

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

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

菅野 隆 澤田 栄浩

前号ではインターネットの登場以降に登場した情報保証／サイバーセキュリティにおけるリスク管理（RMFを含む）の歴史を整理した上で、米国政府の取組みの最新の状況について概観しました。今回は、視点を再びRMFの現場に戻し、運用承認取得後の動きについて解説します。

本稿は官、民を問わず、あらゆるレベルの関係者を対象として執筆しています。

（編集部）

はじめに

本稿は防衛省の公開文書（情報保証訓令¹⁾、省運用通達²⁾）に基づき、「監視」に加え「監査」のステップについて説明し、理解を深めていただくことを目的としています。

令和9年度末までの運用承認取得を設定しているリスク管理枠組み（RMF）は、運用承認を取得後、運用が開始され、防衛省 RMF という「監視」「監査」ステップに入ります。NIST 標準では、RMF は「準備」「分類」「選択」「実装」「アセスメント」「認可」「監視」の7ステップで構成されるとしていますが、防衛省における RMF は、「準備」「分類」「選択」「実装」「評価」「承認」「監視」「監査」の8ステップから構成されています（アンダーラインは、用語の異なるステップまたは防衛省 RMF で追加されたステップ）。

NIST 標準では「監視」はいわゆる継続的監視期、すなわち運用承認後の通常運用段階全体を指しています。本稿では、防衛省 RMF の「監視」ステップで実施される「自己点検」および「リスクの分析・評価」の手続きに加えて、追加

されている「監査」ステップについても併せて取り上げ、これらの手続きおよびステップの全体を「監視」フェーズとして説明します（図1）。「監視」フェーズの内訳を表1に整理します。

なお各機関における RMF の具体的実施要領や細部のルールに関しては、内局や各機関が発簡する通知・通達等に従うことになります。技術支援等にあたる場合、保護情報取扱者登録完了後、必ずそれらの文書も確認してください。

