防衛省訓令第１６０号

防衛省の情報保証に関する訓令を次のように定める。

平成１９年９月２０日

防衛大臣　高村　正彦

防衛省の情報保証に関する訓令

改正　平成２０年　３月２５日　省訓第１２号

改正　平成２１年　７月２９日　省訓第４８号

改正　平成２６年　４月２５日　省訓第２６号

改正　平成２７年１０月　１日　省訓第３９号

改正　平成２８年　３月３１日　省訓第３４号

改正　令和　４年　３月１６日　省訓第１９号

改正　令和　５年　３月３１日　省訓第２６号

改正　令和　５年　６月２９日　省訓第５６号

防衛省の情報保証に関する訓令（平成１６年防衛庁訓令第２９号）の全部を改正する。

目次

第１章　総則

（目的）

第１条　この訓令は、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する。

（定義）

第２条　この訓令において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) 情報保証　情報システム及び電子計算機情報の機密性（電子計算機情報にアクセスすることを許可された者だけが当該情報にアクセスできることを確実にすることをいう。）、完全性（電子計算機情報及び処理方法が正確及び完全である状態を安全防護する

ことをいう。）、可用性（電子計算機情報にアクセスすることを許可された者が、必要なときに当該情報にアクセスできることを確実にすることをいう。）、識別認証（情報システムを利用する者、情報システムの構成品等の身元の真正性を確認できることを確実にすることをいう。）及び否認防止（情報システムを利用して電子計算機情報の送受信を行った者が当該送受信を行ったことを否定できないことを確実にすることをいう。）を維持することをいう。

(2) 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。

(3) 暗号化　電子計算機情報について、所定の暗号による秘匿措置を講ずることをいう。

(4) 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、可搬記憶媒体でないものをいう。

(5) 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。

(6) サイバー攻撃等　サイバー攻撃（ネットワークを通じた情報システムへの電子的な攻撃をいう。）並びにサイバー攻撃と同様の影響を発生させる情報システムの誤操作及びサイバー攻撃以外によるコンピュータ・ウイルスの混入等をいう。

(7) 電子計算機情報　情報システムにおいて取り扱われるプログラム及びデータをいう。

(8) 電子署名　電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

ア　当該情報が、当該措置を行った者の作成に係るものであることを示すためのものであること。

イ　当該情報について改変が行われていないかどうかを確認することができるものであること。

(9) 職場　防衛省の職員（以下「職員」という。）が通常勤務する執務室等及び部隊に勤務する職員が部隊活動のため通常勤務する執務室等以外の場所で活動する場合の活動場所（営舎、船舶、防衛大学校及び防衛医科大学校に居住する者については、居住する営舎、船舶、防衛大学校及び防衛医科大学校の居住区画を除く。）をいう。

(10) 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。

(11) 外部サービス　部外の者が一般向けに情報システムの全部又は一部の機能を提供するものをいう。

(12) 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　次条に規定する情報保証統括責任者は、他国との取り決めに基づき個別の要件を定める必要がある場合等、この訓令の規定が業務の適正な遂行を著しく妨げるなどの相当の理由があると認めるときは、第６条に規定する情報保証責任者の申請によりこの訓令の規定の一部を適用しないことができる。

