防衛研究所達第８号

防衛省の情報保証に関する訓令（平成１９年防衛省訓令第１６０号）の規定を実施するため、防衛研究所の情報保証に関する達を次のように定める。

平成１９年１２月２１日

防衛研究所長　戸田　量弘

防衛研究所の情報保証に関する達

改正　平成２３年９月　１日防衛研究所達５号
平成２６年７月２３日防衛研究所達６号
平成２７年４月１０日防衛研究所達１号
令和２年１２月２３日防衛研究所達１７号
令和４年３月３日防衛研究所達１２号

目次

第１章　　総則

（趣旨）

第１条　この達は、防衛研究所における情報保証に関して必要な事項を定めるものとする。

（定義）

第２条　この達において、次の各号に掲げる用語の意義は、防衛省の情報保証に関する訓令（平成１９年防衛省訓令第１６０号。以下「訓令」という。）に定めるもののほか、それぞれ当該各号に定めるところによる。

（１）防衛研究所情報システム

防衛研究所の情報システムをいう。

（２）官品可搬記憶媒体

職務の遂行のために使用するものであって、防衛省が管理する可搬記憶媒体をいう。

（３）私有可搬記憶媒体

官品可搬記憶媒体以外の可搬記憶媒体をいう。

（４）認証情報等

ユーザ名及び認証情報並びにこれらを記録したＩＣカードその他の媒体をいう。

（５）各部等

企画部総務課、企画部企画調整課、政策研究部、理論研究部、地域研究部、教育部、戦史研究センター及び特別研究官（国際交流・図書担当）及び特別研究官（政策シミュレーション担当）をいう。

（６）職員等

次に掲げる者をいう。

ア　防衛研究所の職員（非常勤職員を含む。）

イ　防衛研究所の研修員

（７）運用通達

防衛省の情報保証に関する訓令の運用について（防運情第９２４８号。１９．９．２０）をいう。

第２章　組織及び任務

（組織）

第３条　訓令第７条第１項に規定する情報システム情報保証責任者（以下「システム責任者」という。）は、企画部長とする。

２　訓令第８条第１項に規定する部隊等情報保証責任者（以下「部隊等責任者」という。）は、各部等の長とする。

３　訓令第８条第３項に規定する臨時に部隊等責任者の職務を代行する職員（以下「代行者」という。）は部隊等責任者が、部下職員の中から指定することができるものとする。

４　訓令第９条第１項に規定する情報システム運用者は、企画部総務課長とする。

５　訓令第９条第２項に規定する情報システム情報保証認証者（以下「システム認証者」という。）及び訓令第１１条に規定する事案対処責任者は、防衛研究所副所長とする。

６　訓令第１２条第２項に規定する情報保証責任者が指定する者は、企画部長をもって充てる。

（補助者等）

第４条　情報保証責任者、システム責任者、部隊等責任者、情報システム運用者、システム認証者、事案対処責任者、防衛省中央ＯＡネットワーク・システム運用管理要綱について（通知）（防整情第３２１４号。令和４年３月２日。）別冊「防衛省中央ＯＡネットワーク・システム管理要綱」（以下「省ＯＡシステム管理要綱」という。）に規定する機関等運用管理者及び情報システム情報保証責任者補助者（機関等運用管理担当）は、それぞれその事務を補佐する補助者等を指定するものとする。

２　前項の場合において、システム責任者、部隊等責任者、省ＯＡシステム要綱に規定する機関等運用管理者及び情報システム情報保証責任者補助者（機関等運用管理担当）は、補助者等を指定するに当たり、補助者等ごとにその業務の内容を明確にするとともに、当該補助者等が行う業務の内容に基づき、技術的知見その