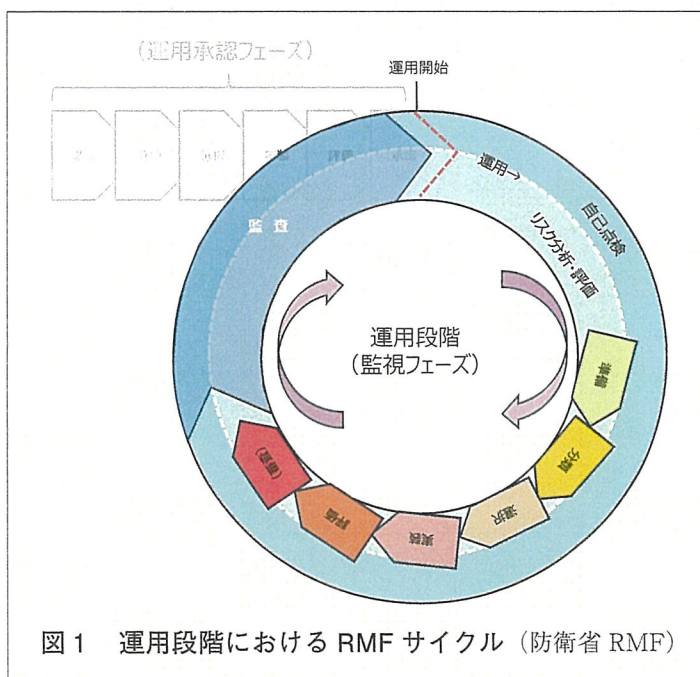


図1 運用段階における RMF サイクル（防衛省 RMF）

表1 「監視」フェーズの内訳

区 分	訓令	毎年度定める 基本方針作成者	指示者	機関内での対象者		指示者の 措置	プロダクト	プロダクトの処理			
				情報システム側	認証側 (監査側)			通知先	提出先	報告先	措置
自己点検	第51条	情報保証統括責任者	情報保証責任者 (防衛省各 機関の長)	(機関内)		必要に応じて情報保証 を確保する ための措置 を講じる	評価結果	情報保証 監査責任者		情報保証 統括責任者	
リスク分析 ・評価	第27条	情報保証統括責任者		情報システム情報 保証責任者 (将来対応計画 書を更新の上、情 報システム情報保 証認証者に提出)	情報システム情報 保証認証者 (毎年度1回以 上、同文書を審 査。情報保証責 任者に報告。必 要に応じ情報シ ステム情報保証 責任者に改善指 示)		リスク分析・評価結 果報告書(情報 システム情報保証 責任者が作成した リスク評価報告書 を踏まえて作成)		情報保証 統括責任者 情報保証 監査責任者	→	情報保証統括 責任者は、必要 に応じ情報保証 責任者の措置を 要請
監 査	第52条	情報保証監査 統括責任者	—	(情報システム情 報保証保証責任 者)	情報保証監査責 任者		監査結果通知書 監査結果報告書 (毎年度作成)	情報システム 情報保証責 任者		→	必要に応じて情 報保証を確保す るための措置を 講じる
参 考	【内局】 情報保証統括責任者 整備計画局長 情報保証監査統括責任者 サイバーセキュリティ・情報化審議官 【各機関等ごと】 情報保証責任者(機関の長) 陸上幕僚長 情報保証監査責任者 通信保全監査隊長 情報システム情報保証認証者 システム通信団長 情報システム情報保証責任者 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 ※陸上自衛隊の場合(陸上自衛隊の情報保証に関する達(陸自達61-8 19.12.17))										

監視

(1) 自己点検(組織的管理策が対象)

自己点検は、情報保証訓令および同訓令に基づき定められた規則、各機関で策定した情報保証確保のための通達などに規定された規則(組織的管理策)が、日常的に適切に遵守されているかを各機関が確認するステップです。

情報システムの運用にあたっては、情報保証統括責任者が毎年度定める自己点検の基本方針(51条)に基づき、情報保証責任者は情報保証訓令および同訓令に基づいて定められた規則の遵守状況について、毎年度、職員に自己点検を行わせることとしています(51条2)。この際、運用通達は、情報保証責任者が自己点検の計画、点検項目、実施要領、その他必要な事項を定め、職員に周知することとしています。更に情報保証責任者は自己点検の結果を踏まえ、必要に応じて情報保証を確保するための措置を講ずるものとしています(51条3)。加えて情報保証責任者は自己点検の結果を分析、評価し、

評価結果を情報保証監査責任者に通知するとともに、情報保証統括責任者に報告するものとしています(51条4)。

なお情報保証責任者は、組織的管理策の徹底状況を機関内で確認するための措置として、後述する監査を実施する裁量を有しています。

(2) リスクの分析・評価

情報保証訓令は、情報保証統括責任者が定めた基本方針(27条の2)を踏まえ、情報保証責任者が情報システム情報保証責任者に対し、年1回以上、リスク分析・評価を行わせることを義務付けています(第27条2の2)。

運用通達では、運用開始後1年を経過するまでの間に、情報システム情報保証責任者がリスク分析・評価の一環として「脆弱性検査」を少なくとも1回は実施することと、1回目の脆弱性検査から2年を経過した後に、再度脆弱性検査を実施することを補足しており、この点に注意が必要です。また情報保証統括責任者は、運用中の各情報システムのリスク管理を一元的に行うため、情報保証責任者に対して、管理する

