情報本部達第５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）第５７条の規定に基づき、情報本部の情報保証に関する達を次のように定める。

平成２０年３月２１日

情報本部長　陸将　椋木　功

改正　平成21年 1月30日情報本部達第　２号（第１次改正）
改正　平成21年11月20日情報本部達第　２５号（第２次改正）
改正　平成23年12月16日情報本部達第　１２号（第３次改正）
改正　平成24年 3月28日情報本部達第　５号（第４次改正）
改正　平成26年 6月19日情報本部達第　７号（第５次改正）
改正　平成26年12月10日情報本部達第　１２号（第６次改正）
改正　平成29年11月16日情報本部達第　１５号（第７次改正）
改正　平成30年 3月29日情報本部達第　５号（第８次改正）
改正　令和 4年 6月29日情報本部達第　８号（第９次改正）
改正　令和 5年 6月29日情報本部達第１３４号（第10次改正）

情報本部の情報保証に関する達

情報本部の情報保証に関する達（平成２０年情報本部達第５号）の全部を改正する。

目次

第１章　総則（第１条－第３条）
第２章　組織及び体制（第４条－第１４条）
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（第１５条・第１６条）

第２節　運用承認（第１７条・第１８条）
第３節　情報システムの運用、管理等に当たっての対策（第１９条－第３１条）
第４節　情報システムの廃棄等に当たっての対策（第３２条）
第４章　目的特化型機器に係る対策（第３３条）
第５章　可搬記憶媒体に係る対策（第３４条）
第６章　私有機器等の取扱い（第３５条－第３８条）
第７章　教育及び訓練（第３９条）
第８章　サイバー攻撃等への対処（第４０条）
第９章　対策の実施状況の確認等（第４１条－第４４条）
第１０章　雑則（第４５条－第４６条）
附則

第１章　総則

（目的）

第１条　この達は、情報本部における情報保証に関し必要な事項を定め、もって情報本部における情報保証を確保することを目的とする。

（定義）

第２条　この達における用語の意義は、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。）及び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。以下「次官通達」という。）によるほか、次の各号に定めるところによる。

（１）部等　部及び通信所をいう。

（２）課等　課、監査・監察官及び通信支所をいう。ただし、課編制を取らない通信所は、これに準ずる単位とする。

（３）部長等　部長及び通信所長をいう。

（４）課長等　課長、監査・監察官及び通信支所長をいう。ただし、課編制を取らない通信所は、これに準ずる者とする。

（５）情報保証担当課　計画部システム通信課をいう。

（６）情報システム　ハードウェア、ソフトウェア（プログラムの集合体をいう。）、ネットワーク又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をいう。

（７）電子計算機　端末、サーバ等の情報システムの物理的な構成要素をいう。

（８）サーバ等　ファイルサーバ、データベースサーバ、電子メールサーバ、アプリケーションサーバ、コミュニケーションサーバ等、情報システムの利用者（以下「システム利用者」という。）に対してサービスを提供するサーバ装置及びこれらを管理するために使用される端末をいう。

（９）スタンドアロン型情報システム　ネットワークを構成要素とせず独立して業務処理を行う１台の電子計算機をいう。

（10）ＤＩＩ未加入インターネット情報システム　部等が所掌する情報システムのうち、防衛情報通信基盤の業務実施に関する訓令（平成１５年防衛庁訓令第１９号）第２条第１号に規定する防衛情報通信基盤（以下「ＤＩＩ」という。）のデータ通信網を経由せず、インターネットに接続する情報システムをいう。

（11）目的特化型機器　情報システムの構成品に該当せず、主たる使用目的が撮影、録音、複写等であり、機器単体でデータを保存できるもので、機器単体でインターネット等の外部ネットワークに接続し保存しているデータを共有できるものであって、可搬記憶媒体ではないものをいう。

（12）可搬記憶媒体　情報システム又は目的特化型機器に挿入又は接続して情報を保存することができる媒体又は機器のうち、可搬型のものをいう。

（13）私有目的特化型機器　防衛省が管理していない目的特化型機器をいう。

(14) 私有可搬記憶媒体　防衛省が管理していない可搬記憶媒体をいう。

(15) 私有機器　私有パソコン、私有携帯電話、私有目的特化型機器及び私有可搬記憶媒体のことをいう。

(16) 業務用データ　職員が職務上作成し（作成中も含む。）、又は取得したデータであって、当該データに行政機関の保有する情報の公開に関する法律（平成１１年法律第４２号）第５条各号の規定に基づき行う開示又は不開示の処分に係る審査基準を適用した場合、不開示情報に該当する情報が含まれるものをいう。