第２章　組織及び体制

（情報保証統括責任者）

第４条　防衛省に、情報保証に関する事務を統括し、情報保証に必要な取組を推進する責任者として、情報保証統括責任者を置く。

２　情報保証統括責任者は、整備計画局長をもって充て

る。

（情報保証統括アドバイザー）

第４条の２　情報保証統括責任者は、情報保証統括責任者を補佐する者として、情報保証統括アドバイザーを置くものとする。

（情報保証監査統括責任者）

第５条　防衛省に、情報保証の監査に関する事務を統括する者として、情報保証監査統括責任者を置く。

２　情報保証監査統括責任者は、サイバーセキュリティ・情報化審議官をもって充てる。

（情報保証責任者）

第６条　別表第１の左欄に掲げる機関等（以下「機関等」という。）に、機関等の情報保証に関する事務を監督する者として、情報保証責任者を置く。

２　情報保証責任者は、別表第１の右欄に掲げる者をもって充てる。

（情報保証監査責任者等）

第６条の２　情報保証責任者は、機関等における情報保

証の監査に関する事務を行う者として、情報保証監査責任者を置くものとする。

２　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ことができる。

（情報システム情報保証責任者等）

第７条　情報保証責任者は、防衛省の情報システムについて、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として、防衛省の情報システムごとに、情報システム情報保証責任者を置くものとする。

２　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ことができる。

（部隊等情報保証責任者等）

第８条　情報保証責任者は、部隊等における防衛省の目的特化型機器及び可搬記憶媒体の管理並びに私有パソコン、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（以下「私有機器」という。）での業務用デー

タの取扱いの禁止等第６章に規定する私有機器の取扱いに関する事務を行う者として、別表第２に掲げる単位ごとに、部隊等情報保証責任者を置くものとする。

２　部隊等情報保証責任者は、その補助者として、部隊等情報保証責任者補助者を指定することができる。

３　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等のため、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及び情報システム情報保証認証者等）

第９条　情報保証責任者は、第２６条第２項及び第４項の規定に基づき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として、防衛省の情報システムごとに情報システム運用者を置く。

２　情報保証責任者は、第２６条第２項及び第４項の規

定に基づき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として、防衛省の情報システムごとに情報システム情報保証認証者を置く。

３　情報システム情報保証認証者は、その補助者として、情報システム情報保証認証者補助者を指定することができる。

（事案対処統括責任者）

第１０条　防衛省に、サイバー攻撃等の対処に関する活動を統括する者として、事案対処統括責任者を置く。

２　事案対処統括責任者は、サイバー攻撃等の未然防止及び対処に関し、情報保証責任者及び次条に規定する事案対処責任者を統制する。

３　事案対処統括責任者は、サイバーセキュリティ・情報化審議官をもって充てる。

（事案対処責任者）

第１１条　情報保証責任者は、機関等が定めるところに

従い、当該機関等の情報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、情報システム情報保証責任者を統制し、又は情報システム情報保証責任者に対し技術的支援を行う者として、事案対処責任者を置くものとする。

（情報保証対策委員会）

第１２条　防衛省の情報保証に関して機関等相互間の調整、連絡及び技術的事項の検討並びにこの訓令及びこの訓令の実施に必要な基準等の見直しの審議を行うため、情報保証対策委員会（以下この条において「委員会」という。）を置く。

２　委員会は、委員長並びに情報保証責任者が指定する者及び委員長が必要と認め指定する者をもって構成する。

３　委員長は、整備計画局サイバー整備課長をもって充てる。

４　委員長は、委員会を招集し、会務を総理する。

５　委員長は、関係のある防衛省職員に対し、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　委員会の庶務は、整備計画局サイバー整備課において処理する。

第３章　防衛省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

（認証機能）

第１３条　情報システム情報保証責任者は、情報システムの利用者を制限する必要がある場合には、情報システムに、情報システムの利用者を識別するための情報（以下「ユーザ名」という。）及び当該ユーザ名を付与された者であることを証明する情報（第２８条において「認証情報」という。）を使用して情報システムの利用者が正当な権限を有することを確認する機能（第２８条において「認証機能」という。）を設けなければならない。

（アクセス制御機能）

第１４条　情報システム情報保証責任者は、防衛省の電子計算機情報のうち利用を制限すべきものがある場合には、情報システムに、当該情報へのアクセスを制限する機能（第２９条において「アクセス制御機能」という。）を設けなければならない。

（証跡管理機能）

第１５条　情報システム情報保証責任者は、情報システムの情報保証を確保するため必要がある場合には、情報システムに、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（第３０条において「証跡」という。）を取得する機能（第３０条において「証跡管理機能」という。）を設けなければならない。

