自衛隊統合達第７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）の規定に基づき、統合幕僚監部及び自衛隊サイバー防衛隊の情報保証に関する達を次のように定める。

令和５年７月１日

統合幕僚長　陸将　吉田　圭秀

統合幕僚監部及び自衛隊サイバー防衛隊の情報保証に関する達

統合幕僚監部及び自衛隊サイバー防衛隊の情報保証に関する達（平成２０年自衛隊統合達第２３号）の全部を改正する。

目次

第１章　総則

（目的）

第１条　この達は、統合幕僚監部、統合幕僚学校及び自衛隊サイバー防衛隊（以下「統合幕僚監部等」という。）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、もって統合幕僚監部等における情報保証を確保することを目的とする。

（用語の定義）

第２条　この達において用いる用語の意義は、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、当該各号に定めるところによる。

(1)　通達　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）をいう。

(2)　セキュリティ情報　サイバー攻撃等及びサイバー攻撃等の対応策に関する情報をいう。

(3)　情報システム室　外部からの侵入が容易にできないよう外壁等に囲まれた、情報システムを設置する区域をいう。

(4)　仕様書等　情報システムの仕様書、ネットワーク構成図、システム設計書、基本設計書（概要設計書等を含む。）及び詳細設計書等並びにこれらを記録した記録媒体をいう。

(5)　各課等　統合幕僚監部等における課、首席参事官、参事官、報道官、首席法務官若しくは首席後方補給官、統合幕僚学校企画室若しくは統合幕僚学校国際平和協力センター又は自衛隊サイバー防衛隊本部若しくは当該　部隊の隷下各部隊等をいう。

（適用範囲）

第３条　統合幕僚監部等において、この達の適用を受ける情報システムは統合幕僚監部等で整備する情報システムのほか、各課等で使用する情報システムとする。

２　訓令第３条に規定される適用除外とするものについては別に定める。

第２章　組織及び体制

（指揮通信システム部長の責務）

第４条　統合幕僚監部指揮通信システム部長（以下「指揮通信システム部長」という。）は、情報保証責任者を補佐するものとする。

（情報保証監査責任者）

第５条　訓令第６条の２に基づく統合幕僚監部等における情報保証監査責任者は自衛隊サイバー防衛隊司令をもって充てる。

（情報システム情報保証責任者）

第６条　訓令第７条に基づく統合幕僚監部等における情報システムの情報システム情報保証責任者は、整備段階で責任を有する情報システム情報保証責任者（整備）と運用段階で責任を有する情報システム情報保証責任者（運用）に区分する。

２　情報システム情報保証責任者（整備）及び情報システム情報保証責任者（運用）はそれぞれ情報システムの整備を計画する各課等の長及び情報システムを運用する各課等の長を基準とし、別に定める者とする。

３　情報システム情報保証責任者（運用）は、情報システム運用者の要請及び情報システムの運用上の必要性に従い、必要な措置を行うものとする。

４　情報システム情報保証責任者（運用）は前項の措置を行うに際して、情報システム運用者に対し、必要な協力を求めることができる。

（部隊等情報保証責任者等）

第７条　訓令第８条に基づく統合幕僚監部等における部隊等情報保証責任者は別に定める。

２　部隊等情報保証責任者は、訓令第８条に規定する事務のほか、各課等における情報システムの管理及びシステム利用者の監督を実施し、情報保証の確保に当たるものとする。

３　部隊等情報保証責任者が補助者を指定するに当たっては、当該補助者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の考慮を行うものとする。

４　部隊等情報保証責任者の職務上の上級者は、部隊等情報保証責任者が、不在のため、その職務を行うことができないと認めるときは、臨時にその職務を代行する職員を指定することができる。

（情報システム運用者）

第８条　訓令第９条第１項に定める情報システム運用者は、情報システム情報保証責任者（整備）が情報システムの運用上の特性を考慮した上で指定する。

２　情報システム運用者は、訓令第９条第１項に規定する業務のほか、情報システムの運用及び維持管理に係る実務を行い、必要な事項について情報システム情報保証責任者（運用）に要請する。

３　情報システム情報保証責任者（運用）は、情報システム運用者が情報システムの運用及び維持管理の実務を行うに当たり、実施すべき業務の区分を規定し、必要に応じて情報システム運用者に業務の一部を統制させるものとする。