他の情報保証に関する知見を有する者を指定する等、指定しようとする者の有する知見を考慮の上行うものとする。

３　補助者等を指定した者は、当該補助者等の行う業務について、その責任を負う。

（情報保証責任者の任務）

第５条　情報保証責任者は、訓令に定めるもののほか、防衛研究所情報システム（以下「本システム」という。）の整備及び運用等に関する事務を統括するものとする。

（システム責任者の任務）

第６条　システム責任者は、本システムの情報保証並びに整備及び運用等に関し、訓令に定めるもののほか、情報保証責任者の命を受け次の各号に掲げる事務を行うものとする。

（１）運用の統制に関すること。

（２）保守に関すること。（システム責任者が別に定めるものを除く。）

（３）ハードウェアの管理に関すること。

（４）ソフトウェアの管理に関すること。

（５）ネットワークの管理に関すること。

（６）本システムに必要な電子計算機情報の管理に関すること。

（７）消耗品の補給に関すること。

（８）その他特に命ぜられた事項

（部隊等責任者の任務）

第７条　部隊等責任者は、本システムの情報保証に関し、情報保証責任者の命を受け次の各号に掲げる事務を行うものとする。

（１）防衛研究所の可搬記憶媒体の管理に関すること。

（２）私有パソコン及び私有可搬記憶媒体の取扱いに関すること。

（３）その他特に命ぜられた事項

（情報システム運用者の任務）

第８条　情報システム運用者は、本システムの運用に関し、情報保証責任者の命を受け次の各号に掲げる事務を行うものとする。

（１）第１９条第１項の規定に基づき、システム責任者が作成する実施計画（以

下「実施計画」という。）について、本システムを利用する者の立場からシステム責任者に対し、必要な提言を行うこと。

（２）その他特に命ぜられた事項

（システム認証者の任務）

第９条　システム認証者は、本システムの運用に関し、情報保証責任者の命を受け次の各号に掲げる事務を行うものとする。

（１）実施計画について、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こと。

（２）実施計画について、審査及び認証を行うこと。

（３）前号の規定に基づき、認証結果報告書を作成し、情報保証責任者に提出すること。

（４）その他特に命ぜられた事項

（事案対処責任者の任務）

第１０条　事案対処責任者は、本システムへのサイバー攻撃等の未然防止及び対処に関し、情報保証責任者の命を受け次の各号に掲げる事務を行うものとする。

（１）システム責任者の統制に関すること。

（２）システム責任者への技術的支援に関すること。

（３）その他特に命ぜられた事項

（システム利用者）

第１１条　本システムを利用することができる者（以下「システム利用者」という。）は、次の各号に掲げる者とする。

（１）職員等

（２）その他情報保証責任者が認めた者

２　システム利用者は、本システムの利用に当たり情報保証責任者、システム責任者及び部隊等責任者の指示に従い、情報保証の確保に努めるものとする。

（防衛研究所情報保証対策委員会）

第１２条　本システムの情報保証並びに整備及び運用に関して、各部等相互間の調整、連絡及び技術的事項の検討並びに第４３条に規定する評価及び見直しの審議を行うため、防衛研究所情報保証対策委員会（以下「委員会」という。）を設置

する。

２　委員会は、委員長及び委員をもって構成し、委員長は企画部長を、委員は各部等の長をもって充てる。

３　委員会の運営に関し必要な事項は、委員長が別に定める。

第３章　情報システムに係る対策

第１節　情報システムの整備等に当たっての対策

（認証機能等）

第１３条　システム責任者は、訓令第１３条から第１９条に規定する各機能等を本システムに設ける場合は、それぞれ訓令に規定する機能を整備し、又は本システムの設定を行わなければならない。

２　システム責任者は、第１項により各機能設計を行うに当たり、必要に応じてシステム運用者の意見を取り入れ、実施計画に示さなければならない。

３　システム責任者は、第１項により各機能を設ける際、本システムが廃止されるまでの間、当該機能が十分に発揮されるよう、必要な利用及び維持管理体制について、合わせて検討しなければならない。

（情報システムの動作確認等）

第１４条　システム責任者は、本システムにソフトウェアを導入し、又はソフトウェアの更新を行う場合は、あらかじめ当該ソフトウェアの導入又は更新に伴い、情報システムに不具合が生じないこと、その他情報保証を確保する上で必要な事項を確認しなければならない。

２　システム責任者は、前項の動作確認に当たり、その結果を実施計画に示さなければならない。

（情報システム間の接続）

第１５条　システム責任者は、本システムを他の情報システムと接続する場合は、当該接続する他の情報システムのシステム責任者と、連接の形態、相互に交換する電子計算機情報の内容、通信内容の監査方法、その他接続に必要な内容について協議し、実施計画に示さなければならない。

