運情第１２９３３号
１９．１２．２７
一部改正　運情第３６７４号
２０．３．２５
一部改正　運情第９２００号
２１．７．３１
一部改正　防運情第１０５７４号
２６．７．１５
一部改正　防運事第１４８９６号
２７．１０．１
一部改正　防整情第７２２５号
２８．３．３１
一部改正　防整情第７１２１号
３１．４．１
一部改正　防整情第５７８２号
令和３年３月３１日
一部改正　防整情第１４０４１号
令和５年６月３０日

大臣官房長
防衛政策局長
人事教育局長
地方協力局長
衛生監
施設監
殿

整備計画局長

防衛省本省の内部部局情報保証実施規程について（通知）

標記について、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）及び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）に基づき、別添のとおり定め、平成２０年１月１日から施行することとしたので通知する。

なお、内部部局情報保証実施規定について（官情第６００２号。１６．７．１）及び秘密電子計算機情報流出等再発防止に係る抜本的対策を実施するための措置の細部について（官情第４７３７号。１８．５．１６）は、平成１９年１２月３１日限りで廃止する。

添付書類：防衛省本省の内部部局情報保証実施規程
配布区分：情報通信課長

防衛省本省の内部部局情報保証実施規程

第１　組織及び体制

（１）情報保証監査責任者

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。）第６条の２第１項に規定する情報保証監査責任者は、情報保証責任者が指定する者とする。

（２）情報システム情報保証責任者

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、当該情報システムを管理する課等（各課、訟務管理官、防衛政策局に置かれる参事官、施設整備官、提供施設計画官、施設技術管理官、服務管理官及び衛生官をいう。以下同じ。）の長とする。

（３）システム管理担当者

①　情報システム情報保証責任者は、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として、必要に応じ、情報システムを管理する業務の実務を担当するシステム管理担当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は、システム管理担当者に情報システム内部の重要な設定等を行うための権限を付与し、これを行使させることができる。

③　システム管理担当者の指定は、必要最小限の範囲の者に限定するものとする。

（４）システム担当者

情報システム情報保証責任者は、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として、課室等（課等又は各室若しくはそれに準ずるものとして別表に掲げるものをいう。以下同じ。）ごとに、必要に応じ、情報システム情報保証責任者又はシステム管理担当者との連絡調整を担当するシステム担当者を指定するものとする。

（５）システム利用者

情報システムを利用する者として、訓令第２８条第１項に基づき情報システム情報保証責任者から認証情報等を付与された者をいう。

（６）部隊等情報保証責任者

訓令第８条第１項に規定する部隊等情報保証責任者は、課室等の長とする。

（７）情報システム運用者

訓令第９条第１項に規定する情報システム運用者は、システム利用者の中から情報システム情報保証責任者が指定する者とする。

（８）情報システム情報保証認証者

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は、情報保証責任者が指定する者とする。

（９）事案対処責任者

訓令第１１条に規定する事案対処責任者は、情報保証責任者が指定する者とする。

（１０）情報保証担当者

事案対処責任者は、セキュリティ情報に関する連絡調整を担当する情報保証担当者を指定するものとする。

（１１）情報保証対策委員会防衛省本省の内部部局委員

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、次のとおりとする。

防衛政策局調査課長

（１２）情報保証監査責任者、情報システム情報保証認証者及び事案対処責任者の指定にあたっては、別紙様式第１による指定書を交付して行うものとする。

第２　防衛省の情報システムに係る対策

１　全般

（１）情報システムを導入する場合の措置

課等の長は、防衛省本省の内部部局に新たに情報システムを導入する場合には、情報保証責任者に通知するものとする。

（２）情報システムの運用を終了した場合の措置

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した場合には、情報保証責任者に通知するものとする。

２　情報システムの運用、管理等に当たっての対策

（１）運用管理要領について

情報システム情報保証責任者は、訓令３７条第１項に規定する運用管理要領を策定し、システム利用者に対し遵守させるとともに、毎年度１回以上、見直し又は更新を行うこと。

（２）認証情報等の管理について

認証情報等の管理については、訓令第２８条及び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。以下「運用通達」という。）第５第１項に規定するもののほか、次のとおりとする。

① 情報システム情報保証責任者は、認証情報等の付与状況を記録しておくこと

② 認証情報は、情報システムが強制的に変更を行わせる設定が可能な場合は当該設定を有効にしておくものとし、利用者毎に固定されている場合は情報システム情報保証責任者が定期的に変更すること

（３）証跡管理について

証跡管理については、訓令第３０条第１項及び運用通達第５第４項に規定するもののほか、次のとおりとする。

① 情報システム情報保証責任者は、監査及び責任追跡性（情報に対する操作と操作したユーザを特定し証拠を残して追跡できる特性）の確保並びにセキュリティ管理を円滑に実施するため、当該システムの特性に応じて、証跡情報（操作ログ、認証ログ、アクセスログ等）を取得するものとする。