４　情報システム運用者は、前項の業務区分に従い、運用及び維持管理の実務を実施し、必要に応じて細部の要領を定めるものとする。

（情報システム利用者）

第９条　情報システムにアクセスしてそれを利用できる者として指定された職員（以下「情報システム利用者」という。）は、情報システムの利用に当たり、部隊等情報保証責任者の指導監督に従い、情報保証の確保に努めるものとする。

（情報システム情報保証認証者）

第１０条　訓令第９条第２項に基づく統合幕僚監部等における情報システムの情報システム情報保証認証者は、指揮通信システム部長をもって充てる。

（事案対処責任者）

第１１条　訓令第１１条の規定に基づく統合幕僚監部等における事案対処責任者は、自衛隊サイバー防衛隊司令をもって充てる。

２　事案対処責任者は、情報システム情報保証責任者（運用）が実施するサイバー攻撃等の未然防止及び対処に関し、必要な統制及び技術支援を行うものとする。

３　事案対処責任者が実施する業務を補佐するため、事案対処責任者補助者を置く。

４　事案対処責任者補助者は、事案対処責任者の指定する者をもって充てる。

（情報保証対策委員）

第１２条　訓令第１２条第２項の規定に基づく防衛省の情報保証対策委員会の委員は、統合幕僚監部指揮通信システム部指揮通信システム企画課長をもって充てる。

（統合幕僚監部情報保証対策委員会）

第１３条　統合幕僚監部等の情報保証に関して統合幕僚監部等内相互の調整、連絡及び技術的事項の検討並びにこの達の見直しの審議を行うため、統合幕僚監部情報保証対策委員会（以下「統幕委員会」という。）を置く。

２　統幕委員会は、委員長及び委員で構成する。

３　委員長は、指揮通信システム部長をもって充てる。

４　委員は、統合幕僚監部の部隊等情報保証責任者等、統合幕僚学校長の指定する者、自衛隊サイバー防衛隊司令の指定する者及びその他委員長が必要と認める者とする。

５　委員長は、関係のある統合幕僚監部職員、統合幕僚学校職員及び自衛隊サイバー防衛隊員に対し、資料の提出、意見の開陳、説明その他必要な協力を求めることができる。

６　委員長は、統幕委員会の議事内容を情報保証責任者に報告するものとする。

７　統幕委員会の庶務は、統合幕僚監部指揮通信システム部指揮通信システム企画課において処理する。

第３章　統合幕僚監部等の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

（情報システムの整備に当たっての対策）

第１４条　情報システム情報保証責任者（整備）は、訓令第１３条から第１９条まで及び通達第３第１項から第７項までの規定に基づき、情報システムの特性を考慮し、情報システムに対し、認証機能、アクセス制御機能、証跡管理機能、暗号化機能、電子署名機能、脆弱性対応のための機能等、情報システムの特性に応じた機能等を設けるものとする。

（情報システムの動作確認等）

第１５条　情報システム情報保証責任者（整備）は、情報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、検証システム等を活用し、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、正当なライセンスを有するものであること、及びスパイウェア等でないことをあらかじめ確認するものとする。

（情報システム間の接続）

第１６条　情報システム情報保証責任者（整備）は、訓令第２１条及び通達第３第９項の規定に基づき、ほかの情報システム又はネットワークと接続する場合、事前に訓令第２６条に規定する運用承認を受けるものとする。

２　前項の場合、当該情報システムは接続する情報システム又はネットワークを把握し、ネットワーク構成に係る文書に反映させなければならない。

３　前２項に規定する場合を除き、ほかの情報システム又はネットワークに対して臨時に接続する必要が生じた際は、別紙様式第１に示す情報システム間の接続申請書により、情報保証責任者に申請し、承認を受けなければならない。

４　情報保証監査及び事案対処において使用する情報システムを対象となる情報システム又はネットワークと接続する場合には、前項の規定は適用せず、情報保証監査責任者及び事案対処責任者が定めるところによるものとする。

（外部サービスの利用）

第１７条　情報システム情報保証責任者（整備）は、外部サービスの利用において防衛省の電子計算機情報を取り扱う場合には、外部サービスを利用する情報システム全体として、訓令第２６条、第２７条の２及び第５３条の規定を適用するものとする。