２　システム責任者は、前項に基づき他の情報システムと接続する場合は、相互に

交換すると定めた情報以外が交換されないようにしなければならない。

（情報システムの設置）

第１６条　システム責任者は、訓令第２２条の規定に基づき、情報保証を確保するために必要と認める場合は、情報システム室に本システムの全部又は一部を設置しなければならない。

２　システム責任者は、本システムの設置に関し、システム運用者の意見を聴取し、設置に必要な事項を実施計画に示さなければならない。

３　システム責任者は、設置される本システムの構成器材に対して、必要に応じ無許可での構成変更等を物理的に阻止するための措置を行うものとする。

４　システム責任者は、必要に応じ訓令第２２条第２項に定めるもののほか、本システムの設置に必要な物理的対策を講じるものとする。

５　システム責任者は、本システムの搬入又は設置を部外者に行わせる場合は、あらかじめ立会者を指名して同行させ、保全のための必要な措置を講じなければならない。

（情報システムの部外への設置）

第１７条　システム責任者は、訓令第２３条の規定に基づき、本システムの全部又は一部を部外に設置する場合は、事前に情報保証責任者の承認を得なければならない。

（情報システムの技術に関する基準）

第１８条　システム責任者は、訓令第２４条の規定により整備計画局長が別に定める情報システムが満たすべき情報保証に関する技術上の基準に従い、本システムの整備等の際に、必要な措置を講じなければならない。

第２節　運用承認

（運用承認）

第１９条　システム責任者は、訓令別表第３の左欄に掲げる場合には、運用承認を得なければならない。

２　前項の運用承認に当たっては、必要に応じて事前に委員会において審議するものとする。

第３節　情報システムの運用、管理等に当たっての対策

（認証情報等の管理）

第２０条　システム責任者は、システム利用者以外の者が利用できないよう、あらかじめ本システムを設定しなければならない。

２　システム責任者は、システム利用者に対し、必要に応じて認証情報等を付与するものとする。

３　システム責任者は、前項の規定に基づき付与した認証情報等の管理に関する規則を定め、システム利用者に周知するものとする。

４　第１項の規定により認証情報等を付与されたシステム利用者は、前項の規定により定めた規則に基づき、付与された認証情報等を適切に管理しなければならない。

（アクセス制御）

第２１条　システム責任者は、訓令第１４条の規定に基づき、本システムにアクセス制御機能を設けた場合は、当該機能の使用について、システム利用者が実施すべきアクセス制御に必要な要領を定め、周知させるものとする。

２　システム利用者は、電子計算機情報のうち利用を制限すべき電子計算機情報がある場合は、必要に応じて前項に定める要領に基づき、本システムに設けたアクセス制御機能により適切にアクセス制御を行わなければならない。

（証跡管理）

第２２条　システム責任者は、訓令第１５条の規定に基づき、本システムに証跡管理機能を設けた場合は、当該機能の管理運用に必要な要領を定め、証跡を適切に取得するとともに、5年を基準に本システムが換装又は運用が終了するまでの間は保存しなければならない。

２　システム責任者は、前項の要領に従い、証跡管理機能を設定し、証跡を取得、保存、破棄及び分析するものとする。

３　事案対処責任者は、サイバー攻撃等未然防止及び対処に当たり必要と認める場合は、証跡に関しシステム責任者に所要の指示をすることができるものとする。

（暗号化）

第２３条　システム責任者は、訓令第１６条の規定に基づき、本システムに暗号化機能を設けた場合は、情報の暗号化が有効に行われるよう、当該機能を適切に運用しなければならない。

２　本システムに設けた暗号化機能の維持及び管理要領は、別に示す。

３　システム利用者は、電子計算機情報を官品可搬記憶媒体に格納し、又は送信するに当たり本システムに設けられた暗号化機能を用いて、当該電子計算機情報の暗号化を適切に実施しなければならない。

