要性を理解いただき、そして、その一つである情報デバイスを伴う既存の装備品等に対するRMF適用にも積極的かつ柔軟に対応願います。

米国においては、RMFの見直し（CSRMC）の動きが出ている模様^{25)、26)}ですが、当面、現行訓令に沿った対応が求められると考えます。

注および参考文献

- 1) 訓令とは、防衛省内部向けの防衛大臣による命令・指示であり、同情報保証訓令の命令・指示は情報保証責任者、情報システム情報保証責任者、情報システム情報保証認証者、情報システム運用者などに対して発せられており、これらの防衛省自衛隊の組織内での手続きを律するもの。
- 2) 防衛省訓練第160号「防衛省の情報保証に関する訓令」 http://www.clearing.mod.go.jp/kunrei_data/a_fd/2007/ax20070920_00160_000.pdf (Accessed Oct.10 2025)
- 3) 管理策を含む「リスク管理枠組み (RMF) におけるセキュリティ管理策について (通知) (防整サ第14550号 (令和5年7月3日)) や、「情報システムにおけるリスク管理枠組み (RMF) 実施要領等について (通知) (防整サ第14550号 (令和5年7月3日)) については公開されていない。
- 4) 防衛省自衛隊におけるこれまでの取組等 (令和6年7月1日、防衛省) https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai2/siryou6-4.pdf (Accessed Oct.10 2025)
- 5) Special Publication (特別出版物) の略
- 6) Revision (修正版) の略
- 7) 2014年に発出された指令が「DoD Instruction 8510.01 Risk Management Framework for DoD Information Technology」で、2022年に改訂された指令が「DoD Instruction 8510.01 Risk Management Framework for DoD Systems」。2022年の改訂で、IT 以外のシステムを含んで適用範囲が明確化・拡大されることになった。
- 8) 2027年8月1日は中国人民解放軍創設100周年にあたり、習近平国家主席が第21回党大会で異例の4期目を目指すのではと見られている。同盟国である米国は同年に台湾侵攻があるとの見積・前提の下、それを抑止するための準備に着手し、わが国も防衛力を整備しているものである。
- 9) 1 スタンド・オフ防衛能力/2 統合防空ミサイル防衛能力/3 無人アセット防衛能力/4 領域横断作戦能力/5 指揮統制・情報関連機能/6 機動展開能力・国民保護/7 持続性・強靱性
- 10) 領域横断作戦能力: 宇宙・サイバー・電磁波の領域および陸・海・空の領域における能力を有機的に融合し、相乗効果によって全体の能力を増幅させる領域横断作戦を実行するための能力
- 11) ロジックモデル「リスク管理枠組み (RMF) 関連事業経費」 https://www.mod.go.jp/j/policy/hyouka/rev_suishin/r04/rev_fin_r05/05-0006.pdf (Accessed Oct.10 2025)
- 12) リスクを特定して評価して対応策を実施し、その結果をモニタリングして継続的に改善していくプロセスを「リスクマネジメント」と言う。
- 13) 令和5年度防衛白書 http://www.clearing.mod.go.jp/hakusho_data/2023/html/n310405000.html (Accessed Oct.10 2025)
- 14) 「ネットワークが侵害されている場合であっても、情報システムやサービスにおいて、各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体」NIST SP800-207 (Zero Trust Architecture) の定義
- 15) 「情報システム及び組織のためのリスクマネジメントフレームワーク」(NIST Special Publication 800-37 Revision2, IPA ホームページ https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/NIST.SP.800-37r2_JA.pdf (Accessed Oct.10 2025))
- 16) 前掲 IPA
- 17) 官が策定するのは組織的管理策
- 18) Federal Information Processing Standard の略で NIST (国立標準技術研究所) が発行する情報技術関連の標準規格のこと。FIPS199は、連邦の情報及び情報システムに対するセキュリティ分類規格。
- 19) 「防衛省の情報保証に関する訓令の運用について (通達)」(防運情第9248号, 19.9.20)
- 20) セキュリティ評価計画書とセキュリティ評価報告書を合わせて「セキュリティ評価文書」と呼ぶ。
- 21) 運用承認申請文書とは、(準備・分類・選択・実装・アセスメントのフェーズで作成された) リスク評価報告書、セキュリティ計画書、継続監視計画書、将来対応計画書を指す (情報保証訓令第26条 第5項)。
- 22) セキュリティ評価文書とは、セキュリティ評価計画書及びセキュリティ評価報告書を指す (情報保証訓令第26条 3項)。
- 23) <独自>「国家防衛戦略・整備計画改正前倒しへ 防衛費2%超に、紛争頻発で安全保障環境悪化」(2025.8.12) 産経新聞 HP <https://www.sankei.com/article/20250812-TFCUGU504FKKJBNGR7HTAKRLF4/> (Accessed Oct.10 2025)
- 24) (共同通信)「小泉氏、安保3文書改定に意欲 防衛相着任式で訓示」(2025.10.22) 47NEWS HP <https://www.47news.jp/13330465.html> (Accessed Oct.22 2025)
- 25) <https://www.war.gov/News/Releases/Release/Article/4314411/departments-of-war-announces-new-cybersecurity-risk-management-construct/> (Accessed Nov.3 2025)
- 26) 米国連邦政府、関係機関への「コンプライアンスベースモデル」である RMF 導入は2005年 (DoD 装備品システムへの RMF 導入は2022年) に行われた。導入当時と現在では環境 (インフラ、ソフトウェア技術、求められる調達サイクル等) が大きく異なってきたため、その遅さ、柔軟性の欠如、官僚主義に対し多くの批判が集まっていた。そして、統合と自動化/運用の透明性/継続的な監視/財政的責任を優先した、自動で継続的監視・運用許可の体制の必要性を求める声が高まり、「リスクベースモデル」である CSRM の取組の検討・公表に至ったものである。併せて、その実現にあたり、実行に必要な SWFT (ソフトウェア・ファスト・トラック) イニシアティブも開始した。SWFT は、RMF と運用許可プロセスを自動化及び最新化し、ソフトウェアの取得と承認のため、高速な AI 主導型システムを構築することを目指しており、SWP (ソフトウェア取得パスウェイ) を活用することで、DevSecOps [SW 開発 (Dev)、セキュリティ (Sec)、運用 (Ops)] を連携させ、開発プロセス全体にセキュリティを統合するアプローチ) を通じ、迅速かつ反復的な SW 開発と継続的な運用許可を可能にする。その際、サプライチェーン・セキュリティを向上させるため、SW 部品表 (SBOM) を取り入れ、SW コンポーネントの可視性を向上させる模様である。