② 情報システム情報保証責任者は、当該システムの特性に応じて、前項で取得した証跡情報と脆弱性スキャン情報、性能データ、システム監視情報等を相互に関連付けし、必要に応じて他機関の事案対処責任者から提供される情報を含め分析を行うものとする。

③ 証跡の保存期間は、情報システムの証跡管理について（防運情第６０７３号。２６．４．２５）によるものとする。

（４）情報システム室の入退室管理について

情報システム室の入退室管理については、訓令第３４条及び運用通達第５第７項に規定するもののほか、防衛省以外に情報システムを設置する場合を除き、次のとおりとする。

① 情報システム情報保証責任者は、情報システム室への立入を許可した者に対して、知識情報（ＰＩＮコード、パスワード等)、所持情報（ハードウェアトークン、ＩＣカード等)、生体情報等を用いた機器により、当該施設への入退室を制御するとともに、入退室の履歴を記録すること

② 情報システム情報保証責任者は、防衛省本省の内部部局が管理する情報システムを他の情報保証責任者が管理する情報システム室に設置する場合には、当該情報システム室への入室を許可された者を記録しておくこと

（５）電子計算機の盗難防止について

① 電子計算機の盗難防止については、訓令第３５条及び運用通達第５第９項に規定するもののほか、次のとおりとする。

ア　電子計算機を設置している事務室等であって、パスワード認証又はＩＣカード認証等により入室を制限していない事務室等の課等の長は、職員が不在にする場合には確実に施錠するものとする。

イ　電子計算機を設置している事務室等であって、パスワードにより入室を制限している事務室等の課等の長は、パスワードについて、必要な者以外に知らせない、メモを作らない、職員の異動があったとき等に適宜変更する等適切に管理・維持するものとする。

ウ　電子計算機を設置している事務室等であって、認証情報を記録したＩＣカード等により入室を制限している事務室等の課等の長は、当該ＩＣカード等の利用者に、当該ＩＣカード等を無断で貸与しない等適切に管理させるものとする。

②　運用通達第５第９項第２号の規定によるかぎの管理は、情報システム情報保証責任者又は情報システム情報保証責任者補助者が行うものとする。

（６）職員以外の情報システムの利用について

情報システム情報保証責任者は、訓令第３９条の規定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には、次に掲げる事項を職員以外の者に説明するとともに情報保証を確保するためシステム利用者から職員を指定し、監督させる等の措置を講じなければならない。

①　当該情報システムを利用して行うことのできる行為

②　当該情報システムを利用して得られる情報の範囲

③　その他注意事項

（７）課室等におけるシステム利用者の管理

システム担当者は、担当する課室等に所属する者であって担当するシステム利用者を記録しておくものとする。

（８）情報システムの廃棄等

情報システム情報保証責任者は、情報システムの構成品を廃棄する場合は、物理的な破壊、外部磁界による消磁、データ上書き方式等により必要な措置を講じるものとする。ただし、当該情報システムがセキュリティ分類において機密性が区分「高」の場合は、物理的な破壊又は外部磁界による消磁によるものとする。

第３　目的特化型機器に係る対策

１　目的特化型機器の保管について

（１）部隊等情報保証責任者は、目的特化型機器をかぎのかかる容器に保管す

るものとする。ただし、使用状態のもの、若しくは形状、設置方法等により、これによりがたい場合は、不正利用等を防止する措置を講じるものとする。

（２）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、前号のかぎの管理を適切に行うものとする。

（３）部隊等情報保証責任者は、必要に応じて目的特化型機器の保管数及び使用数と次項の目的特化型機器管理簿を照合し、目的特化型機器の管理が確実になされていることを確認するものとする。

２　目的特化型機器の管理について

（１）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、一つの目的特化型機器ごとに別紙様式第１に示す目的特化型機器管理簿（以下、第３において単に「管理簿」という。）を設けるものとする。

（２）目的特化型機器にはそれぞれに固有の機器番号を付すこととし、当該番号を目的特化型機器の見えやすい位置に貼付等するものとする。

３　目的特化型機器の使用について

（１）職員は、第１項第１号の保管場所に保管されている目的特化型機器を使用する場合は、その都度、使用開始日時、使用者名、使用目的、設置場所（使用場所）を管理簿に従い記入するとともに、退庁の際は、目的特化型機器を保管場所に返却し、返却日時を管理簿に記入するものとする。

（２）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、返却を受けた目的特化型機器にデータが保存されていないか確認を行い、保存されている場合は、データの削除を行うものとする。