（暗号化機能）

第１６条　情報システム情報保証責任者は、防衛省の電子計算機情報のうち可搬記憶媒体に格納し、又は送信するに当たり暗号化すべきものがある場合には、情報システムに、可搬記憶媒体に格納し、又は送信する電子

計算機情報を暗号化することができる機能（第３１条において「暗号化機能」という。）を設けなければならない。

（電子署名機能）

第１７条　情報システム情報保証責任者は、情報システムで取り扱われるデータのうち、当該データの作成者の真正性を特に確保し、及び当該データの改ざんを特に防止すべきものがある場合には、情報システムに、電子署名を付することができる機能（第３２条において「電子署名機能」という。）を設けなければならない。

（脆弱性対応のための機能等）

第１８条　情報システム情報保証責任者は、情報システムが有する脆弱性に対応できるよう、必要な機能を情報システムに設け、又は情報システムの設定を行わなければならない。

（情報システムの特性に応じた機能等）

第１９条　情報システム情報保証責任者は、第１３条から前条まで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措置を講ずるものとする。

２　情報システムを取り扱う上で措置すべきセキュリティ管理策は、情報保証統括責任者が定める。

（情報システムの動作確認等）

第２０条　情報システム情報保証責任者は、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には、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。

（情報システム間の接続）

第２１条　情報システム情報保証責任者は、情報システムを他の情報システム又はネットワークと接続する場合には、情報保証を確保する上で支障がないよう必要な措置を講じなければならない。

２　業務用データを取り扱う情報システムは、次に掲げる場合を除き、他の情報システム又はネットワークと

接続してはならない。

(1) 防衛省が保有し、かつ、部外の者が保有する情報システム又はネットワークと接続されていない情報システムと接続する場合

(2) 他省庁が整備した情報システムと接続する場合

(3) 特別な理由があるとして、当該情報システムを運用する情報保証責任者が防衛大臣の承認を得た場合

（外部サービスの利用）

第２１条の２　情報システム情報保証責任者は、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、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は、外部サービスを調達する際に、セキュリティ管理策の適用及び監査の実施を担保するため、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２２条　情報システム情報保証責任者は、情報保証を確保するため必要がある場合には、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区域（第３４条において「情報システム室」という。）に、情報システムの全部又は一部を設置しなければならない。

２　前項に定めるもののほか、情報システム情報保証責任者は、情報保証を確保するため必要がある場合には、地震、火災その他の災害による影響を可能な限り排除した場所に、情報システムの全部又は一部を設置しなければならない。

３　情報システム情報保証責任者は、情報システムの搬入、設置等を部外の者に行わせる場合には、情報システム情報保証責任者の指定する者を同行させる等の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２３条　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には、情報保証責任者の承認を得なければならない。

（情報システムの調達）

第２４条　防衛省の情報システムの調達について必要な事項は、別に定める。

（情報システムセキュリティ台帳の整備）

第２５条　情報保証統括責任者は、防衛省の情報システムについて、当該情報システムに講ずるセキュリティ管理策の実施状況を把握するため、情報システムセキュリティ台帳を整備するものとする。

２　情報システム情報保証責任者は、情報システムを新たに整備し、又は情報保証上のリスクに変化が生じた場合には、当該情報システムのセキュリティに係る事項について情報保証責任者を通じて情報保証統括責任者に報告するものとする。

第２節　運用承認

（運用承認）

第２６条　情報システム情報保証責任者は、別表第３の左欄に掲げる場合には、同表の右欄に掲げる時期までに、第１３条から第２２条（同条第３項を除く。）まで

の規定に基づく措置の実施内容及び当該措置を実施した上で情報システムを運用することについて、情報保証責任者の承認（以下「運用承認」という。）を受けなければならない。ただし、情報システム情報保証責任者は、別に定める情報システムについては、情報保証責任者の承認を得た場合には、運用承認を要しないものとする。