（電子署名）

第２４条　システム責任者は、訓令第１７条の規定に基づき、本システムに電子署名機能を設けた場合は、当該機能の運用に必要な要領を定め、適切に運用するものとする。

２　システム責任者は、システム利用者に対し、前項により定められた要領に基づき、電子署名機能を利用させるものとする。

（脆弱性対応）

第２５条　システム責任者は、本システムの脆弱性対応機能の運用及び本システムに、新たに発生する脆弱性の管理に対応するための要領を定めるものとする。

２　システム利用者は、前項によりシステム責任者の定めた要領に基づき、本システムの脆弱性に対応するため、必要な措置を行わなければならない。

（情報システム室の入退室管理）

第２６条　システム責任者が定める情報システム室及びこれに準ずる施設に立ち入る者は、システム責任者の許可を得なければならない。

２　システム責任者は、前項により立入りを許可した者に許可札を交付し、当該許可札を装着させて立入りさせるものとする。

３　第１項の規定に基づき、許可を得た者は、入退出の際、システム責任者が別に定める入退出記録に所要の事項を記録しなければならない。

（電子計算機の管理）

第２７条　システム責任者は、電子計算機について、設置場所、使用者名等を記載した管理簿を設け、適切に管理しなければならない。

２　システム利用者は、電子計算機を職場から持ち出してはならない。ただし、シ

ステム責任者は、業務上の必要性により電子計算機を職場から持ち出す必要があると認めた場合は、持ち出しの都度当該電子計算機の持出しを許可することができるものとする。

3　システム責任者は、前項ただし書の規定による電子計算機の持出しについて、情報保証を確保するために必要な措置の実施を確認しない限り、当該電子計算機の持出しを許可してはならない。

4　システム責任者は、第２項ただし書の規定により電子計算機の持出しを許可した場合は、第１項に規定する管理簿に持出し先、持出し期間等の必要な事項を記録し、適切に管理しなければならない。

5　第２項ただし書の規定により電子計算機の持出しを許可されたシステム利用者は、当該電子計算機の持出し先での盗難及び紛失防止に努めなければならない。

6　第２項ただし書の規定により電子計算機の持出しを許可されたシステム利用者は、当該電子計算機を盗難され又は紛失した場合は、直ちにシステム責任者に通報するものとする。

7　システム責任者は、可搬型の電子計算機（第２項により許可を得て持ち出されているものを除く。）については、ワイヤーで机等に固定の上当該ワイヤーを施錠し、又はワイヤーで机等に固定することが困難な場合は、電子計算機を使用しないときにロッカー等に保管の上これを施錠するものとする。

8　前項において使用するワイヤー又はロッカー等のかぎは、システム責任者又はシステム責任者の補助者が管理するものとする。

（情報システムの変更）

第２８条　システム利用者は、本システムについて次の各号に掲げる事項を変更する場合は、事前にシステム責任者の許可を得なければならない。

（１）本システムに係る配線の変更、改造

（２）機器の増設又は交換

（３）ソフトウェアの新規導入及び変更

2　システム責任者は、前項の許可を求められた場合は、本システムの情報保証を確保する上で問題がないことを確認しない限り、これを許可してはならない。

3　システム責任者は、第１項について所要事項を記録し、保存しなければならな

い。

（情報システムに関する文書の整備等）

第２９条　システム責任者は、本システムの仕様、設計、機器の設置場所、使用者名、その他本システムの管理に関する事項を記載した文書を整備しなければならない。

２　システム責任者は、必要に応じ本システムの保有する機能について、その運用に必要な要領等を定めるものとする。

３　システム責任者は、本システムの利用及び管理に関する規則を定めなければならない。

４　システム責任者は、第２項及び前項により定めた要領等及び規則について、適宜見直しを行うものとする。

５　システム責任者は、第２項及び第３項により定めた要領等及び規則をシステム利用者に周知しなければならない。

６　システム利用者は、第３項のシステム責任者が定める規則に基づき、本システムを利用及び管理しなければならない。

（業務目的外の使用禁止）

第３０条　システム利用者は、次の各号に掲げる目的以外のために本システムを使用してはならない。

（１）調査研究

（２）教育訓練

（３）前２号に掲げるもののほか、防衛研究所において必要な業務

（４）その他情報保証責任者が認めた使用

（使用の制限）

第３１条　システム責任者は、第３０条に規定するシステム利用者が認められた目的以外で本システムを使用した場合、公序良俗に反する使用を行った場合、又は本システムに重大な障害を起こした場合は、当該システム利用者に対し、一定の期間を限り、使用の承認の全部又は一部を取り消すことができる。