４　目的特化型機器の貸出しについて

（１）職員は、目的特化型機器を一時的に職場から持出し、自らが所属する課室等の職員以外の者に貸出しする場合は、あらかじめ、前項第１号により記入する事項に加え、貸出しの都度、期間、貸出し相手、貸出し目的を管理簿に記入するとともに、当該目的特化型機器から貸出し先で業務上必要となるデータ以外のデータを消去する等、情報保証を確保するための措置を講じなければならない。

（２）部隊等情報保証責任者は、前号により管理簿に必要な事項が記入されていること及び当該目的特化型機器に貸出し先で業務上必要となるデータ以外のデータが保存されていないことを確認するとともに、保存されている業務用データを複製しないことを指導する等により情報保証を確保するた

めの措置の実施を確認の上、目的特化型機器の貸出しを許可するものとする。

5　目的特化型機器の持出し又は貸出し先におけるデータの複製について

（1）職員は、特段の業務上の必要性から、目的特化型機器内に保存されている業務用データを持出し又は貸出し先で複製しようとする場合は、あらかじめ、第3項第1号及び第4項第1号により記入する事項に加え、複製する業務用データの内容、複製する相手方及び複製目的を管理簿に記入するものとする。

（2）部隊等情報保証責任者は、前号により管理簿に必要な事項が記入されていること及びその他の業務用データを複製しないことを指導する等により情報保証を確保するための措置の実施を確認の上、目的特化型機器の持出し又は貸出し先における複製を許可するものとする。

6　目的特化型機器の廃棄等について

（1）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、目的特化型機器を廃棄等（管理換え等を含む。）する場合は、データが抹消されていることを確認の上、廃棄等の日時及び廃棄等の実施者を管理簿に記入するものとする。

（2）目的特化型機器の廃棄等は、当該物品の管理要領等に基づき、適切に措置を行うものとする。

第4　防衛省の可搬記憶媒体に係る対策

1　集中保管について

（1）部隊等情報保証責任者は、管理する可搬記憶媒体を、全て一つのかぎのかかる容器に保管する等により、一箇所に集中して保管するものとする。

（2）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、前号のかぎの管理を適切に行うものとする。

（3）部隊等情報保証責任者は、必要に応じて可搬記憶媒体の保管数と次項の可搬記憶媒体管理簿を照合し、可搬記憶媒体の保管が確実になされていることを確認するものとする。

2　可搬記憶媒体管理簿の管理について

（1）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、一つの可搬記憶媒体ごとに、別紙様式第2に基づき可搬記憶媒体管理簿（以下、第4

において単に「管理簿」という。）を設けるものとする。
（２）可搬記憶媒体にはそれぞれに固有の媒体番号を付すこととし、当該番号を可搬記憶媒体の見えやすい位置に貼付等するものとする。

３　可搬記憶媒体の使用について
（１）職員は、第１項第１号の保管場所（以下「保管場所」という。）から可搬記憶媒体を取り出して使用する場合は、その都度、使用開始日時、使用者名、使用目的を管理簿に従い記入するとともに、退庁の際は、可搬記憶媒体を保管場所に返却し、返却日時を管理簿に記入するものとする。
（２）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、返却を受けた可搬記憶媒体にデータが保存されていないか確認を行い、保存されている場合は、データの削除を行うものとする。

４　可搬記憶媒体の持出し・貸出しについて
（１）職員は、可搬記憶媒体を一時的に職場から持ち出そうとし、又は自らが所属する課室等の職員以外の者に貸し出そうとする場合は、あらかじめ、第３項第１号により記入する事項に加え、持出し又は貸出しの都度、持出し又は貸出し期間、持出し又は貸出し先、持出し又は貸出し目的を管理簿に記入するとともに、当該可搬記憶媒体から持出し先で業務上必要となるデータ以外のデータを消去する等、情報保証を確保するための措置を実施しなければならない。
（２）部隊等情報保証責任者は、前号により管理簿に必要な事項が記入されていること及び当該可搬記憶媒体に持出し又は貸出し先で業務上必要となるデータ以外のデータが保存されていないことを確認するとともに、持出しの場合には保存されている業務用データを複製しないことを指導する等により情報保証を確保するための措置の実施を確認の上、可搬記憶媒体の持出しを許可するものとする。
（３）職員は可搬記憶媒体を貸し出した場合には、貸出し相手を管理簿に記入するものとする。

５　可搬記憶媒体の持出し又は貸出し先におけるデータの複製について
（１）職員は、特段の業務上の必要性から、可搬記憶媒体内に保存されている業務用データを持出し又は貸出し先で複製しようとする場合は、あらかじめ、第３項第１号及び第４項第１号により記入する事項に加え、複製する業務用データの内容、複製する相手方及び複製目的を管理簿に記入するものとする。

（２）部隊等情報保証責任者は、前号により管理簿に必要な事項が記入されていること及びその他の業務用データを複製しないことを指導する等により情報保証を確保するための措置の実施を確認の上、可搬記憶媒体の持出し又は貸出し先における複製を許可するものとする。