2　情報システム情報保証責任者は、運用承認を受ける場合には、情報システムのリスクの分析及び評価（以下「リスク分析・評価」という。）の結果を記載した運用承認時リスク評価報告書、当該情報システムに適用するセキュリティ管理策等を記載したセキュリティ計画書及び当該情報システムに適用するセキュリティ管理策が適切に講じられているか監視するための計画を記載した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ものとする。

3　情報システム情報保証認証者は、前項に規定する運用承認時リスク評価報告書、セキュリティ計画書及び

継続監視計画書の提出を受けた場合には、これらを踏まえ、当該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したセキュリティ評価計画書及び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たセキュリティ評価報告書（以下「セキュリティ評価文書」という。）を作成し、情報システム情報保証責任者に提出するものとする。

4　情報システム情報保証責任者は、前項に規定するセキュリティ評価文書の提出を受けた場合には、これを踏まえ、当該情報システムに適用するセキュリティ管理策について必要な改善策を講じていくための計画を記載した将来対応計画書を作成し、情報システム情報保証認証者に提出するものとする。

5　情報システム情報保証責任者は、第２項及び前項の規定に基づき運用承認時リスク評価報告書、セキュリティ計画書、継続監視計画書及び将来対応計画書（以下この条において「運用承認申請文書」という。）を作成

するに当たっては、情報システム運用者の意見を聴かなければならない。

6　情報システム情報保証認証者は、第４項に規定する将来対応計画書の提出を受けた場合には、これを審査し、情報システムを運用することが可能と認める場合には、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するものとする。

7　情報システム情報保証責任者は、前項に規定する認証結果報告書の提出を受けた場合には、運用承認申請文書、セキュリティ評価文書及び認証結果報告書を添えて情報保証責任者に運用承認の申請を行うものとする。

8　情報保証責任者は、前項に規定する運用承認の申請を受けた場合には、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、当該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及び情報システム情報保証認証者に通知するものとする。

（情報保証統括責任者への報告等）

第２６条の２　情報保証責任者は、毎年度、運用承認の実績を記載した運用承認結果報告書を作成し、情報保証統括責任者に報告するとともに、その写しを情報保証監査責任者に提出しなければならない。

（運用承認実績の大臣報告）

第２７条　情報保証統括責任者は、毎年度、運用承認の実績を取りまとめ、防衛大臣に報告しなければならない。

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２７条の２　情報保証統括責任者は、リスク分析・評価を行うに当たっての基本方針を定めるものとする。

２　情報保証責任者は、情報システム情報保証責任者に対し、毎年度１回以上リスク分析・評価を実施させなければならない。その際、他の機関等の情報保証責任者に協力を依頼することができる。

３　情報システム情報保証責任者は、運用承認を受けた

運用中の情報システムについて、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なければならない。また、その結果を踏まえ、セキュリティ計画書及び継続監視計画書を更新しなければならない。

4　情報システム情報保証責任者は、前項の規定に基づき作成及び更新したリスク評価報告書並びにセキュリティ計画書及び継続監視計画書を情報システム情報保証認証者に提出するものとする。

5　情報システム情報保証認証者は、前項に規定する文書の提出を受けた場合には、これらを踏まえ、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するものとする。

6　情報システム情報保証責任者は、前項に規定するセキュリティ評価文書の提出を受けた場合には、これを踏まえ、将来対応計画書を更新し、情報システム情報保証認証者に提出するものとする。

7　情報システム情報保証認証者は、毎年度１回以上、前

項の規定に基づき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するとともに、必要に応じて、情報システム情報保証責任者に改善指示等を行うものとする。

８　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及び情報保証監査責任者に提出しなければならない。

９　情報保証統括責任者は、前項の規定に基づきリスク分析・評価結果報告書の提出を受けた場合には、これを踏まえ、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る。

