

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

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（第1条－第3条）

第2章 組織及び体制（第4条－第12条）

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（第

13条－第25条）

第2節 運用承認（第26条・第27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28条－第41条）

第4節 情報システムの廃棄等に当たっての対策（第  
42条）

第4章 防衛省の可搬記憶媒体に係る対策（第43条）

第5章 私有パソコン及び私有可搬記憶媒体の取扱い  
（第44条・第45条）

第6章 教育及び訓練（第46条）

第7章 サイバー攻撃等への対処（第47条－第50  
条）

第8章 対策の実施状況の確認等（第51条－第56  
条）

第9章 雑則（第57条）

附則

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情報システムにおいて取り扱われるデータに関して、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 情報システム及び情報システムにおいて取り扱われるデータの機密性（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じることをいう。

(4) 可搬記憶媒体 パソコン又はその周辺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。

(5) 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

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。

(6) 電子計算機情報 防衛省の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。

(7) 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。

(8) 職場 職員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。

(9) 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。

(適用除外)

第3条 この訓令は、別に定める情報システム及び当該情報システムにおいて取り扱われるデータについては、第6条第1項に規定する情報保証責任者が必要と認める場合を除き、適用しない。

## 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する者として、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可搬記憶媒体の管理並びに私有パソコン及び私有可搬記憶媒体での業務用データの取扱いの禁止等第5章に規定する私有パソコン及び私有可搬記憶媒体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)

第9条 情報保証責任者は、第26条第2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実施計画について、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。

(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し、機関等の連携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 1 1 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 1 2 条 防衛省の情報保証に関して機関等相互間の調整、連絡並びに技術的事項の検討及びこの訓令の見直しの審議を行うため、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、整備計画局情報通信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、整備計画局情報通信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（以下「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（以下「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、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（以下「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（以下「証跡」という。）を取得する機能（以下「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、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（以下「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（以下「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うものとする。

(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。

(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（以下「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。

(情報システムの技術に関する基準)

第24条 第13条から第19条までに規定する情報システムの機能及び設定に関し、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の細部は、整備計画局長が定める。

(情報システムの調達)

第25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。

## 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、同表の中欄に掲げる範囲を対象として、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。

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、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を記載した実施計画を作成し、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責任者は、前項の規定に基づき実施計画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。
- 4 情報システム情報保証認証者は、第2項の規定に基づき実施計画の提出を受けた場合には、これを審査し、当該実施計画に記載された措置を実施した上で情報システムを運用することが可能と認める場合には、当該実施計画を認証し、当該実施計画及び認証結果報告書を情報保証責任者に提出するものとする。
- 5 情報保証責任者は、前項の規定に基づき実施計画及び認証結果報告書の提出を受けた場合には、これを審査し、当該実施計画に記載された措置を実施した上で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に通知するものとする。

(運用承認実績の報告)

第27条 情報保証責任者は、毎年度、運用承認の実績を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

(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、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、アクセス制御の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、情報システムで取り扱われる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 3 2 条 情報システム情報保証責任者は、第 1 7 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、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 3 3 条 情報システム情報保証責任者は、第 1 8 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。

(電子計算機の管理)

第35条 情報システム情報保証責任者は、電子計算機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、防衛省の電子計算機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。

(情報システムに関する文書の整備等)

第37条 情報システム情報保証責任者は、情報システムの仕様、設計、機器の設置場所、使用者名その他の

情報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 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。

3 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、維持管理等において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 4 4 条 職員は、私有パソコンを職場及び船舶の居住区画に持ち込んで서는ならない。

2 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。

(私有可搬記憶媒体の取扱い)

第 4 5 条 職員は、私有可搬記憶媒体を防衛省の情報システムで使用して서는ならない。

2 職員は、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 4 6 条 情報保証責任者は、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。

2 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 7 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、特に必要な情報システムについては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、必要に応じ、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。

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括するものとする。

(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括するものとする。

(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に報告しなければならない。

## 第8章 対策の実施状況の確認等

(自己点検)

第51条 情報保証責任者は、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、毎年度、職員に自己点検を行わせるものとする。

- 2 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。

- 3 情報保証監査統括責任者は、情報保証責任者に対し、必要に応じ自己点検の結果について報告を求めることができる。

(自己点検の基本方針)

第52条 情報保証統括責任者は、前条第1項の規定に基づき情報保証責任者が職員に自己点検を行わせるに当たり、必要に応じて自己点検の基本方針を定めることができる。

- 2 情報保証責任者は、前項の基本方針が定められた場合には、当該基本方針に基づいて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、第1項の基本方針に基づき自己点検を行わせた場合には、その結果について、情報保証統括責任者に報告するものとする。

(監査)

第53条 情報保証責任者は、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、毎年度、監査を行うものとする。

- 2 情報保証責任者は、監査を行うに当たっては、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 情報保証責任者は、監査の結果を取りまとめるとともに、当該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。
- 4 情報保証監査統括責任者は、情報保証責任者に対し、必要に応じ監査の結果について報告を求めることができる。

(監査の基本方針)

第54条 情報保証監査統括責任者は、前条第1項の規定に基づき情報保証責任者が監査を行うに当たり、必要に応じて監査の基本方針を定めることができる。

- 2 情報保証責任者は、前項の基本方針が定められた場合には、当該基本方針に基づいて監査を行うものとする。
- 3 情報保証責任者は、第1項の基本方針に基づいて監査を行った場合には、その結果について、情報保証監

査統括責任者に報告するものとする。

(特別監査)

第55条 前2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に報告しなければならない。

(職員による報告等)

第 5 6 条 第 5 1 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 9 章 雑則

(委任規定)

第 5 7 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 2 0 年 1 月 1 日から施行する。
- 2 第 1 6 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



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 1 3 条から第 2 2 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 1 5 年防衛庁訓令第 6 4 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 I C 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 2 0 年省訓第 1 2 号）

- 1 この訓令は、平成 2 0 年 3 月 2 6 日から施行する。

附 則（平成 2 1 年省訓第 4 8 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。

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指揮通信システム隊	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	
自衛隊指揮通信システム隊	
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		対象となる範囲	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	情報システム全体	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	換装を行った部分	換装後の情報システムの運用を開始するまでの時期
前2項に掲げる場合以外で、次のいずれかに該当する場合			
3	ア 第13条から第22条まで（同条第3項を除く。）の規定に基づく措置を変更する場合	変更する措置	変更した措置を適用するまでの時期
	イ 第13条から第22条まで（同条第3項を除く。）の規定に基づく措置を実施し、又は実施しないと判断する前提となった事項に変更がある場合	変更がある事項を前提とした措置	前提となった事項が変更されるまでの時期