６　可搬記憶媒体の交付について

（１）職員は、可搬記憶媒体を自らが所属する課室等の職員以外の者に交付（当該職員以外の者に譲渡し返却されない場合をいう。以下同じ。）しようとする場合は、あらかじめ、第３項第１号により記入する事項に加え、交付日時、交付先、交付目的、交付実施者を管理簿に記入するとともに、当該可搬記憶媒体から交付する必要があるデータ以外のデータを消去する等、情報保証を確保するための措置を実施しなければならない。

（２）部隊等情報保証責任者は、前号により管理簿に必要な事項が記入されていること及び当該可搬記憶媒体に交付する必要があるデータ以外のデータが保存されていないことを確認する等により情報保証を確保するための措置の実施を確認の上、可搬記憶媒体の交付を許可するものとする。

（３）職員は可搬記憶媒体を交付した場合には、交付相手を管理簿に記入するものとする。

（４）部隊等情報保証責任者は、職員が、可搬記憶媒体を自らが所属する課室等の職員以外の者より交付を受けた場合は、第２項の例による。

７　可搬記憶媒体の破棄について

（１）職員は、可搬記憶媒体を破棄する場合は、破棄の日時及び破棄の実施者を管理簿に記入したうえ部隊等情報保証責任者が指定する者の立会いのもとに破棄を実施するものとする。その際、破棄立会者は自己の所属及び名前を管理簿に記入するものとする。

（２）可搬記憶媒体の破棄は、焼却、粉砕、細断、溶解、破壊等の方法により、確実に行わなければならない。

（３）部隊等情報保証責任者は、業務上不要となった可搬記憶媒体を必要に応じて破棄しなければならない。

第５　教育及び訓練

教育及び訓練については、訓令第４６条に規定するもののほか、次のとおりとする。

（１）整備計画局サイバー整備課長は、情報漏えい対応を含めた情報保証に

関する教育資料を作成の上、自らあるいは課等の長を通じ、職員に対し、毎年度１回以上教育を行うものとする。

（２）情報システム情報保証責任者は、自らの管理する情報システム特有の情報保証上の問題点を考慮の上、必要に応じ、システム利用者に対し、教育を行うものとする。

（３）（１）及び（２）により教育を行った場合には、教育の実施日、被教育者等実施状況を別紙様式第２により記録しておくものとする。この場合、①において、課等の長を通じて教育を行った場合には、当該課等の長が記録しておくものとする。

（４）情報システム情報保証責任者は、訓令第２６条第２項に規定するセキュリティ計画書において作成する緊急時対応計画について、その有効性を判断するため、チェックリスト、手順書の確認訓練、机上演習、シミュレーション、総合演習等の手法により、少なくとも毎年度１回以上、確認するものとする。

第６　サイバー攻撃等への対処

訓令第４７条に規定する要領は、別添のとおりとする。

第７　対策の実施状況の確認等

１　自己点検及び監査について

自己点検及び監査に関する事務は、整備計画局サイバー整備課において処理する。。

２　インターネット上への情報流出を把握した場合の対応について

（１）運用通達別紙の第２項第１号に規定する情報通信担当課は、整備計画局サイバー整備課とし、秘密保全担当課は、防衛政策局調査課とする。

（２）前号の情報通信担当課の連絡先は、整備計画局サイバー整備課事案対処班とし、秘密保全担当課の連絡先は、防衛政策局調査課情報保全企画室とする。

別表

室に準ずるもの	室に準ずるものの長
大臣官房文書課に所属する者のうち、防衛省本省の内部部局の内部組織に関する訓令（平成１９年防衛省訓令第５３号。以下「内部組織訓令」という。）第５条第１１項に規定する法令審査官及び法令審査官が総括する事務に従事するため配置された者で構成されるグループ	法令審査官
大臣官房文書課に所属する者のうち、内部組織訓令第５条第１５項に規定する国会担当連絡調整官及び同項に規定する事務に従事するため配置された者（次項に掲げる者を除く。）で構成されるグループ	国会担当連絡調整官
大臣官房文書課に所属する者のうち、内部組織訓令第５条第１５項に規定する国会担当連絡調整官及び同項に規定する事務に従事するため配置された者であって、参議院別館に配置されたもので構成されるグループ	グループを構成する者のうち先任の者
防衛省図書館	図書館長
防衛白書作成事務の円滑な遂行に資するため、別に定めるところにより大臣官房広報課に設置された防衛白書作成事務室	構成員のうち部員の者
弾道ミサイル防衛調査分析チーム及び連絡調整会議設置について（防防防第３３１０号。１６．３．３１）別紙の第１に規定する弾道ミサイル防衛調査分析チームを構成するチーム長及びチーム員のうち、Ｅ２棟に配置された者で構成されるグループ	チーム長