（認証情報等の管理）

第２８条　情報システム情報保証責任者は、第１３条の規定に基づき認証機能を設けた場合には、情報システムの利用を認める職員を決定し、当該職員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　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付与された職員は、これらを適切に管理しなければならない。

（アクセス制御）

第２９条　情報システム情報保証責任者は、第１４条の規定に基づきアクセス制御機能を設けた場合には、当該機能を適切に運用しなければならない。

２　職員は、防衛省の電子計算機情報のうち利用を制限すべきものについては、別に定めるところにより、当該情報へのアクセスを制限するために必要な措置を講じなければならない。

（証跡管理）

第３０条　情報システム情報保証責任者は、第１５条の規定に基づき証跡管理機能を設けた場合には、証跡を適切に取得するとともに、一定の期間保存しなければならない。

２　情報システム情報保証責任者は、必要に応じて証跡を分析するものとする。

（暗号化）

第３１条　情報システム情報保証責任者は、第１６条の規定に基づき暗号化機能を設けた場合には、当該機能を適切に運用しなければならない。

２　職員は、防衛省の電子計算機情報のうち可搬記憶媒体に格納し、又は送信するに当たり暗号化すべきものについては、別に定めるところにより、暗号化するために必要な措置を講じなければならない。

（電子署名）

第３２条　情報システム情報保証責任者は、第１７条の規定に基づき電子署名機能を設けた場合には、当該機能を適切に運用しなければならない。

２　職員は、情報システムで取り扱われるデータのうち、当該データの作成者の真正性を特に確保し、及び当該データの改ざんを特に防止すべきものについては、別に定めるところにより、電子署名を付するために必要

な措置を講じなければならない。

（脆弱性対応）

第３３条　情報システム情報保証責任者は、第１８条の規定に基づいて情報システムの脆弱性に対応するために導入した機能等を適切に運用するとともに、必要に応じて当該機能等を更新することにより、情報システムの脆弱性への対応を適切に行わなければならない。

２　職員は、情報システムの脆弱性に対応するため、コンピュータ・ウイルスへの対策その他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３４条　情報システム情報保証責任者は、情報システム室を設けた場合には、情報システム室の入退室管理を適切に行わなければならない。

（情報システムの管理）

第３５条　情報システム情報保証責任者は、情報システムの盗難を防止するため必要な措置を講じなければならない。

２　職員は、防衛省の情報システムを職場から持ち出す場合には、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。

（情報システムの変更）

第３６条　職員は、防衛省の情報システムに係る配線の変更、改造、機器の増設、交換、ソフトウェアの変更等を行う必要がある場合には、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。

（情報システムの利用及び管理に関する規則）

第３７条　情報システム情報保証責任者は、情報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。

２　職員は、情報システム情報保証責任者が定める規則に基づき、情報システムの利用及び管理を行わなければならない。

（業務目的外の使用禁止）

第３８条　職員は、業務目的以外で防衛省の情報システムを使用してはならない。

（職員以外の情報システムの利用）

第３９条　情報システム情報保証責任者は、職員以外の者に情報システムを利用させる場合には、当該情報システムを取り扱う際に職員が守るべき内容を当該職員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４０条　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には、速やかに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、一定の期間保存しなければならない。

２　情報システム情報保証責任者は、前項の措置を講ずるため、定期的に防衛省の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　職員は、自ら使用する防衛省の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４１条　情報システム情報保証責任者は、第２８条から前条まで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は、情報保証を確保するために実施した対策については、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４２条　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、返却、修理等のため部外の者に受け渡す場合には、情報保証を確保する上で必要な措置を講じなければならない。