(17) セキュリティ管理策　防衛省の情報システム及び電子計算機情報の機密性、完全性及び可用性を維持し、情報保証上のリスクを管理するために、情報システム又は組織内で講じられる具体的な措置及び対策をいう。

（適用除外）

第３条　訓令第３条の規定に基づき、訓令を適用しない情報システムを申請する場合、当該情報システムを所掌する部長等は、次官通達第１第３項第１号に示す事項を記載した申請書を作成し、情報保証責任者に申請するものとする。

第２章　組織及び体制

（情報保証責任者補助者）

第４条　訓令第６条第１項に規定する情報保証責任者の業務を補佐し、情報保証の確保に関する事務を統括する者として、情報保証責任者補助者を置くものとする。

２　情報保証責任者補助者は、計画部長をもって充てる。

３　情報保証責任者補助者は、情報システムの情報保証に関する知見を要する検討について、必要に応じ支援するものとする。

（情報保証監査責任者等）

第５条　訓令第６条の２第１項に規定する情報保証監査責任者は、計画部長とする。ただし、計画部の監査については、監査対象から独立し、公正かつ客観的な判断を行うため、情報保全官を情報保証監査責任者とする。

２　訓令第６条の２第２項に規定する情報保証監査責任者補助者の指定は、次による。

（１）情報保証監査責任者は、その補助者として、情報保証監査責任者補助者を指定するものとする。

（２）情報保証監査責任者補助者の指定要領については、別に定める。

（情報システム情報保証責任者等）

第６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は、情報システムを所掌する部長等とする。ただし、これにより難い場合は、情報本部長の指定する部長等とする。

２　訓令第７条第２項に規定する情報システム情報保証責任者補助者の指定は、次による。

（１）情報システム情報保証責任者は、その補助者として、情報システム情報保証責任者補助者を指定するものとする。

（２）情報システム情報保証責任者補助者の指定要領については、別に定める。

（部隊等情報保証責任者等）

第７条　訓令第８条第１項に規定する部隊等情報保証責任者は、課長等とする。

２　前項により難い場合は、部長等が勤務の実状に合わせた単位で指定することができる。

３　部隊等情報保証責任者は、訓令第８条第１項に規定する事項のほか、課等における職員の情報保証に関する規則等の遵守状況の確認及び指導を行うものとする。

４　部隊等情報保証責任者及び訓令第８条第２項に規定する部隊等情報保証責任者補助者の指定要領については、別に定める。

５　訓令第８条第３項に規定する臨時に部隊等情報保証責任者の職務を代行する職員の指定要領については、別に定める。

（情報システム運用者等）

第８条　訓令第９条第１項に規定する情報システム運用者は、情報システム情報保証責任者が指定する者とする。

２　情報システム運用者は、その補助者として、情報システム運用者補助者を指定することができる。

３　情報システム運用者及び情報システム運用者補助者は、情報システム情報保証責任者補助者を兼ねて指定することができる。

４　情報システム運用者及び情報システム運用者補助者の指定要領については、別に定める。

（情報システム情報保証認証者等）

第９条　訓令第９条第２項に規定する各情報システムにおける情報システム情報保証認証者は、情報保全官とする。

２　訓令第９条第３項の規定に基づき、情報システム情報保証認証者は、その補助者として、情報保証担当課より情報システム情報保証認証者補助者を指定するものとする。

３　情報システム情報保証認証者補助者の指定要領については、別に定める。

（事案対処責任者）

第１０条　訓令第１１条に規定する事案対処責任者は、情報保全官とする。

（情報本部情報保証対策委員会）

第１１条　情報保証に関して部等相互の情報共有を図るとともに、重大事案の発生（そのおそれがある場合を含む。）に伴う対応等を行うため、情報本部情報保証対策委員会（以下「委員会」という。）を置く。