情報システムの「リスク評価報告書」の随時提出を求めることができますとしています。

① 審査

運用承認段階において検討・実装した管理策の有効性を、情報システム情報保証責任者と情報システム情報保証認証者により評価していくのが、審査のプロセスです。

情報保証責任者の指示で、運用承認を受けた運用中の情報システムの「リスクの分析・評価」の段階が実質的にスタートすることになります。

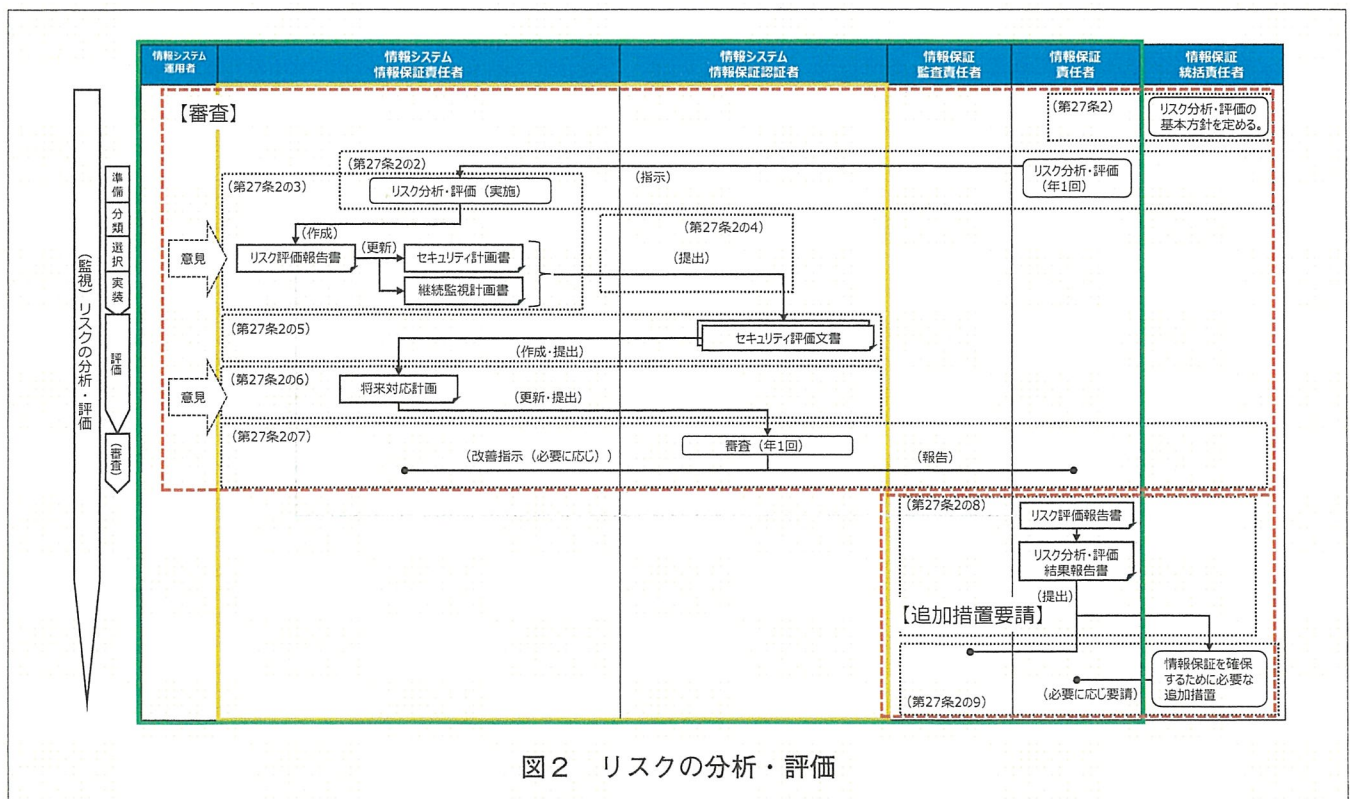
指示を受けた情報システム情報保証責任者はリスク分析・評価を実施し、その結果を記載した「リスク評価報告書」を作成します。そして、その結果を踏まえ、運用承認手続き時に提出した「セキュリティ計画書」「継続監視計画書」を更新し（27条2の3）、これらを情報システム情報保証認証者に提出することとしています（27条2の4）。

文書の提出を受けた情報システム情報保証認証者は、これを踏まえてセキュリティ評価文書（セキュリティ評価計画書、セキュリティ評価

報告書）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（27条2の5）。情報システム情報保証責任者はこれを踏まえて、運用承認手続き時に提出した「将来対応計画」を更新した上で、情報システム情報保証認証者に提出します（27条2の6）。それを受けて、情報システム情報保証認証者は、毎年度1回以上、将来対応計画書を審査して情報保証責任者に報告し、必要に応じて情報システム情報保証責任者に改善指示を行います（27条2の7）。

なお「リスク分析・評価」のステップ内で脆弱性診断を行う場合、エアギャップのあるオンプレミスで運用中の情報デバイスを伴う情報システムにおいては、外部のクラウドサービスは使用することができないため、あらかじめ情報システムにオフラインで動作する脆弱性診断ツールをインストールするか、脆弱性診断ツールがインストールされたスタンドアローンPC等により実施する必要があるため、これらを情報システムに実装、または別途準備する必要があります。

以上が、情報システム情報保証責任者と情報



システム情報保証認証者が関係する、主として機関内で実施される「審査」のプロセスです。

② 追加措置要請

機関内のプロセス終了後は、省レベルのプロセスに移行します。

情報保証責任者は、情報システム情報保証責任者がステップの当初に指示を受けて作成した「リスク評価報告書」を踏まえて「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と情報保証監査責任者に提出します（27条2の8）。情報保証統括責任者は、情報保証を確保するために、必要に応じ措置を講じることを情報保証責任者に要請します（27条2の9）。