別紙様式第１

指　　定　　書

所　　属
官名又は階級　　氏　　名

防衛省本省の内部部局情報保証実施規程について（運情第１２９３３号。１９．１２．２７）［第１第１項　情報保証監査責任者／第１第８項　情報システム情報保証認証者／第１第９項　事案対処責任者］の規定によるに指定する。

令和　　年　　月　　日

情報保証責任者

官　　職　　氏　　名

別紙様式第２

目的特化型機器管理簿

機器番号：

番号	目的特化型機器の使用					目的特化型機器の一時貸出し			持出し又は貸出し先における業務用データの複製		
	使用開始日時	使用者名	使用目的	設置場所 （使用場所）	返却日時	期間	貸出し相手	貸出し目的	複製する 業務用データ の内容	複製する相手方	複製目的
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

廃棄等日時

廃棄等実施者　　所属　　氏名

※ この様式は一つの目的特化型機器ごとに作成するものとする。

別紙様式第３

可搬記憶媒体管理簿

媒体番号：

番号	可搬記憶媒体の使用				可搬記憶媒体の一時持出し・貸出し・交付				持ち出し又は貸出し先における業務用データの複製		
	使用開始日時	使用者名	使用目的	返却日時	持出し 貸出し 交付の別	持出し 貸出し期間 （交付日時）	持出し 貸出し先 （交付者名）	持出し 貸出し目的 （交付目的）	複製する 業務用データ の内容	複製する相手方	複製の目的
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

破棄（交付）日時

破棄（交付）実施者　　所属　　名前

破棄立会者　　所属　　名前

※ この様式は一つの可搬記憶媒体ごとに作成するものとする。

別紙様式第４

教育実施状況記録

局　　課　　室又はグループ

実施日	実施者	実施手段	教育内容	被教育者

（注）１　「実施手段」の欄には、集合教育、ホームページ掲載、メールによる資料送付等教育の手段を記入する。

２　「教育内容」の欄には、教育内容の概要を記入する。

３　「被教育者」の欄には、対象者（例：課員全員、システム担当者）及び教育を受けた人数を記入する。

別添

サイバー攻撃等対処要領

１　基本的枠組み

サイバー攻撃、データ侵害、セキュリティ違反等に係るセキュリティインシデントに対応するための処要を定め、サイバー攻撃を未然に防ぎ、又は発生したサイバー攻撃に対して、その影響を軽減するもの

２　連絡体制

（１）連絡先の把握

ア　情報保証担当者は、情報保証統括責任者、情報保証責任者、事案対処統括責任者、事案対処責任者及びシステム管理担当者の連絡先を把握しておくものとする。

イ　システム管理担当者は、事案対処責任者、情報システム情報保証責任者、情報保証担当者及びシステム担当者の連絡先を把握しておくものとする。

ウ　システム担当者は、情報システム情報保証責任者、システム管理担当者及びシステム利用者の連絡先を把握しておくものとする。

エ　システム利用者は、情報システム情報保証責任者、システム管理担当者及びシステム担当者の連絡先を把握しておくものとする。

（２）連絡要領

連絡要領は、運用通達第１１第２項及び第３項に規定するもののほか、次のとおりとする。（付図１及び２参照）

ア　運用通達第１１第３項第１号に規定する情報システム情報保証責任者への通報は、システム管理担当者に対して行うことで足りるものとする。

イ　システム管理担当者は、アの通報を受けた場合又は自らサイバー攻撃等を検知した場合には、情報システム情報保証責任者に通報するとともに情報保証担当者に通報するものとする。

ウ　運用通達第１１第３項第２号に規定する事案対処責任者への通報は、情報保証担当者に対して行うことで足りるものとする。

エ　情報保証担当者は、ウの通報を受けた場合には、事案対処責任者にホームページ、電子メール等を用いて通報するものとする。

３　セキュリティ情報の収集・配布・対処

（１）システム管理担当者は、最新のセキュリティ情報の把握に努めるものとし、次に掲げるインシデント分類の兆候を認知したとき又は重要と思われるセキュリティ情報（以下「セキュリティ情報等」という。）を入手したときは、情報システム情報保証責任者及び情報保証担当者に通報するものとするとともに、必要に応じ、ホームページ、メール等によりシステム利用者に、一斉通報を行うこと。

ア　不正アクセス

イ　ホームページの改ざん

ウ　サービス不能攻撃

エ　コンピュータ・ウイルス等のうち広範囲な情報システムに重大な影響を及ぼすおそれのあるもの

オ　情報システムに係る情報の窃盗、漏えい又は改ざん

カ　自然災害によるシステム停止

キ　インサイダー脅威

ク　その他情報システムに係る犯罪、不正行為等

（２）情報保証担当者は、前号によりセキュリティ情報等の通報を受けたとき又は防衛省以外の政府機関等からセキュリティ情報等を入手したときは、システム管理担当者に通報するとともに、必要に応じ事案対処責任者及び情報保証責任者に通報するものとする。