２　システム責任者は、前項の取消しを行う場合は、事前に情報保証責任者の承認を得るものとする。

（職員等以外の情報システムの利用）

第３２条　システム責任者は、維持管理等において職員等以外の者に本システムを利用させる場合は、第２９条第３項の規定に基づきシステム責任者が定める規則、その他関係規則のうち、必要な事項を当該職員等以外の者に理解させ、遵守させるようにしなければならない。

（情報システムの障害発生時の措置等）

第３３条　システム責任者は、本システムに障害が発生した場合は、速やかに当該障害を復旧するための措置を講ずるとともに、当該障害の記録を作成し、一定期間保存しなければならない。

２　システム責任者は、本システムに要求される可用性及び完全性に応じて、電子計算機情報の複製を作成し、保存しなければならない。

３　システム利用者は、自ら使用する電子計算機情報について、必要に応じ複製を作成し、保存するものとする。

第４節　情報システムの廃棄等に当たっての対策

（情報システムの廃棄等）

第３４条　システム責任者は、本システムの全部又は一部を修理、廃棄又は返却のため部外の者に受け渡す場合は、必要に応じて当該情報システムに保存された電子計算機情報の複製を作成するとともに、ハードディスク等の物理的な破壊又は当該情報システムに保存された電子計算機情報を完全に消去する措置を講じ、当該電子計算機情報を復元不可能な状態にしなければならない。

第４章　防衛研究所の可搬記憶媒体に係る対策

（可搬記憶媒体の管理）

第３５条　部隊等責任者は、官品可搬記憶媒体について、使用者名等を記載した管理簿を設けるとともに、集中保管を行わなければならない。

２　システム利用者は、官品可搬記憶媒体を業務上の必要性から職場から持ち出す場合は、持出しの都度、部隊等責任者の許可を得るものとする。

３　部隊等責任者は、前項の規定による官品可搬記憶媒体の持出しについて、情報

保証を確保するために必要な措置の実施を確認しない限り、当該官品可搬記憶媒体の持出しを許可してはならない。

4　部隊等責任者は、第２項の規定により官品可搬記憶媒体の持出しを許可した場合は、第１項に規定する管理簿に持出し先、持出し期間等必要な事項を記録し、適切に管理しなければならない。

5　第２項の規定により官品可搬記憶媒体の持出しを許可されたシステム利用者は、当該官品可搬記憶媒体の持出し先での盗難及び紛失防止に努めなければならない。

6　第２項の規定により官品可搬記憶媒体の持出しを許可されたシステム利用者は、当該官品可搬記憶媒体を盗難され又は紛失した場合は、直ちに部隊等責任者及びシステム責任者に通報するものとする。

第５章　私有パソコン及び私有可搬記憶媒体の取扱い

（私有パソコンの取扱い）

第３６条　職員等は、私有パソコンを職場に持ち込んではならない。

２　職員等は、私有パソコンで業務用データを取り扱ってはならない。

（私有可搬記憶媒体の取扱い）

第３７条　職員等は、私有可搬記憶媒体を本システムで使用してはならない。

２　職員等は、私有可搬記憶媒体で業務用データを取り扱ってはならない。

第６章　教育及び訓練

（教育及び訓練）

第３８条　情報保証責任者は、職員等の情報保証に関する意識の高揚及び情報保証に必要な知識の習得並びに遵守事項の徹底を図るため、計画的に又は機会をとらえて情報保証に関する教育及び訓練を実施するものとする。

２　システム責任者は、本システムの有効活用を図るため、職員等への情報の提供又は教育を実施するものとする。

３　情報保証責任者及びシステム責任者は、第１項及び前項の規定に基づき、教育及び訓練を実施するに当たり、年度計画を作成し、計画的に実施するものとする。

４　情報保証責任者、システム責任者、部隊等責任者、情報システム運用者、システム認証者及び事案対処責任者は、それぞれその補助者に対して、情報保証及び情報システムに関する知識及び技能の向上を促すとともに、機会を捉えて部外の教育等に参加させるものとする。