加えて情報保証統括責任者は、運用中の情報システムのリスク管理を一元的に行うことを目的として、情報保証責任者に対し、管理する情報システムのリスク評価報告書の随時提出を求めることができますとしています。

以上の流れを図2に整理します。

監査ステップ

(1) 監査

運用通達によると、情報保証監査責任者の実施する監査には「定期監査」と「臨時監査」があるとされています（表2）。

以下は、基本となる定期監査の手続きについてです。

情報保証監査統括責任者が毎年度定める監査の基本方針（52条）に基づき、情報保証監査責任者は「運用承認結果報告書」および「リスク分析・評価結果報告書」を踏まえ、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定めた「監査実

施計画書」を作成し、情報保証訓令および同訓令に基づき定められた規則の遵守状況について、毎年度、監査を実施します（52条2）。一般的なTCP/IPプロトコルを採用していない情報システムや、旧式のOS上で動く情報デバイスを伴う装備品において、侵入試験の実施難易度は高いとされており、実施要領に関してあらかじめ確認および検討が必要です。

以上の規定に加え、情報保証監査責任者には必要に応じて監査を行う裁量を認めるとともに（52条3）、監査の実施にあたっては、情報保証責任者および他機関等の情報保証監査責任者の協力を依頼することが可能となっています（52条4）。

情報保証監査責任者は、監査の結果を記載した「監査結果通知書」を作成の上、情報システム情報保証責任者に通知し（52条の5）、毎年度、監査結果を取りまとめた「監査結果報告書」を作成し、情報保証責任者および情報保証監査統括責任者に提出します（52条6）。情報保証責任者は監査結果を踏まえて必要に応じて、情報保証を確保するための措置を講じ（52条7）、情報保証監査統括責任者は、毎年度「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。

なお運用通達では、情報保証監査責任者に対し監査対象となる部署とは異なる部署の職員に監査を行わせること等により、第三者的観点を確保するとともに、監査の実効性を確保するための措置を講ずることを求めています。

また運用承認の対象となる情報システムのうち、セキュリティ分類の完全性「高」に該当する情報システムおよび情報システム情報保証責任者、または情報保証監査責任者が必要と認める情報システムを対象として、情報システムの製造が完了し実際の運用環境と同等の環境となった後、運用開始から1年を経過するまでの間に少なくとも1回は侵入試験を実施することとしています。更に1回目の侵入試験から2年を経過した後に、再度侵入試験を実施すること