２　情報システム情報保証責任者（整備）は、外部サービスを調達する際、必要なセキュリティ管理策及び情報保証の監査への対応を仕様として示すものとする。

（情報システムの設置場所）

第１８条　情報システム情報保証責任者（整備）及び情報システム情報保証責

任者（運用）（以下「情報システム情報保証責任者（整備・運用）」という。）は、情報保証を確保するために必要がある場合、情報システム室に情報システムの全部又は一部を設置するものとする。

２　情報システム情報保証責任者（運用）は、ハブのポート等のネットワークの接続口及び通信回線を設置する場合、必要に応じ、床下に配線する等その設置場所を秘匿し、部外者に容易に発見できない場所に設置する。

（情報システムの部外への設置）

第１９条　情報システム情報保証責任者（運用）は、情報システムの一部又は全部を部外に設置する場合、情報システムが取り扱う電子計算機情報の秘密区分等に応じ、部外設置場所と防衛省の管理する区域との施設間の通信回線秘匿及び部外設置場所における保全を確保した上で、別紙様式第２により、情報保証責任者の承認を得るものとする。

第２節　運用承認

（運用承認）

第２０条　情報システム情報保証責任者（整備）は訓令別表第３に掲げる場合、情報システムの運用承認を受けなければならないものとし、細部要領については別に定める。

（運用承認時に関する通知）

第２１条　情報システム情報保証責任者（整備）は、運用承認の通知を受けたときは、速やかに事案対処責任者に情報システムの構成に関する情報を通知するものとする。

第３節　情報システムの運用、管理に当たっての対策

（リスク分析・評価）

第２２条　情報システム情報保証責任者（運用）及び情報システム情報保証認証者は、訓令第２７条の２に基づき、毎年度１回以上リスク分析・評価を実施するものとし、細部要領については別に定める。

（利用者の登録及び認証情報の管理）

第２３条　情報システム情報保証責任者（運用）は、情報システム利用者を定め、当該情報システム利用者にユーザ名及び認証情報を付与するとともに、必要に応じこれらを記録したＩＣカードその他の媒体を付与するものとする。

２　情報システム情報保証責任者（運用）は、情報システム利用申請手続を定め、情報システム利用者の登録、変更、抹消等を適切に実施するほか、ＩＣカードその他の媒体の管理要領を定め、情報システム利用者に適切な管理を実施させるものとする。

３　情報システム利用者は、付与されたＩＣカード及びその他の媒体を適切に管理するとともに、認証情報等が不正に使用され、又はその恐れがあると認

めたときは、直ちに情報システム情報保証責任者（運用）に通報するものとする。

（アクセス制御）

第２４条　情報システム情報保証責任者（整備）は、必要に応じ電子計算機情報の利用を制限できるよう情報システムにアクセス制御機能を付加する。

２　情報システム情報保証責任者（運用）は、電子計算機情報の利用を制限すべきものについてアクセス制御を実施する。

３　情報システムにおいて、ネットワークの構成にＶＰＮ（ネットワーク上に仮想的な専用ネットワークを設ける技術をいう。）、無線ＬＡＮ又は公衆電話網を経由したリモートアクセス機能を使用する必要がある場合は、通達第３第７項第１号の規定により、それらによりアクセスする通信回線の範囲を限定し、制限された情報システム利用者以外からの接続ができない措置を講じるとともに、情報保証責任者の許可を得るものとする。

４　情報システム情報保証責任者（運用）は、情報システムに対して部外からアクセスする必要がある場合は、通達第５第３項第１号に規定される事項を遵守した上で、情報保証責任者の許可を得るものとする。

（証跡管理）

第２５条　情報システム情報保証責任者（運用）は、証跡管理機能を設けた場合、証跡を適切に取得するものとする。

２　証跡は、情報システム内に保存し、必要に応じ情報システム情報保証責任者（運用）又はその指定する者のみが利用できるものとし、その保存期間は、情報システム情報保証責任者（運用）が定めるものとする。

３　情報システム情報保証責任者（運用）は、必要に応じて証跡を分析するものとする。

（暗号化）

第２６条　情報システム情報保証責任者（運用）は、暗号化機能を設けた場合、情報システムで取り扱われる電子計算機情報を可搬記憶媒体に格納し、又は送信するに当たり当該機能が実効できるよう運用しなければならない。