第７章　サイバー攻撃等への対処

（対処要領の策定）

第３９条　訓令第４７条の規定に基づくサイバー攻撃等に対処するための要領は、別に示す。

２　事案対処責任者は、前項に規定する要領に基づき、サイバー攻撃等の対処のための必要な措置に関し、事案対処統括責任者及び他の機関等の事案対処責任者と調整を行い、システム責任者を統制し、又はシステム責任者に対し技術的支援を行うものとする。

第８章　対策の実施状況の確認等

（自己点検）

第４０条　職員等（システム責任者が別に定める者を除く。次条において同じ。）は、訓令及びこの達に基づき定められた規則の遵守状況について、毎年度、自己点検を行わなければならない。

２　第１項に規定する自己点検の要領については、システム責任者が別に示す。

（監査等）

第４１条　情報保証責任者は、本システムの監査を適宜実施し、本システムの情報保証の確保に努めるものとする。

２　情報保証責任者は、前項に規定する本システムの監査の結果、本システムの改善の必要があると認められる場合、その改善についてシステム責任者に提案するものとする。

３　システム責任者は、前項の情報保証責任者の提案に基づき、本システムの改善に努めるものとする。

４　システム責任者は、訓令、この達その他関係規則の遵守状況について、次の各

号に掲げる監査を行うものとする。

（１）第４０条第１項の規定に基づく自己点検の結果を踏まえ、毎年度１回以上行う定期監査

（２）情報保証に関する問題点等を考慮の上、必要に応じて行う臨時監査

５　システム責任者は、前項の規定に基づき、監査を実施するに当たり、年度計画を作成し、計画的に実施するものとする。

６　部隊等責任者は、第４項のシステム責任者が行う監査に協力するものとする。

７　部隊等責任者は、運用通達第１１第３項第１号に規定する自宅の私有パソコン等の確認について、職員等のうち、同意を得た者について、管下の当該職員等のプライバシーに十分配慮して行うものとする。

８　部隊等責任者は、前項の確認の結果、ファイル共有ソフトがインストールされていることが確認された場合は、ファイル共有ソフトの使用に伴う危険性等を教育することにより、当該ファイル共有ソフトの自発的な削除を促すものとする。

９　職員等は、私有パソコン及び私有可搬記憶媒体で業務用データを取り扱っていない旨の誓約書を情報保証責任者に提出するものとする。

（職員等による報告等）

第４２条　職員等は、訓令、この達その他関連規則に関する違反が発生し、又は発生したおそれがあると認める場合は、直ちにシステム責任者に通報しなければならない。

２　システム責任者は、前項の通報を受けた場合は、直ちに情報保証責任者に報告しなければならない。

３　インターネット上への情報流出を把握した場合の対応要領は、システム責任者が別に定める。

第９章　評価及び見直し

（評価及び見直し）

第４３条　委員会は、技術の進歩等により本システムに新たな対策等を講じる必要が生じた場合は、この達その他関連規則の実効性を評価し、必要に応じ見直しを審議する。

第１０章　雑則

（委任規定）

第４４条　この達に定めるもののほか、情報保証の確保に関し必要な事項は、システム責任者が別に定めることができる。

附　則

１　この達は、平成２０年１月１日から施行する。ただし、予算的措置を必要な条項の規定は、所要の措置がなされた時期から適用する。

２　防衛研究所情報システム管理運用規則（平成１６年防衛研究所達第１０号）は、平成１９年１２月３１日限り廃止する。

附　則（平成２３年９月１日防衛研究所達第５号）

この達は、平成２３年９月１日から施行する。

附　則（平成２６年７月２３日防衛研究所達第６号）

この達は、平成２６年７月２３日から施行する。

附　則（令和３年１月１日防衛研究所達第７号）

この達は、令和３年１月１日から施行する。

附　則（令和４年３月３日防衛研究所達第１２号）

この達は、令和４年３月３日から施行する。