２　委員会は、委員長、副委員長及び委員をもって構成する。

３　委員長は、情報保全官とする。

４　副委員長は、計画部長とする。

５　委員は、委員長が必要と認める者とする。

６　委員長は、委員会を招集し、会務を総理する。

７　委員会の庶務は、情報保証担当課において処理する。

（情報保証担当課）

第１２条　情報保証担当課の行う事務については、別に定める。

（部長等）

第１３条　部長等は、部等における情報保証の確保に関する事務を監督し、部隊等情報保証責任者を統括するものとする。

（部等情報保証担当者）

第１４条　部長等は、部等における情報保証の確保に関する事務を担当する者として、部等情報保証担当者を置き、指定するものとする。

２　部長等は、前項の規定に基づき２名以上の部等情報保証担当者を指定した場合、全般統制等を行うため、必要に応じて、当該担当者の中から総括業務を行う者を指定することができる。

３　部等情報保証担当者の行う事務及び指定要領については、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

（情報システムの設置場所）

第１５条　情報本部における立入禁止場所等に関する達（平成２０年情報本部達第４号）により指定された立入禁止場所及び保全区画（以下「立入禁止場所等」という。）は、訓令第２２条に規定する情報システム室として取り扱うものとする。

２　特別防衛秘密電子計算機情報及び特定秘密電磁的記録を取り扱う情報システムは、情報システム室に設置するものとする。

３　秘密電子計算機情報を取り扱う情報システムのサーバ等は、情報システム室に設置するものとする。

４　第２項及び第３項の規定により難い場合は、保全上の必要な許可を受けた後、リスク分析・評価に基づく対策を検討し、運用承認により情報保証責任者の承認を受けなければならない。

（情報システムの部外への設置）

第１６条　訓令第２３条の規定に基づき、情報システム情報保証責任者は、情報システムの全部又は一部を部外に設置する場合、リスク分析・評価に基づく対策を検討し、選択したセキュリティ管理策の実装状況を明確にした上で、運用承認により情報保証責任者の承認を受けなければならない。

第２節　運用承認

（運用承認）

第１７条　訓令第２６条の規定に基づき、情報システム情報保証責任者は、所掌する情報システムが訓令別表第３の左欄に掲げる条件に該当する場合、情報保証責任者に運用承認を受けるものとする。

２　情報システム情報保証責任者は、次官通達第４第１項第１号①から③に定める情報システムについて、情報保証責任者補助者と協議の上、情報保証責任者の承認を得た場合は、運用承認を要しないものとする。

３　第１項の実施については、情報保証統括責任者が定める要領（以下「ＲＭＦ実施要領」という。）に基づき行うものとする。

（情報システムの運用終了報告）

第１８条　情報システム情報保証責任者は、情報システムの運用を終了する場合、速やかに情報保証責任者に報告するものとする。

２　前項の報告要領については、別に定める。

第３節　情報システムの運用、管理等に当たっての対策

（リスク分析・評価）

第１９条　訓令第２７条の２の規定に基づき、情報システム情報保証責任者は、所掌する情報システムについて、毎年度１回以上、リスク分析・評価を行うものとする。

２　情報システム情報保証責任者は、リスク分析・評価を実施するに当たり、当該年度内に運用終了を予定している情報システムがある場合は、あらかじめ、実施の要否、範囲等について、情報保証責任者補助者と調整を行うものとする。

３　情報システム情報保証責任者は、前項の調整結果について、情報保証責任者に報告するものとする。

４　第１項の実施については、ＲＭＦ実施要領に基づき行うものとする。

５　情報システム情報保証責任者は、次官通達第４第１項第１号①から③に該当する情報システムについて、リスク分析・評価の結果を情報保証責任者に報告するものとする。

（認証情報等の管理）

第２０条　訓令第２８条第１項の規定に基づき、情報システム情報保証責任者は、ユーザ名及び認証情報（パスワード、生体情報等）並びにこれらを記録したＩＣカードその他の媒体（以下「認証情報等」という。）の作成、管理等を適切に行うものとする。

２　訓令第２８条第２項の規定に基づき、システム利用者は、認証情報等を盗難、紛失、破損又は忘却した場合、別に定める要領により情報システム情報保証責任者に速やかに報告しなければならない。

３　情報システム情報保証責任者は、前項による報告のうち、特に盗難及び紛失の報告を受けた場合は、直ちに当該認証情報等による情報システムの利用ができないよう情報システムを設定するとともに、不正アクセスの有無を確

認する等の措置を講じなければならない。

（アクセス制御）

第２１条　訓令第２９条の規定に基づき、情報システム情報保証責任者は、情報システムの特権アカウントの使用を適切に行うものとする。

２　情報システムの特権アカウントは、情報システム情報保証責任者が特に認める場合を除き、情報システムの運用、維持管理、リスク分析・評価及び監査に限り使用するものとする。