（３）システム管理担当者は、前号により通報を受けたセキュリティ情報等のうち、必要と思われるものを情報システム情報保証責任者及びシステム利用者に連絡するとともに、セキュリティ情報等が情報システムに与える影響を考慮し、情報システム情報保証責任者の指示のもと、情報システムに対する措置を行うものとする。

４　統幕事案対処責任者からの通報等を受けた措置

（１）事案対処責任者は、防衛情報通信基盤及びこれに接続する情報システムに関するサイバー攻撃等対処要領について（運情第３６６８号。２０．３．２５。以下「防衛情報通信基盤等対処要領」という。）第３第１号、第２号又は第５号の通報を受けた場合には、防衛情報通信基盤に接続している情報システムの情報システム情報保証責任者に通報するとともに、情報保証責任者に報告するものとする。

（２）事案対処責任者は、防衛情報通信基盤等対処要領第３第７号の調整を受けた場合には、必要に応じて、切断等の対象となる防衛情報通信基盤に接続している情報システムの情報システム情報保証責任者と調整するものとする。

5　応急処置

（1）情報システム情報保証責任者又はシステム管理担当者は、被害が拡大する恐れがある場合又は被害が拡大するかどうか判断できないような場合には、情報システム又は事案が発生した電子計算機をネットワークから切断又は隔離等することにより、被害の拡大防止に努めるものとする。

（2）情報システム情報保証責任者又はシステム管理担当者は、システム利用者が行うことが適切な応急処置について、システム担当者又はシステム利用者に連絡し対処させるものとする。

6　原因探求

（1）情報システム情報保証責任者及びシステム管理担当者は、障害の記録及び運用状況を調査しサイバー攻撃等の原因となる事項を特定するよう努めるものとし、新たに明らかになった事実について速やかに事案対処責任者又は情報保証担当者に通報するものとする。

（2）事案対処責任者及び情報保証担当者は、サイバー攻撃等の原因となる事項に関する情報を得た場合又はネットワーク監視装置等において自動検知した場合には、速やかに情報システム情報保証責任者及びシステム管理担当者にホームページ、メール等によりシステム利用者に、一斉通報を行うこととする。

7　復旧処置

（1）情報システム情報保証責任者及びシステム管理担当者は、情報システムの復旧に長時間要すると判断した場合には、その旨システム担当者を通じてシステム利用者に連絡するとともに、システム復旧計画を作成し、事案対処責任者及び情報保証担当者に報告するものとする。