第４章　防衛省の目的特化型機器に係る対策

（目的特化型機器）

第４２条の２　部隊等情報保証責任者は、防衛省の目的特化型機器について管理簿を作成し、適切に管理する

ものとする。

２　部隊等情報保証責任者は、防衛省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。

第５章　防衛省の可搬記憶媒体に係る対策

（可搬記憶媒体の管理）

第４３条　部隊等情報保証責任者は、防衛省の可搬記憶媒体について、集中保管を行わなければならない。

２　職員は、防衛省の可搬記憶媒体を職場から持ち出す場合には、部隊等情報保証責任者の許可を受けなければならない。

３　職員は、防衛省の可搬記憶媒体を使用する場合には、安全性を確認した上で使用しなければならない。

第６章　私有機器の取扱い

（私有パソコンの取扱い）

第４４条　職員は、私有パソコンを職場に持ち込んではならない。ただし、防衛大学校学生及び防衛医科大学校学生が学修に使用する私有パソコンを教場、自習室、実験室、図書館その他情報保証責任者が定める学修場所（防衛医科大学校病院を除く。）に持ち込む場合については、この限りでない。

２　職員は、船舶の居住区画へ私有パソコンを持ち込む場合は、情報保証責任者の定める対策を実施しなければならない。

３　職員は、私有パソコンで業務用データを取扱ってはならない。

（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４５条　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　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。

第７章　教育及び訓練

（教育及び訓練）

第４６条　情報保証統括責任者は、毎年度、情報保証に関する教育及び訓練の基本方針を定めるものとする。

２　情報保証責任者は、前項の基本方針に基づいて、職員に対し、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、情報保証に関する教育及び訓練を行うものとする。

３　情報保証責任者は、情報保証統括責任者に教育及び訓練の実施状況を報告するものとする。

４　情報保証責任者は、情報保証に関する高度な知識及び技能を有する人材を育成するものとする。

第８章　サイバー攻撃等への対処

（対処要領の策定）

第４７条　情報保証責任者は、事案対処統括責任者と調整し、サイバー攻撃等に対処するための要領（以下「対処要領」という。）を定めるものとする。

２　情報保証統括責任者は、事案対処統括責任者と調整し、機関等に共通の対処要領を定めることができる。

（サイバー攻撃等の未然防止に関する措置）

第４８条　情報保証責任者は、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（以下この条において「セキュリティ情報」という。）を継続的に収集するものとする。

２　情報保証統括責任者は、機関等相互間のセキュリティ情報の共有のために必要な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、セキュリティ情報によりサイバー攻撃等が発生するおそれがあると認める場合には、対処要領に基づき、サイバー攻撃等による被害を未然に防止するための措置を実施するものとする。

４　事案対処責任者は、前項の規定に基づき情報システム情報保証責任者が実施する措置について、対処要領に基づき情報システム情報保証責任者を統制し、又は

情報システム情報保証責任者に対し技術的支援を行うものとする。

5　事案対処統括責任者は、サイバー攻撃等が発生するおそれがある場合の措置について、機関等の事案対処責任者間の連携を図るとともに、必要に応じて事案対処責任者を統制するものとする。

（サイバー攻撃等の発生時の措置）

第４９条　情報システム情報保証責任者は、サイバー攻撃等が発生した場合には、対処要領に基づき、証拠保全、被害拡大防止、復旧等の措置を迅速に実施するとともに、再発防止のための措置を講ずるものとする。

2　事案対処責任者は、前項の規定に基づき情報システム情報保証責任者が実施する措置について、対処要領に基づき情報システム情報保証責任者を統制し、又は情報システム情報保証責任者に対し技術的支援を行うものとする。

3　事案対処統括責任者は、サイバー攻撃等が発生した場合の措置について、機関等の事案対処責任者間の連

携を図るとともに、必要に応じて事案対処責任者を統制するものとする。

（被害状況等の報告）

第５０条　事案対処統括責任者は、サイバー攻撃等により重大な被害が生じた場合には、被害の状況その他必要な事項を防衛大臣及び情報保証統括責任者に報告しなければならない。