２　情報システム利用者は、取り扱う防衛省の電子計算機情報のうち、可搬記憶媒体に保存し、又はネットワークを介して送信するに当たり、暗号化すべきものについては、情報システムに設けられた暗号化機能により暗号化を行うものとする。

（電子署名）

第２７条　情報システム情報保証責任者（運用）は、電子署名機能を設けた場合、必要に応じて電子署名を付すことができるよう設定し、電子署名の検証を行う者に対し電子署名の正当性を検証するための情報又は手段を提供しな

ければならない。

２　情報システム利用者は、取り扱われるデータの作成者の真正性を特に確保するとともに、当該データの改ざんを特に防止すべきものについては、情報システムに設けられた電子署名機能により電子署名を行うものとする。

（脆弱性対応）

第２８条　情報システム情報保証責任者（運用）は、情報システムの脆弱性対応が有効に行われるよう、次の各号に掲げる措置を行うものとする。

(1)　情報システムで使用するハードウェア及びソフトウェアについて、新たな脆弱性に関する情報を収集するとともに、脆弱性への対応が十分に行われているかについて定期的に確認を行うこと。

(2)　前号の結果、情報システムで使用するハードウェア及びソフトウェアについて新たな脆弱性が判明し、又は脆弱性への対応が不十分であることが判明した場合には、当該脆弱性が情報システムに与える影響を分析の上、当該脆弱性への対応を適切な手段により計画的に行うこと。

(3)　ウイルス対策ソフトによるコンピュータ・ウイルス等の検索を行うこと等により、コンピュータ・ウイルス等の感染の有無を定期的に確認すること。

(4)　ウイルス対策ソフトの更新等、新たなコンピュータ・ウイルス等への対応を行うこと。

(5)　ハードウェア及びソフトウェアの脆弱性に関する情報、コンピュータ・ウイルス等に関する情報等を必要に応じほかの情報システム情報保証責任者（整備・運用）等と共有すること。

(6)　その他情報システムの特性に応じ必要な対応を行うこと。

２　情報システム利用者は、脆弱性に対応するため、情報システムに設けられたウイルス対策ソフトを有効に活用し、不審なファイルを実行しないこと等により、コンピュータ・ウイルス等への感染防止に努めるとともに、情報システム情報保証責任者（運用）が定める事項に従わなければならない。

（情報システム室の入退室管理）

第２９条　情報システム情報保証責任者（運用）は、情報システム室への入室を許可した者だけに限定する等、入退室管理を適切に実施するものとする。

２　情報システム情報保証責任者（運用）は、必要に応じ、開閉制御装置、開放防止装置等により入退室を管理し、情報システム室の入退出の記録、身分証明書等の装着その他の入退室管理に必要な措置を講じるものとする。

３　情報システム情報保証責任者（運用）は、情報システムの搬入、設置、保守、維持整備等を部外の者に実施させる場合、情報システム室の入退室に当たり、情報システム情報保証責任者（運用）が指定する者を同行させる等の措置を講じるものとする。

（情報システムの管理）

第３０条　情報システム利用者は、情報システムの盗難を防止するため、情報システムを設置している事務室等を関係職員が不在にする場合、事務室等に施錠するものとする。

２　部隊等情報保証責任者は、情報システムの盗難を防止し、管理の適正化を図るため、端末情報、システム利用者等を記載した別紙様式第３に示す情報システム管理簿を設け、常に最新の状態に保たなければならない。

３　職員は、情報システムを一時的に省外に持ち出す場合には、別紙様式第４に示す情報システム持出簿により、情報システム情報保証責任者（運用）の許可を受けるものとする。また、携行を前提とする情報システムを省外へ持ち出す場合の持ち出し期間の標準は、情報システム情報保証責任者（運用）が定めるものとする。

４　省外に持ち出した情報システムを返却する場合、ウイルスの駆除等を確実に実施するものとし、情報システム情報保証責任者（運用）は、情報システム持出簿（「ウイルスチェック結果」欄）により、実施結果を確認するものとする。

（情報システムの変更）

第３１条　情報システムの配線変更、改造、機器の増設、交換、ソフトウェアの変更等、情報システムの形態を変更する場合は、情報システム情報保証責任者（整備）の許可を得るものとする。