表2 情報保証監査責任者が実施する監査

区分	開催の契機	実施回数
定期監査	監査実施計画書および自己点検等の結果に基づく。	毎年1回以上
臨時監査	情報保証に関する問題点等を考慮して実施	必要の都度

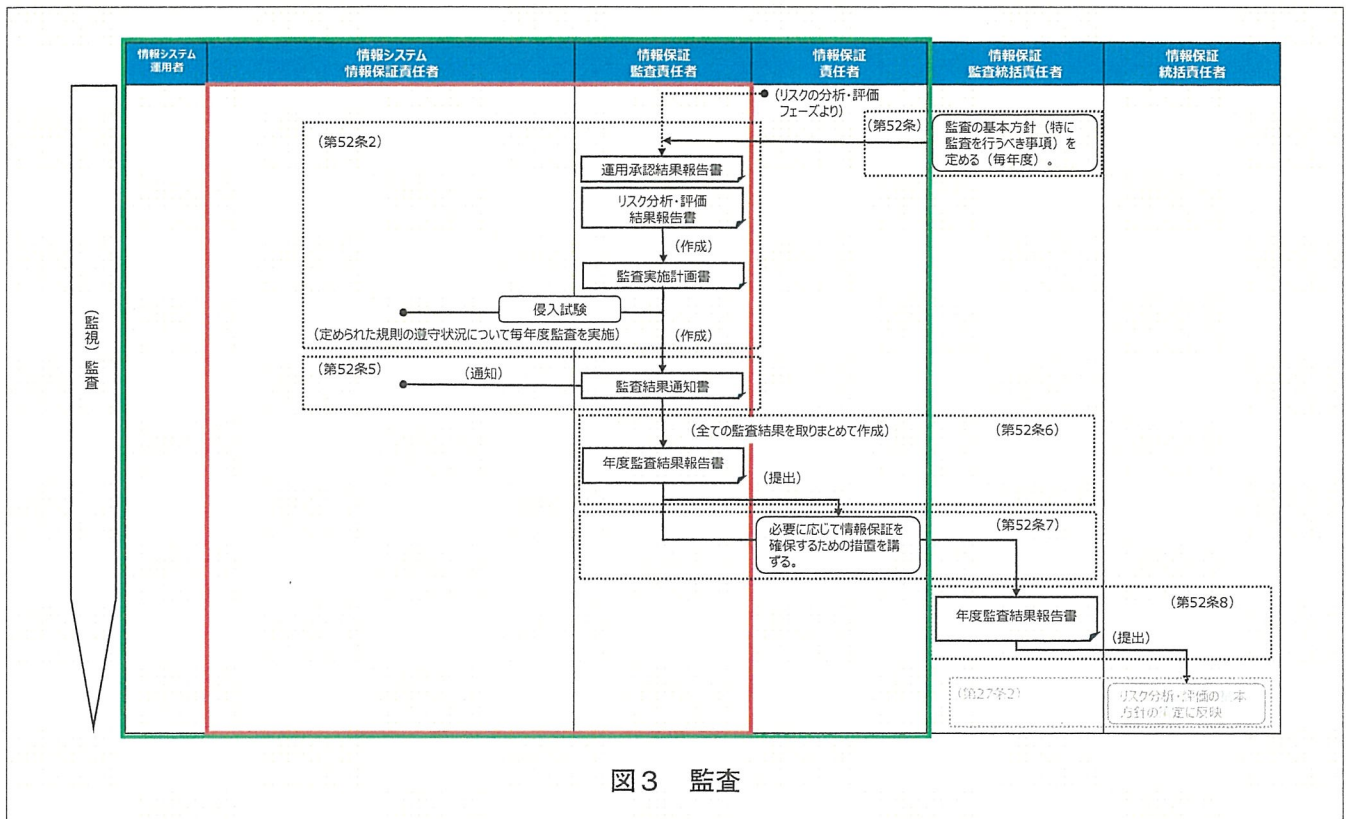


図3 監査

を求めています。

加えて年に1回実施する監査に関連して、情報保証責任者は、私有機器にて業務用データを取り扱っていない旨の誓約書を職員に提出させる旨が明示されています。

情報保証統括責任者は、運用中の各情報システムのリスク管理を一元的に行うことを目的として、情報保証監査責任者に対し管理する情報システムの「監査結果報告書」について、随時提出を求めることができますとしています。

以上の流れを図3に整理します。

監査の種類や実施周期などについては、機関ごとに確認が必要です。

(2) 特別監査

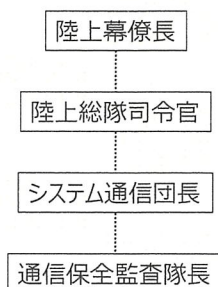
情報保証監査統括責任者は、通常の監査に加え、情報保証訓令および同訓令に基づき定められた規則の遵守状況について、必要に応じて特別監査を行うとされています（第53条）。この際、運用通達は、特別監査の計画、特別監査の項目、その他必要な事項を定めるとしています。

情報保証監査統括責任者は、特別監査を行う

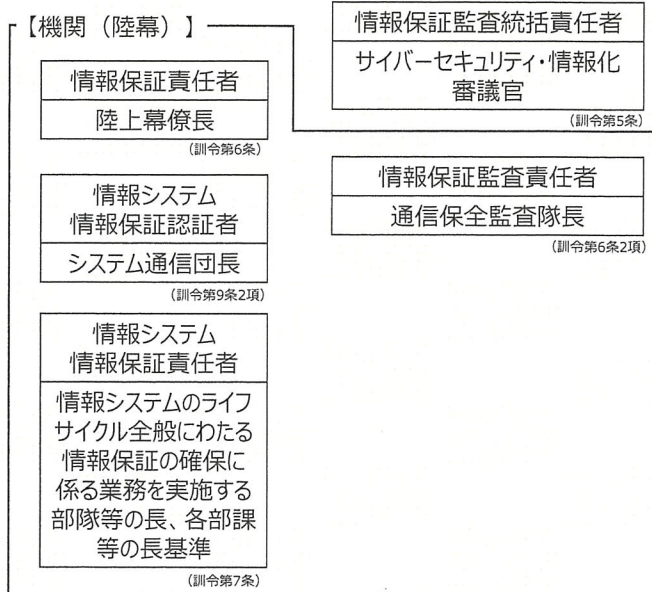
にあたり、情報保証責任者および特別監査の対象となる機関等以外の情報保証監査責任者に協力を依頼することができます（53条2）。このことを、運用通達では「特別監査の対象機関等ではなく第三者的観点を確認するとともに特別監査の実効性を確保するための措置」として実行を要求することに加え、情報保証監査責任者の情報保証監査統括責任者に対する協力も求めています。