（証跡管理）

第２２条　訓令第３０条の規定に基づき、情報システム情報保証責任者は、情報システムへのアクセス、情報システムの動作その他情報システムの運用に関する記録（以下「証跡」という。）の設定、取得、分析、保存等を適切に行うものとする。

２　情報システム情報保証責任者は、重要な証跡については常時取得するとともに、必要に応じて証跡を分析し、不正アクセス、障害等を未然に防止して情報保証の確保に努めなければならない。

３　情報システム情報保証責任者は、情報システムの特性に応じ、必要な証跡を記録するものとする。当該証跡については、５年を基準として保存し、当該情報システムが換装又は運用終了後も保存期間満了まで適切に管理するものとする。

４　情報システム情報保証責任者は、証跡を分析した結果、情報保証上の問題点その他改善すべき点が明らかとなった場合は、速やかに対策を講ずるものとする。

（暗号化）

第２３条　訓令第３１条の規定に基づき、情報本部における可搬記憶媒体に電子計算機情報を格納する際の暗号による秘匿を行うべき電子計算機情報の種類は、業務用データとする。

２　情報システム情報保証責任者は、情報システムの機能上、暗号による秘匿を行うことができない可搬記憶媒体について、特に厳重に管理するものとする。

３　システム利用者は、業務用データを可搬記憶媒体に格納する場合、情報システムに設けられた暗号化機能により秘匿しなければならない。

（脆弱性対応）

第２４条　訓令第３３条の規定に基づく脆弱性に関する情報の取扱いについては、次による。

（１）事案対処責任者は、脆弱性に関する情報を収集、分析し、情報システム情報保証責任者に通知するものとする。

（２）情報システム情報保証責任者は、脆弱性に関する情報を入手した場合、事案対処責任者に通報するものとする。

２　情報システム情報保証責任者は、事案対処責任者から脆弱性に関する情報を受け取った場合、適切に対応しなければならない。

３　システム利用者は、情報システムを使用する際に、情報システムに設けられた脆弱性に対応するために導入した機能等（ウイルス対策ソフト等）が正常に動作していない場合は、直ちに当該情報システムの利用を停止するとともに、速やかに情報システム情報保証責任者に通報し、正常に動作することが確認できるまで使用してはならない。

４　コンピュータ・ウイルス等の感染拡大防止に係る対策については、別に定める。

（情報システム室の入退室管理）

第２５条　訓令第３４条の規定に基づき、情報システム情報保証責任者は、立入禁止場所等に該当しない情報システム室について、当該情報システム室で勤務する職員（関係部等の職員を含む。）以外の者の入退室を、別に定める要領により記録するものとする。

（情報システムの管理）

第２６条　訓令第３５条の規定に基づき、情報システムの盗難対策及び持出し時における管理要領については、別に定める。

（情報システムの変更）

第２７条　訓令第３６条の規定に基づき、職員は、情報システムの変更を行う必要がある場合、別に定める要領により情報システム情報保証責任者の許可を受けなければならない。

２　情報システム情報保証責任者は、システム利用者からの申請又は情報システムの運用及び維持管理の必要により行う情報システムの変更が情報システムの情報保証の確保に影響を及ぼすおそれのある場合、訓令別表第３に従い、運用承認を受けなければならない。

（情報システムの利用及び管理に関する規則等）

第２８条　訓令第３７条の規定に基づき、情報システム情報保証責任者は、必要に応じて情報システムに関する組織体制、運用、維持管理、障害発生時の対応、保全等に関する規則を定め、システム利用者に周知しなければならない。

（職員以外の情報システムの利用）

第２９条　訓令第３９条の規定に基づき、情報システム情報保証責任者は、情報システムの維持管理契約等に基づく場合を除き、職員以外の者に情報システムを利用させてはならない。

２　情報システム情報保証責任者は、前項に基づき職員以外の者に情報システムを利用させる場合、情報システムの利用状況について常に把握するとともに、別に定める要領により記録するものとする。

（情報システムの障害発生時の措置等）

第３０条　訓令第４０条第１項の規定に基づき、情報システム情報保証責任者は、情報システムに障害が発生した場合、別に定める要領により障害内容を

記録するものとする。

２　訓令第４０条第２項の規定に基づき、情報システム情報保証責任者は、定期的に電子計算機情報のバックアップを実施する等、速やかに障害復旧するための措置を講ずるものとする。