（2）情報システム情報保証責任者及びシステム管理担当者は、事案に対処する方策を確立した場合には、次のとおり対処する。

ア　情報システム情報保証責任者又はシステム管理担当者の対処で復旧する場合には、復旧措置後システム担当者にその旨連絡する。

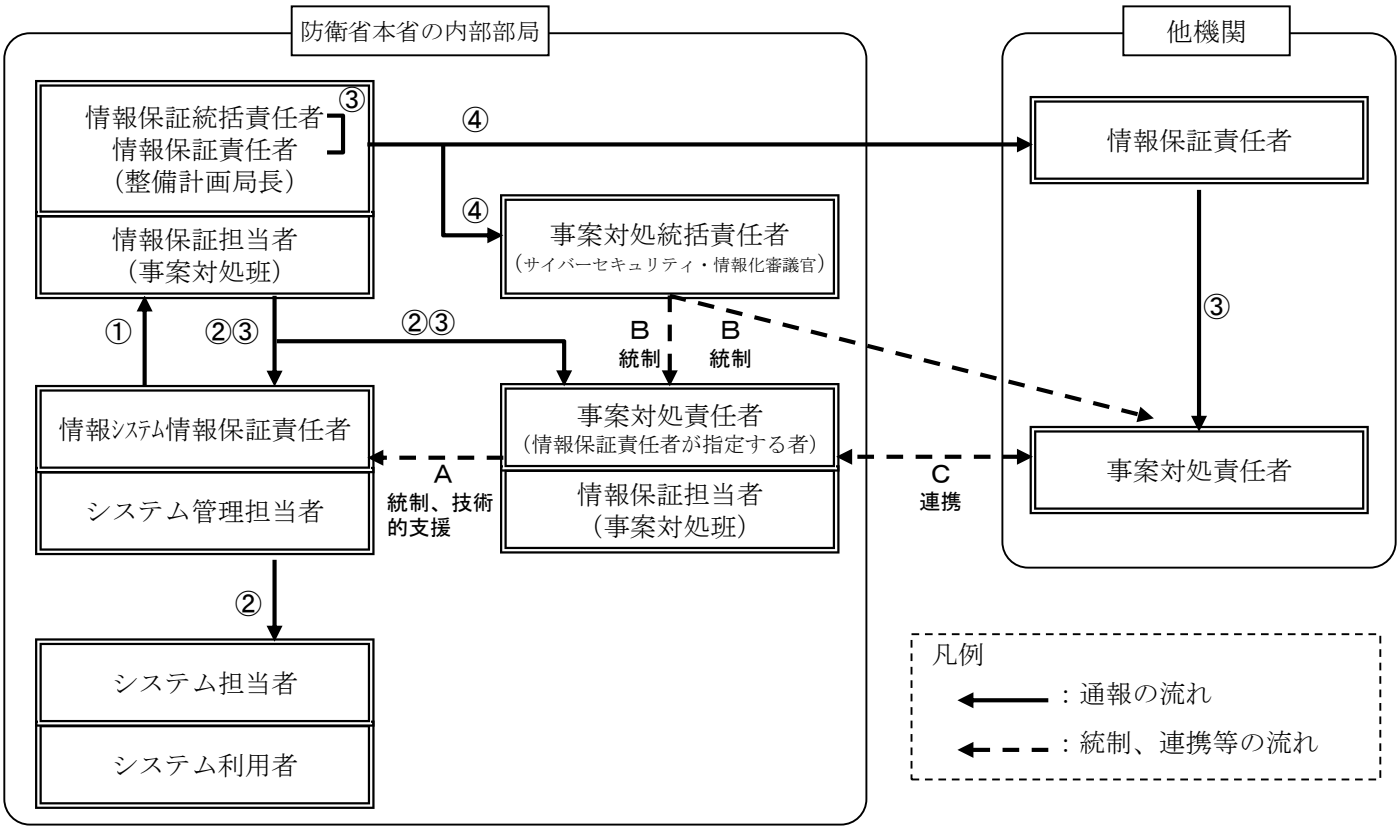
イ　システム利用者の作業が必要な場合には、システム担当者又はシステム利用者に所要の作業を実施させることができる。

（3）情報システム情報保証責任者及びシステム管理担当者は、情報システムの復旧が終了した場合には、事案対処責任者及び情報保証担当者に報告するものとする。

８　インシデント対応能力に対する評価

システム管理担当者及びシステム利用者は、インシデント対応能力の評価について、訓令第５１条第２項及び運用通達第１２第１項に規定する自己点検において実施させるものとする。

事案対処系統図（未然防止のための措置）



通報の流れ

①運用通達第１１第２項第２号

情報システム情報保証責任者は、セキュリティ情報を入手した場合には、情報保証責任者に通報するものとする。

②運用通達第１１第２項第３号

情報保証責任者は、セキュリティ情報を入手した場合又は前号の通報を受けた場合には、必要に応じ、情報システム情報保証責任者、事案対処責任者その他の関係職員に周知するものとする。

③運用通達第１１第２項第４号

情報保証責任者は、セキュリティ情報のうち、次に掲げる被害のいずれかの兆候を認知した場合又は他の機関等の情報システムに影響を及ぼすおそれがあると認めるセキュリティ情報を入手した場合には、情報システム情報保証責任者及び事案対処責任者に通報するとともに、情報保証統括責任者に通報するものとする。

・不正アクセス　・ホームページの改ざん　・サービス不能攻撃
・コンピュータ・ウイルス等のうち広範囲な情報システムに重大な影響を及ぼすおそれのあるもの
・情報システムに係る情報の窃盗、流出又は改ざん　・その他情報システムに係る犯罪、不正行為等