２　情報システム情報保証責任者（整備）は、情報システムの形態に変更が生じた場合は、形態管理の記録を作成し、適切に情報システムの形態管理を実施するものとする。

３　情報システム情報保証責任者（整備）は、情報システムの構成を変更し、新たにほかの情報システムと接続する場合又は当該接続形態を変更する場合は、当該接続する情報システムの情報システム情報保証責任者（整備）と接続に関する協議を実施し、情報保証上の支障が生じないよう必要な措置を講ずるとともに、再度運用承認を得なければならない。

（情報システムに関する文書の整備等）

第３２条　情報システム情報保証責任者（整備）は、情報システムの仕様書等を当該情報システムの廃棄時まで保管するものとする。

２　情報システム情報保証責任者（運用）は、必要に応じ、機器の設置場所や使用者名等を記載した文書を整備する等により、情報システムの構成を適切に管理するものとする。

３　情報システム情報保証責任者（運用）は、情報システムの利用及び管理に関する規則を定め、必要な事項を情報システム利用者に徹底しなければならな

い。
４　情報システム利用者は、情報システム情報保証責任者（運用）が定める規則に基づき、情報システムの利用及び管理を適切に行わなければならない。
（職員以外の情報システムの利用）
第３３条　情報システム情報保証責任者（運用）は、防衛省職員以外の者に情報システムを利用（保守整備作業を含む。）させる場合は、情報システム利用者が守るべき事項を当該職員以外の者に理解させるとともに、遵守させるために関係職員を立会いさせる等の処置を行うものとする。
２　情報システム情報保証責任者（運用）は、防衛省職員以外の者に情報システムを利用させる場合は、別紙様式第５に示す情報システム部外者利用記録簿に記録するものとする。ただし、情報システム情報保証責任者（運用）が業務の遂行上、恒常的に利用する必要を認める者を除く。
（情報システムの障害発生時の措置等）
第３４条　情報システム情報保証責任者（運用）は、情報システムに障害が発生した場合には、速やかに復旧させるための措置を講ずるとともに、原因究明のためのログの収集整理及び障害記録を作成するものとする。
２　情報システム情報保証責任者（運用）及びその指名する者は、必要に応じ障害記録を障害状況の分析や必要な対策等に活用することとし、その保存要領及び期間については、情報システム情報保証責任者（運用）が定めるものとする。
３　情報システム情報保証責任者（運用）は、ほかの情報システムと接続した情報システムの障害で、接続した情報システムに影響を及ぼす又はその恐れがある場合には、情報保証責任者に報告するとともに、関係する情報システム情報保証責任者（運用）に通報し、必要があればほかの情報システムとの接続を障害復旧までの間、切断することができる。
４　情報システム情報保証責任者（運用）は、情報システム障害時に情報システムを障害発生前の状態に復元させるため、情報システムの電子計算機情報を１週間に１度を基準に複製するものとする。
５　情報システム利用者は、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、保存するよう努めなければならない。
（情報システムの特性に応じた対策等）
第３５条　情報システム情報保証責任者（運用）は、この達に定めるもののほか、情報システムの特性に応じ、情報保証を確保するために必要な対策を行うものとする。
２　情報システム情報保証責任者（運用）は、前項に基づき実施した対策について、必要に応じ見直しを行うものとする。

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３６条　情報システム情報保証責任者（運用）は、電子計算機情報を扱う情報システムの全部又は一部を廃棄、返却、修理等のため、部外の事業者に受け渡す場合は、記録装置内の電子計算機情報を物理的な破壊又は消去プログラム等を活用し、情報システムに保存された電子計算機情報を復元不可能な状態にした上で受け渡しを実施するものとする。ただし、情報システムの動作確認等のためにプログラムを残置する必要がある場合は、データのみの消去とすることができる。

２　電子計算機情報の消去方法については、秘密保全に関する訓令等の解釈及び運用について（通達）（防防調第４６０７号。１９．４．２７）別紙第３第２項第１４及び特定秘密の保護に関する訓令の運用について（通達）（防防調第１７８８２号。２６．１２．８）別紙中第１８により実施するものとする。

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）

第３７条　部隊等情報保証責任者は、訓令第４２条の２及び通達第７第１号の規定に基づき、統合幕僚監部等の目的特化型機器の管理について、別紙様式第６に示す目的特化型機器管理簿を作成し管理するものとする。