３　情報システム情報保証責任者は、障害の原因を分析するとともに、障害復旧後、速やかに再発防止のための措置を講ずるものとする。

４　情報システム情報保証責任者は、障害の原因を分析した結果、情報保証上の問題点その他改善すべき点が明らかとなった場合は、速やかに対策を講ずるとともに、必要に応じて、情報システム運用者及び情報システム情報保証認証者と協議するものとする。

（情報システムの特性に応じた対策等）

第３１条　訓令第４１条の規定に基づき、情報システム情報保証責任者は、ＤＩＩ未加入インターネット情報システムについて、別に定める要領により電子メール（Ｗｅｂメールを含む。）及びオンラインストレージ（以下「電子メール等」という。）の利用を禁止する措置を講ずるものとする。ただし、情報システム情報保証責任者が、業務上の必要性からやむを得ないと認める場合は、情報保証責任者補助者と協議の上、電子メール等の利用を許可することができる。

２　システム利用者は、前項で許可された場合を除き、ＤＩＩ未加入インターネット情報システムで電子メール等を利用してはならない。

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３２条　訓令第４２条の規定に基づき、情報システム情報保証責任者は、情報システムの全部又は一部を廃棄、修理又は返却する場合、次の処置を講ずるものとする。

（１）電子計算機の内蔵ハードディスク等に格納された電子計算機情報の消去については、記憶媒体及び格納されている電子計算機情報の種類を考慮した消去方法（データ消去ソフト等による上書き消去、ＯＳ又は機器のフォーマット（初期化）機能、消磁、物理破壊等）により、当該電子計算機情報を復元不可能な状態に抹消するものとする。ただし、業者への返却等、契約上の理由又は機能上の制約により格納された電子計算機情報を抹消することができない場合を除く。

（２）ルータ、複合プリンタ等に記録されている情報システム独自の設定等は、設定内容の初期化又は削除を行うものとする。

２　情報システム情報保証責任者は、前項の処置を行なった場合、別に定める要領により記録するものとする。

第４章　目的特化型機器に係る対策

（目的特化型機器の管理要領）

第３３条　訓令第４２条の２の規定に基づく目的特化型機器の管理要領については、別に定める。

第５章　可搬記憶媒体に係る対策

（可搬記憶媒体の管理要領）

第３４条　訓令第４３条の規定に基づく可搬記憶媒体の管理要領については、別に定める。

第６章　私有機器等の取扱い

（私有パソコンの持込・使用要領）

第３５条　訓令第４４条第１項の規定に基づき、職員は、私有パソコンを職場に持ち込んではならない。

２　訓令第４４条第３項の規定に基づき、職員は、私有パソコンで業務用データを取り扱ってはならない。

３　部外者の職場への私有パソコンの持込み及び使用要領については、別に定める。

（私有目的特化型機器及び私有可搬記憶媒体の持込・使用要領）

第３６条　職員又は部外者の職場への私有目的特化型機器及び私有可搬記憶媒体の持込み及び使用要領については、別に定める。

（私有携帯電話、私有目的特化型機器及び私有可搬記憶媒体の取扱い）

第３７条　訓令第４５条第１項の規定に基づき、職員は、私有携帯電話、私有目的特化型機器及び私有可搬記憶媒体を防衛省の情報システムで使用してはならない。

２　訓令第４５条第２項の規定に基づき、職員は、私有携帯電話、私有目的特化型機器及び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。

（電子計算機、目的特化型機器及び可搬記憶媒体の持込・使用要領）

第３８条　職場への電子計算機、目的特化型機器及び可搬記憶媒体の持込み及び使用要領については、別に定める。

第７章　教育及び訓練

（教育及び訓練）

第３９条　訓令第４６条第１項の規定により定められた基本方針に基づき実施する情報保証に関する教育及び訓練については、次による。

（１）情報保証責任者補助者は、情報保証全般に関する教育資料を作成し、部長等へ配付するものとする。

（２）情報保証責任者補助者は、前号の資料に基づき教育及び訓練を定期的に実施するものとする。

（３）部長等は、職員に対し、第１号の資料に基づく教育及び訓練を計画的に実施し、又は前号の教育及び訓練に参加させるものとする。

（４）部長等は、前号によるほか、情報保証に必要な知識の習得及び意識の高揚を図るため、必要の都度、職員の職務等を考慮した教育及び訓練を行うものとする。

（５）情報システム情報保証責任者は、情報システム情報保証責任者補助者及びシステム利用者に対し、情報システムの特性に応じた教育及び訓練を計画的に実施するものとする。