第９章　対策の実施状況の確認等

（自己点検）

第５１条　情報保証統括責任者は、毎年度、自己点検の基本方針を定めるものとする。

２　情報保証責任者は、前項の基本方針に基づき、この訓令及びこの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、職員に自己点検を行わせるものとする。

３　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する。

４　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５２条　情報保証監査統括責任者は、毎年度、特に監査を行うべき事項について監査の基本方針を定めるものとする。

２　情報保証監査責任者は、前項の基本方針に基づき、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作成し、この訓令及びこの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、監査を行うものとする。

３　前項の規定は、第１項の基本方針に基づく監査のほか、情報保証監査責任者が必要に応じ監査を行うことを妨げるものではない。

４　情報保証監査責任者は、前２項の監査を行うに当た

っては、情報保証責任者及び他の機関等の情報保証監査責任者に協力を依頼することができる。

5　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し、情報システム情報保証責任者に通知するものとする。

6　情報保証監査責任者は、毎年度、監査の結果を取りまとめた監査結果報告書を作成し、情報保証責任者及び情報保証監査統括責任者に提出するものとする。

7　情報保証責任者は、監査の結果を踏まえ、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する。

8　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するものとする。

（特別監査）

第５３条　前条に定めるもののほか、情報保証監査統括責任者は、この訓令及びこの訓令に基づき定められた規則の遵守状況について、必要に応じ特別監査を行う

ものとする。

２　情報保証監査統括責任者は、特別監査を行うに当たっては、情報保証責任者及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る。

３　情報保証監査統括責任者は、特別監査の結果を取りまとめ、当該特別監査の対象となった機関等の情報保証監査責任者に通知するとともに、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する。

４　情報保証監査統括責任者は、特別監査により情報保証を確保する上で重要な問題が明らかとなった場合には、特別監査の結果その他必要な事項を防衛大臣及び情報保証統括責任者に報告しなければならない。

（職員による報告等）

第５４条　第５１条から前条までに定めるもののほか、職員は、この訓令及びこの訓令に基づき定められた規則に関する違反が発生し、又は発生したおそれがあると認める場合には、直ちに情報保証責任者に報告する

ものとする。

２　情報保証責任者は、前項の報告があった場合には、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する。

第１０章　雑則

（委任規定）

第５５条　この訓令の実施に関し必要な事項は、別に定める。

附　則

１　この訓令は、平成２０年１月１日から施行する。

２　第１６条の規定に基づき暗号化機能を設けるべき情報システムのうち、情報システムの性能その他の技術的な理由により可搬記憶媒体に格納する電子計算機情報を暗号化する機能を設けることが困難なものについては、別に定めるところにより、可搬記憶媒体に電子計算機情報を格納する機能を使用できないように措置しなければならない。

３　この訓令の施行の際現に運用を開始している情報シ

ステム（整備計画局長が定めるものを除く。）については、第１３条から第２２条（同条第３項を除く。）までの規定は、この訓令の施行の後に別表第３の左欄に掲げる場合に該当することとなる場合に同表の中欄に掲げる範囲から適用するものとし、その他の範囲については、なお従前の例による。

４　この訓令の施行の際現に設計が終了している情報システム（整備計画局長が定めるものを除く。）については、第１３条から第２２条（同条第３項を除く。）までの規定は、当該情報システムの運用を開始した後に別表第３の左欄に掲げる場合に該当することとなる場合に同表の中欄に掲げる範囲から適用するものとし、その他の範囲については、なお従前の例による。

５　前２項の規定により整備計画局長が定める情報システムについては、第１３条から第２２条（同条第３項を除く。）までの規定は、この訓令の施行の日から起算して１年を経過した日から適用する。