２　部隊等情報保証責任者は、統合幕僚監部等の目的特化型機器について、取り扱う情報、利用方法、通信回線への接続形態等当該機器の特性に応じた対策を講ずるものとする。

３　部隊等情報保証責任者は、目的特化型機器の全部又は一部の廃棄等においては前条の規定を準用する。

４　部隊等情報保証責任者は、目的特化型機器の保管状況について月１回以上点検し、別紙様式第７に示す目的特化型機器点検簿に記録するものとする。

第５章　可搬記憶媒体に係る対策

（可搬記憶媒体の管理）

第３８条　部隊等情報保証責任者は、訓令第４３条及び通達第８第１号の規定に基づき、統合幕僚監部等の可搬記憶媒体について、別紙様式第８に示す可搬記憶媒体管理簿を設け、集中保管を行わなければならない。ただし、集中保管が困難な場合、部隊等情報保証責任者は、班室等保管単位ごとに、部隊等情報保証責任者補助者を指定するものとする。

２　秘密及び指定前秘密を保存する場合は秘密保全に関する達（平成２０年自衛隊統合達第１６号）、特定秘密を保存する場合は特定秘密の保護に関する達（平成２６年自衛隊統合達第１７号）によるものとする。

３　職員は、可搬記憶媒体を使用するため保管容器から持ち出す場合には、そ

の都度、別紙様式第９に示す可搬記憶媒体使用記録簿に記録しなければならない。ただし、第５項に示す職場から持ち出す場合を除く。

なお、部隊等情報保証責任者又は部隊等情報保証責任者補助者は、可搬記憶媒体の使用状況について、原則１日１回確認を実施するものとする。

４　職員は、可搬記憶媒体を使用する場合には、情報保証上の安全性を確認した上で使用しなければならない。

５　職員は、可搬記憶媒体を職場から持ち出す必要のある場合には、別紙様式第１０に示す可搬記憶媒体持出簿により、部隊等情報保証責任者の許可を受けなければならない。

６　職場から持ち出した可搬記憶媒体を返却する場合、ウイルスの駆除等を確実に実施するものとし、部隊等情報保証責任者は、第５項の可搬記憶媒体持出簿（「ウイルスチェック結果」欄）により、実施結果を確認するものとする。

７　通達第８第７号が示す区域とは、防衛省が管理する区域のうち、当該部隊等が所在する区域と定め、この区域内において、可搬記憶媒体を持ち出す場合には、第３項に示す記録をもって足りる。

８　部隊等情報保証責任者は、可搬記憶媒体の保管状況について月１回以上点検し、別紙様式第１１に示す可搬記憶媒体点検簿に記録するものとする。

第６章　私有機器の取扱い

（私有機器の取扱い）

第３９条　職員は、訓令第４４条及び第４５条の規定に基づき、私有パソコンの職場への持ち込み、並びに防衛省の情報システムにおいて私有携帯電話、私有目的特化型機器及び私有可搬記憶媒体の使用を行ってはならない。

２　職員は、私有機器で業務用データを取り扱ってはならない。

第７章　教育及び訓練

（教育及び訓練）

第４０条　事案対処責任者、情報システム情報保証責任者（運用）及び部隊等情報保証責任者は、職員に対し、被教育者の職務及び情報システムの特性を考慮し、情報保証の重要性を認識させるため、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　情報保証教育の実施について、情報システム情報保証責任者（運用）は情報システムの運用、操作要領に係る教育を所掌し、部隊等情報保証責任者は情報保証規則に基づく教育を所掌するものとする。

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の策定）

第４１条　訓令第４７条の規定に基づき、統合幕僚監部等におけるサイバー攻撃等対処要領は、別に定める。

（セキュリティ情報の収集）

第４２条　事案対処責任者は、セキュリティ情報を継続的に収集・分析し、必要に応じ、情報システム情報保証責任者（運用）に連絡するものとする。

２　事案対処責任者は、収集・分析したセキュリティ情報の内、情報システムに重大な影響を及ぼす恐れのあるセキュリティ情報については、速やかに情報保証責任者に報告するとともに、通達第１１第２項により、関係する機関に連絡し、情報共有するものとする。