２　前項の教育及び訓練を実施した場合は、別に定める要領により記録するものとする。

３　情報保証責任者補助者は、情報本部における情報保証に関する高度な知識及び技能を有する人材育成計画について部長等と協議し、必要な措置を講ずるものとする。

第８章　サイバー攻撃等への対処

（サイバー攻撃等対処要領）

第４０条　訓令第４７条第１項の規定に基づくサイバー攻撃等対処要領については、別に定める。

第９章　対策の実施状況の確認等

（自己点検）

第４１条　訓令第５１条第１項の規定により定められた基本方針に基づき、情報保証責任者が実施する自己点検の細部については、別に定める。

（監査）

第４２条　訓令第５２条第１項の規定により定められた基本方針に基づき、情報保証監査責任者が実施する監査の区分は、次のとおりとする。

（１）定期監査

（２）臨時監査

２　訓令第５２条第２項の規定に基づき、情報保証監査責任者は、運用承認結果報告書及びリスク分析・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毎年度作成する。

３　情報保証監査責任者は、前項で作成した監査実施計画書及び自己点検の結果等に基づき、訓令及び訓令に基づき定められた規則の遵守状況の確認等を目的として、毎年度定期監査を実施する。

なお、定期監査の要領については、別に定める。

４　情報保証監査責任者は、情報保証に関する問題点等を考慮の上、必要に応じて臨時監査を行うものとする。

なお、臨時監査の実施計画、監査対象等の細部については、その都度、情報保証監査責任者が別に示す。

５　訓令第５２条第６項の規定に基づき、情報保証監査責任者は、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、情報保証責任者へ報告の上、情報保証監査統括責任者に提出するものとする。

（特別監査）

第４３条　訓令第５３条の規定に基づき、情報保証監査統括責任者が実施する特別監査については、その都度、別に示す。

（職員による報告等）

第４４条　訓令第５４条の規定に基づき、職員は、訓令及び訓令に基づき定められた規則に関する違反が発生し、又は発生するおそれがあると認められる場合は、直ちに部等情報保証担当者に通報するものとする。

２　部等情報保証担当者は、通報内容を確認し、部長等へ報告するとともに、部長等の判断により、情報保証責任者補助者へ通報するものとする。

３　情報保証責任者補助者は、前項の通報があった場合、直ちに調査を実施し、事案対処責任者及び情報保証責任者に報告するものとする。

第１０章　雑則

第４５条　この達の実施に関し必要な事項については、別に定める。

第４６条　本達は、情報保証に関する新たな対策等を講ずる必要が生じた場合には、随時、実効性の再評価及び見直しを行うものとする。

附　則

１　この達は、平成２０年１月１日から実施する。

２　訓令附則第３項から第５項の規定により整備されていない機能等に関する事項は、その整備後から適用する。

附　則（第１次改正）

この達は、平成２１年２月１日から施行する。

附　則（第２次改正）

この達は、平成２１年１１月２４日から施行する。

附　則（第３次改正）

この達は、平成２４年１月１日から施行する。

附　則（第４次改正）

この達は、平成２４年４月１日から施行する。

附　則（第５次改正）

この達は、平成２６年７月１日から施行する。

附　則（第６次改正）

この達は、平成２６年１２月１０日から施行する。

附　則（第７次改正）

この達は、平成２９年１２月１日から施行する。

附　則（第８次改正）

この達は、平成３０年３月２９日から施行する。

附　則（第９次改正）

この達は、令和４年７月１日から施行する。

附　則（第１０次改正）

１　この達は、令和５年７月１日から施行する。

２　この達の施行の際、現に運用を開始している情報システムについて、訓令別表第３の左欄に掲げる場合に該当する場合は、第１７条の規定に基づく運用承認を受けるものとする。ただし、これらの場合に該当しない場合であっても、第１７条の規定に基づき、令和９年度末までに運用承認を受けるものとする。

３　この達の施行の際、現に設計が終了している情報システムの運用承認については、なお従前の例による。ただし、令和９年度末までに、第１７条の規定に基づく運用承認を受けるものとする。

４　前２項の情報システムについて、情報保証責任者は、やむを得ない理由により令和９年度末までに第１７条の規定に基づく運用承認を行うことができない場合には、運用承認を行うことができない理由及び運用承認を受ける期限について、令和９年度末までに情報保証統括責任者と協議の上、防衛大臣に報告するものとする。