特別監査を実施した場合、その結果を取りまとめ、対象となった機関等の情報保証監査責任者に通知し、必要に応じて情報保証を確保するための措置を講じます（53条3）。そして特別監査の結果、情報保証を確保する上で重要な問題が発見された場合、防衛大臣および情報保証統括責任者に報告することが義務付けられています（53条4）。これに関連して、運用通達では、情報保証監査統括責任者は特別監査の結果、重大な問題が発見されない場合においても、その結果を情報保証統括責任者に通知することと補足しています。

【基本的指揮系統】



【情報保証訓令上の関係（抜粋）】



陸上自衛隊の情報保証に関する達（陸自達61-8（19.12.17））より

図4 情報保証訓令上の役職の指定（陸上自衛隊の場合）

機関レベルのRMFについて

一例として、陸上自衛隊の場合、情報保証責任者である陸上幕僚長は、システム通信団長を情報システム情報保証認証者、その隷下である通信保全監査隊長を情報保証監査責任者に指定しています。つまり対象となる情報システムは、情報システム情報保証認証者であるシステム通信団長による認証結果を踏まえ、情報保証責任者である陸上幕僚長により運用が承認されますが、承認を受けた運用開始後の監視フェーズにおいては、同情報システムを対象に、情報保証監査責任者である通信保全監査隊長が監査を実施することになっています（図4）。

この点については、監査の独立性について検討の余地が残されている可能性があり、他機関も含め、確認の必要があるかもしれません。

おわりに

防衛省機関内の承認申請側で勤務する管理者および担当者は、新規の情報システムについて

運用承認申請を行うことに加え、運用承認を得て運用を開始する情報システムについてはリスク分析・評価を実施した上で策定した文書を更新し、審査を受けるとともに、監査を受けるといった手続きがライフサイクルを通じて毎年必要となります。しかしながら、管理者および担当者は、情報システムやRMFの処理手順に習熟した段階で異動となるなど、防衛省・自衛隊の特性に起因する勤務サイクルを避けることができません。

一方、認証側、監査側についても同様・同質の課題、すなわち育成した人材や知見が十分に蓄積されないといった問題が存在します。この結果、各情報システムの特性や継続的監視への対応経緯の細部といった点について、官のみで維持することがやや難しい状況にあるのではないかと推測します。

このような状況を踏まえると、今後も、ユニフォームにしか担うことのできない業務はユニフォームが実施し、ユニフォームが実施することが望ましいものの、その特性上、継続的な対応が困難な場合は民間の支援を受けるといった、現行の取り組みを継続していくことについて

も検討の余地があるのではないかと考えます。

一方で、前号でも触れましたが、米国防省はRMFの承認プロセスにおける長期化や硬化、チェックボックス・セキュリティ、静的評価、更にはそれらに伴うコストやリソースの増大を課題と認識しています。こうした課題を踏まえ、同省は2025年9月24日、サイバーセキュリティリスク管理構造(CSRMC)のリリースを宣言しました(細部は前号を参照)。CSRMCは、RMFのプロセスを上書き・包含し、文書ベースの認定から自動化された継続モニタリングに移行することで、自動化・高速化を図り、常時接続・常時監視による常時運用認可(cATO)、つまり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しているとされています。しかしながら、その詳細は依然として不明な点も多く、今後の動向を注視していく必要があります。

防衛省・自衛隊においては、当面は現行の情

報保証訓令に従った対応が求められていくことになると思われますが、情報システム業務に従事する可能性のある隊員の方々のみならず、組織全体でサイバーセキュリティに関する知見の底上げが求められ始めており、部隊運用に係わる管理者の方々においても、サイバーセキュリティへの理解が必須となる時代が到来しています。

今後、サイバーセキュリティの基礎やRMFなどの基本的な事項は、防衛大学校における教育や自衛隊における基本教育において、共通素養として位置づけていくことも有力な選択肢の一つであると考えます。

参考文献

- 1) 「防衛省の情報保証に関する訓令」(防衛省訓令第160号 19.9.20), 防衛省 HP (Accessed on Feb. 16, 2026)
- 2) 「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), 防衛省 HP (Accessed on Feb. 16, 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>