３　情報システム情報保証責任者（運用）は、当該情報システムに関連するセキュリティ情報を常に把握し、必要に応じ当該情報システムを使用する職員に周知徹底するものとし、当該情報システムに重大な影響を及ぼす恐れのあるセキュリティ情報については、情報保証責任者に報告するとともに、事案対処責任者に連絡するものとする。

第９章　対策の実施状況の確認等

（自己点検）

第４３条　職員、部隊等情報保証責任者及び情報システム情報保証責任者（運用）は、訓令及びこの達の遵守状況について、毎年度１回、自己点検を実施するものとし、細部要領は別に定める。

２　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する。

（監査）

第４４条　情報保証監査責任者は、訓令第５２条の規定により、別に示される監査の基本方針に基づき、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、監査を行うほか、訓令第５３条の規定に基づく特別監査を行うものとし、監査の実施要領については別に定める。

（職員による報告等）

第４５条　第４２条から前条までに定めるもののほか、職員は、訓令及びこの達に関し違反が発生し、又は発生した恐れがあると認める場合には、直ちに情報システム情報保証責任者（運用）に報告するものとする。

２　情報システム情報保証責任者（運用）は、訓令及びこの達に関する違反が発生し、当該違反が情報保証上重大な影響を及ぼす可能性があると判断した場合は、情報保証責任者に報告するものとする。

３　通達別紙の規定に基づき、インターネット上への情報流出を把握した場合の対応の細部については、別に定める。

第１０章　雑則

（委任規定）

第４６条　この達の実施に関し必要な事項は、情報システム情報保証責任者（整

備・運用）が別に定める。

附　則

この達は令和５年７月１日から施行する。

別紙様式第１（第１６条関連）

情報システム間の接続申請書

情報システム名		
情報システム情報保証責任者（運用）		
情報システムで扱う電子計算機情報の 秘密取扱いの最高区分		特定秘密・秘・注意・区分なし
利用者の秘密取扱い区分の最低区分		特定秘密・秘・注意・区分なし
情報システムの区分		機密性：高・中・低 可用性：高・中・低 完全性：高・中・低
使用部課等		
接続先	情報システム名	
	情報システム情報保証責任者	
	扱う情報の最高の秘密区分	特定秘密・秘・注意・区分なし
	システム利用者の秘密取扱い 区分の最低区分	特定秘密・秘・注意・区分なし
	情報システムの区分	機密性：高・中・低 可用性：高・中・低 完全性：高・中・低
	使用部課等	
接続する理由		
接続に関する保全措置等		

別紙様式第２（第１９条関連）

情報システムの部外設置申請書

情報システム名	
情報システム情報保証責任者	
情報システムで扱う電子計算機情報の秘密取扱いの最高区分	特定秘密・秘・注意・区分なし
利用者の秘密取扱い区分の最低区分	特定秘密・秘・注意・区分なし
情報システムの区分	機密性：高・中・低 可用性：高・中・低 完全性：高・中・低
部外に設置する目的	
設置場所　注１	
期間　注２	
部外に設置する機器の構成等	
部外に設置する機器において扱う電子計算機情報の秘密取扱いの最高区分	特定秘密・秘・注意・区分なし
部外に設置する機器の管理要領及び保全措置　注３	

注：１　設置場所は、利用者により管理できるか、又は契約により契約相手方が確実に管理できる場所であること。

２　期間は必要最小限とすること。

３　部外に設置する機器の管理要領及び保全措置について、情報システム情報保証責任者（運用）が細部を定めること。また、適切に管理されていることを定期的にあるいは随時に確認を実施すること。

別紙様式第３（第３０条関連）

情報システム管理簿

（情報システム名）

登録番号	端末名称（型式）	使用者	設置場所	登録		解除		備考
		所属 階級 氏名		年月日	部隊等情報保証責任者確認欄	年月日	部隊等情報保証責任者確認欄	

注：１　登録番号は、班室略称名－情報システム名－班室内の一連番号とする。
　　２　端末名称（型式）は、情報システムの形式とする。
　　３　使用者、設置場所、登録年月日は登録時に記載する。
　　４　部隊等情報保証責任者確認欄は、部隊等情報保証責任者が確認したことを自署又はその他、部隊等情報保証責任者が確認したことを明示する手段により記載するものとする。
　　５　解除年月日は、業務用データが全て消去されていることを確認した後に記載する。