④運用通達第１１第２項第５号

情報保証統括責任者は、前号の通報を受けた場合には、他の機関等の情報保証責任者及び事案対処統括責任者に通報するものとする。

統制、連携等の流れ

A　訓令第４８条第４項

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。

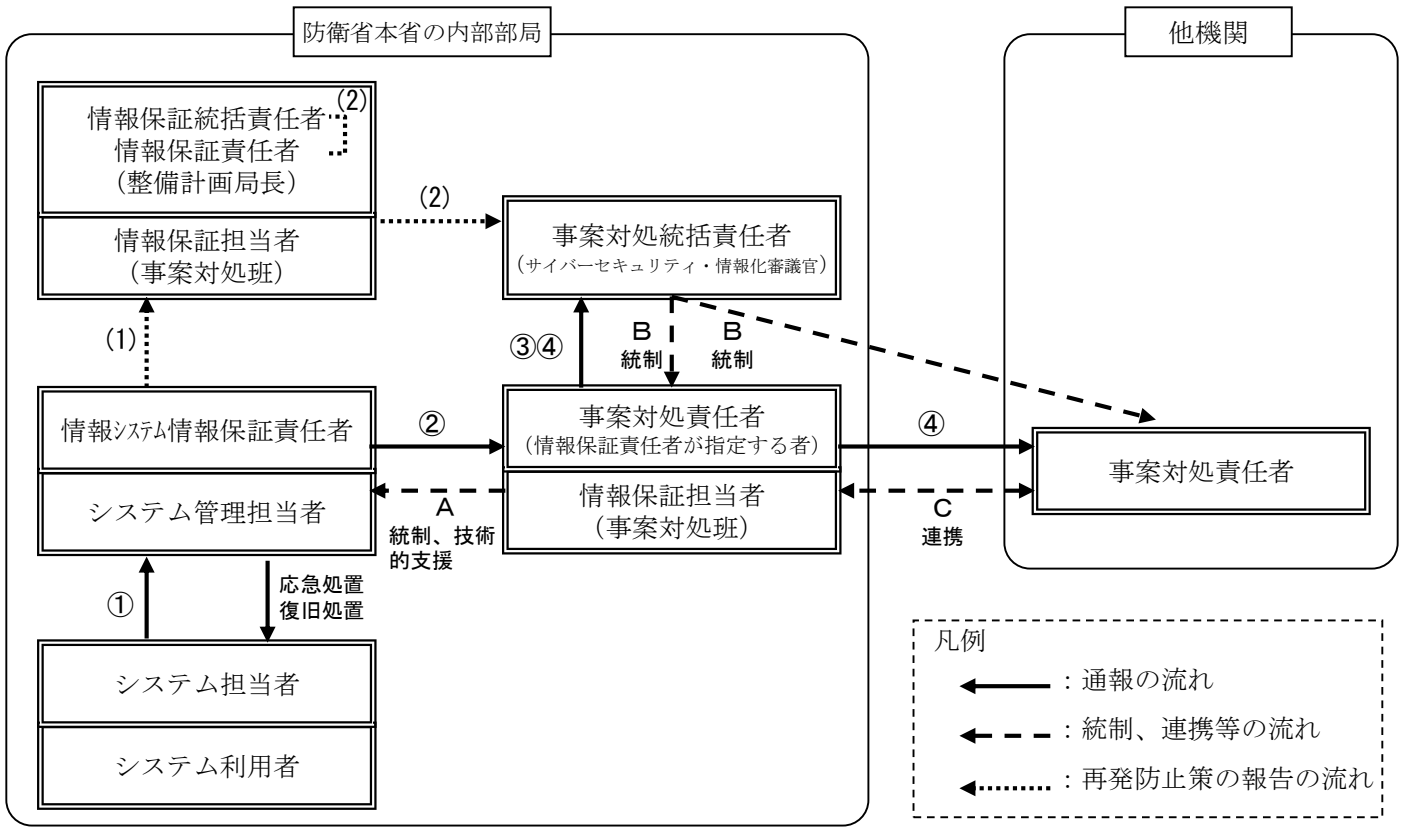
B　訓令第４８条第５項

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。

C　運用通達第１１第２項第７号

事案対処責任者は、第４号の通報を受けた場合には、他の機関等の事案対処責任者と連携して対処するものとする。

事案対処系統図（サイバー攻撃等発生時の措置）



通報の流れ

①運用通達第１１第３項第１号
職員は、サイバー攻撃等が発生したことを検知した場合には、速やかに情報システム情報保証責任者に通報するものとする。

②運用通達第１１第３項第２号
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ことを検知した場合又は前号の通報を受けた場合には、事案対処責任者に通報するものとする。

③運用通達第１１第３項第３号
事案対処責任者は、前号の通報を受けた場合には、事案対処統括責任者に通報するものとする。

④運用通達第１１第３項第４号
事案対処責任者は、前号の通報を受けた場合において、第２項第４号①から⑤までに掲げる被害が発生している場合又はサイバー攻撃等が他の機関等の情報システムに影響を及ぼすおそれがあると認める場合には、事案対処統括責任者に通報するとともに、他の機関等の事案対処責任者に通報・・・するものとする。

統制、連携等の流れ

Ａ　訓令第４９条第２項
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。

Ｂ　訓令第４９条第３項
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。

Ｃ　運用通達第１１第３項第４号
事案対処責任者は、前号の通報を受けた場合において、第２項第４号①から⑤までに掲げる被害が発生している場合又はサイバー攻撃等が他の機関等の情報システムに影響を及ぼすおそれがあると認める場合には、・・・他の機関等の事案対処責任者に通報し、連携して対処するものとする。

再発防止策の報告の流れ

(1)　運用通達第１１第３項第５号
情報システム情報保証責任者は、サイバー攻撃等により重大な被害が生じた場合には、各種情報保証対策の改善等再発防止に必要な事項を情報保証責任者に報告しなければならない。

(2)　運用通達第１１第３項第６号
情報保証責任者は、前号の報告を受けた場合には、必要に応じ、報告の内容について事案対処統括責任者及び情報保証統括責任者に通知するものとする。