６　防衛省における電子署名に関する訓令（平成１５年

防衛庁訓令第６４号）の一部を次のように改正する。

題名を次のように改める。

防衛省における認証局システムによる電子署名に関する訓令

第１条中「電子署名」を「認証局システムによる電子署名」に改める。

第２条第２号に次のように加える。

ウ　第５条第１項及び第３項の規定により運用企画局長から交付されたＩＣカードを使用して行うものであること。

第３条中第１項を削り、同条第２項を第１項とする。

附　則（平成２０年省訓第１２号）

１　この訓令は、平成２０年３月２６日から施行する。

附　則（平成２１年省訓第４８号）

１　この訓令は、平成２１年８月１日から施行する。

附　則（平成２６年省訓第２６号）

この訓令は、平成２６年７月１日から施行する。

附　則（平成２７年省訓第３６号）

この訓令は、平成２７年１０月１日から施行する。

附　則（令和５年省訓第２６号）

１　この訓令は、令和５年７月１日から施行する。

２　この訓令の施行の際、現に運用を開始している情報システムについては、この訓令による改正後の別表第３の左欄に掲げる場合に該当する場合には、この訓令による改正後の第２６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、この訓令による改正後の第２６条の規定の例により運用承認を受けるものとする。この場合において同条本文中「別表第３の左欄に掲げる場合には、同表の右欄に掲げる時期」とあるのは、「令和９年度末」と読み替えるものとする。

３　この訓令の施行の際、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、この訓令による改正後の第２６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年度末までにこの訓令による改正後の第２６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。

附　則（令和５年省訓第５６号）

この訓令は、令和５年７月１日から施行する。

別表第１（第６条関係）

機関等	情報保証責任者
防衛省本省の内部部局	整備計画局長
防衛大学校	防衛大学校長
防衛医科大学校	防衛医科大学校長
防衛研究所	防衛研究所長
統合幕僚監部及び自衛隊サイバー防衛隊	統合幕僚長
陸上自衛隊、自衛隊情報保全隊、自衛隊体育学校、自衛隊中央病院、陸上幕僚長の監督を受ける自衛隊地区病院及び自衛隊地方協力本部	陸上幕僚長
海上自衛隊及び海上幕僚長の監督を受ける自衛隊地区病院	海上幕僚長
航空自衛隊及び航空幕僚長の監督を受ける自衛隊地区病院	航空幕僚長
情報本部	情報本部長
防衛監察本部	防衛監察監
地方防衛局	地方防衛局長
防衛装備庁	防衛装備庁長官

別表第２（第８条関係）

機関等	部隊等情報保証責任者を置く単位
防衛省本省の内部部局	課及びこれに準ずる単位並びにこれらに準ずるものとして情報保証責任者が定める単位
防衛大学校	
防衛医科大学校	
防衛研究所	
統合幕僚監部	
陸上幕僚監部	
海上幕僚監部	
航空幕僚監部	
情報本部	
防衛監察本部	
地方防衛局	
防衛装備庁	
自衛隊サイバー防衛隊	情報保証責任者が定める単位
陸上自衛隊(陸上幕僚監部を除く。)、自衛隊情報保全隊、自衛隊体育学校、自衛隊中央病院、陸上幕僚長の監督を受ける自衛隊地区病院及び自衛隊地方協力本部	
海上自衛隊（海上幕僚監部を除く。）及び海上幕僚長の監督を受ける自衛隊地区病院	
航空自衛隊（航空幕僚監部を除く。）及び航空幕僚長の監督を受ける自衛隊地区病院	

別表第３（第２６条関係）

運用承認を受ける場合		運用承認を受ける時期
1	新たに情報システムを整備する場合	新たに整備した情報システムの運用を開始するまでの時期
2	情報システムの換装を行う場合	換装後の情報システムの運用を開始するまでの時期
3	運用承認から情報保証責任者が定める期間を経過する場合	情報保証責任者が定める期間を経過するまでの時期
4	運用環境の変化や情報システムの構成の変更により、情報保証に係る機能及び対策に変更がある場合等、情報保証責任者が運用承認を新たに行うことが必要と認める場合	情報保証責任者が運用承認を新たに行うことが必要と認める事情変更等がなされるまでの間