別紙様式第４（第３０条関連）

情報システム持出簿

（情報システム名）

登録番号 （端末名称）	持出者	持出					返却		
	所属 階級 氏名	期間	用途	通常設置場所	持出先	情報システム情報保証責任者確認欄	年月日	返却確認 （ウイルスチェック結果）	情報システム情報保証責任者確認欄

注：　情報システム情報保証責任者確認欄は、情報システム情報保証責任者（運用）が確認したことを自署又はその他、情報システム情報保証責任者（運用）が確認したことを明示する手段により記載するものとする。

別紙様式第５（第３３条関連）

情報システム部外者利用記録簿

（情報システム名）

登録番号 （端末名称）	利用開始日時	用途	利用者 所属　氏名	利用終了日時	立会者 所属　階級　氏名	情報ｼｽﾃﾑ情報保証 責任者確認欄	備考

注：　情報システム情報保証責任者確認欄は、情報システム情報保証責任者（運用）が確認したことを自署又はその他、情報システム情報保証責任者（運用）が確認したことを明示する手段により記載するものとする。

別紙様式第６（第３７条関連）

目的特化型機器管理簿

目的特化型機器登録番号	機器の種類	機器の型番等	設置場所	登録		登録解除		備考
				年月日	部隊等情報保証責任者確認欄	年月日	部隊等情報保証責任者確認欄	

注：１　登録番号は「班室略称名－目的－一連番号」により記載する。
　　２　部隊等情報保証責任者確認欄は、部隊等情報保証責任者が確認したことを自署又はその他、部隊等情報保証責任者が確認したことを明示する手段により記載するものとする。

別紙様式第７（第３７条関連）

目的特化型機器点検簿

年月日	点検結果	部隊等情報保証 責任者確認欄	備考	年月日	点検結果	部隊等情報保証 責任者確認欄	備考

注：１　部隊等情報保証責任者確認欄は、部隊等情報保証責任者が確認したことを自署又はその他、部隊等情報保証責任者が確認したことを明示する手段により記載するものとする。

２　備考には点検を受ける目的特化型機器について種類ごとの数を記載するものとする。

別紙様式第８（第３８条関連）

可搬記憶媒体管理簿

登録番号	媒体の種類	保管場所	登録		登録解除		備考
			年月日	部隊等情報保証責任者確認欄	年月日	部隊等情報保証責任者確認欄	

注：１　登録番号は「班室略称名－可搬－一連番号」により記載する。
２　送達の場合は、不必要な業務用データが保存されていないことを確認する等、業務用データが外部に流出することを防止するための措置を実施したことを確認した後、備考欄に、送達年月日、送達先を記載し、登録解除する。
３　送達票の様式については別に定める。
４　部隊等情報保証責任者確認欄は、部隊等情報保証責任者が確認したことを自署又はその他、部隊等情報保証責任者が確認したことを明示する手段により記載するものとする。

別紙様式第９（第３８条関連）

可搬記憶媒体使用記録簿

使用開始日時	登録番号	使用者 所属 階級 氏名	返却日時	部隊等情報保証責任者確認欄	備考

注：　部隊等情報保証責任者確認欄は、部隊等情報保証責任者が確認したことを自署又はその他、部隊等情報保証責任者が確認したことを明示する手段により記載するものとする。

別紙様式第１０（第３８条関連）

可搬記憶媒体持出簿

登録番号	持出者	持出				返却		
	所属 階級 氏名	期間	用途	持出先	部隊等情報保証責任者確認欄	年月日	返却確認（ｳｲﾙｽﾁｪｯｸ結果）	部隊等情報保証責任者確認欄

注：　部隊等情報保証責任者確認欄は、部隊等情報保証責任者が確認したことを自署又はその他、部隊等情報保証責任者が確認したことを明示する手段により記載するものとする。

別紙様式第１１（第３８条関連）

可搬記憶媒体点検簿

年月日	点検結果	部隊等情報保証 責任者確認欄	備考	年月日	点検結果	部隊等情報保証 責任者確認欄	備考

注：１　部隊等情報保証責任者確認欄は、部隊等情報保証責任者が確認したことを自署又はその他、部隊等情報保証責任者が確認したことを明示する手段により記載するものとする。

２　備考には点検を受ける可搬記憶媒体について種類ごとの数を記載するものとする。