防運情第９２４８号
１９．９．２０
一部改正　防運事第９２４４号
２１．７．３１
一部改正　防運情第７０３４号
２２．５．２８
一部改正　防運情第１０１２２号
２２．８．９
一部改正　防運情第６０６７号
２６．４．２５
一部改正　防運情第１８２１９号
２６．１２．１０
一部改正　防官文(事)第１８号
２７．１０．１
一部改正　防整情(事)第１６４号
２８．３．３１
一部改正　防整情(事)第９２号
令和５年３月３１日
一部改正　防整情(事)第２２９号
令和５年６月２８日

大臣官房長
各局長
各防衛参事官
衛生監
技術監
施設等機関の長
各幕僚長
情報本部長
技術研究本部長
装備施設本部長
防衛監察監
各地方防衛局長
殿

事務次官

防衛省の情報保証に関する訓令の運用について（通達）

標記について、下記のとおり定め、平成２０年１月１日から施行することとされたので、管下の職員に周知せられ、この実施に遺漏のないよう期せられたい。

なお、防衛省の情報保証に関する訓令の運用について（防官情第３２０３号。１６．３．３０）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について（防防調第４３６１号。１８．４．２８）は、平成１９年１２月３１日限り廃止する。

記

第１　総則（第１章関係）

１　この通達において使用する用語は、特別の定めのある場合を除くほか、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。）において使用する用語の例による。

２　定義について(第２条関係)

訓令第２条第１０号に規定する業務用データには、次に掲げるものが含まれる。

(1) 秘密電子計算機情報（秘密保全に関する訓令（平成１９年防衛省訓令第３６号）第１４条に定める秘密電子計算機情報をいう。以下同じ。）

(2) 特定秘密電磁的記録（特定秘密の保護に関する訓令（平成２６年防衛省訓令第６４号）第２条に定める特定秘密電磁的記録をいう。以下同じ。）

(3) 特別防衛秘密電子計算機情報（特別防衛秘密の保護に関する訓令（平成１９年防衛省訓令第３８号）第１３条に定める特別防衛秘密電子計算機情報をいう。以下同じ。）

(4) 注意電子計算機情報（取扱い上の注意を要する文書等及び注意電子計算機情報の取扱いについて（防防調第４６０８号。１９．４．２７）第８に定める注意電子計算機情報をいう。以下同じ。）
(5) 個人情報電磁的記録（防衛省本省における保有個人情報等の安全管理等に関する訓令の実施について（防官文第６１７４号。令和４年３月３０日）第１７第１項に定める個人情報電磁的記録をいう。以下同じ。）

３　適用除外について（第３条関係）
(1) 適用除外を申請する情報保証責任者は、次に掲げる事項を記載し、又は記録した申請書を情報保証統括責任者に提出すること。
①　適用除外を申請する情報システムの名称
②　適用除外とする訓令の該当箇所
③　適用除外とする期間
④　適用除外とする措置内容（講ずる代替手段等）
⑤　適用除外とすることにより生じる情報保証上の影響と対処方法
⑥　適用除外を終了した旨の報告方法
⑦　適用除外を申請する理由
(2) 情報保証統括責任者は、前号の申請書により申請を受けた場合、その内容を審査し、当該審査の結果を、次に掲げる事項を記載し、又は記録した通知書により、前号の情報保証責任者に通知する。
①　許可又は不許可の別
②　許可又は不許可の理由
③　適用除外を許可した訓令の該当箇所
④　適用除外を許可した期間
⑤　許可した措置内容（講ずるべき代替手段等）
⑥　適用除外を終了した旨の報告方法

第２　組織及び体制について（第２章関係）

１　情報保証統括アドバイザーについて（第４条の２関係）
情報保証統括責任者は、情報保証統括アドバイザーを置くに当たり、その業務の内容を明確化し、技術的知見その他の情報保証に関する知見を考慮の上行うものとする。

２　情報保証監査責任者補助者について（第６条の２関係）
(1) 情報保証監査責任者は、情報保証監査責任者補助者（以下この項にお

いて「補助者」という。）を指定する場合には、補助者ごとにその業務の内容を明確化するものとする。

(2) 情報保証監査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など、指定しようとする者の有する知見を考慮の上行うものとする。

3　情報システム情報保証責任者補助者について（第７条関係）

(1) 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（以下この項において「補助者」という。）を指定する場合には、補助者ごとにその業務の内容を明確化するものとする。

(2) 情報システム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など、指定しようとする者の有する知見を考慮の上行うものとする。

4　部隊等情報保証責任者補助者について（第８条関係）

(1) 部隊等情報保証責任者は、部隊等情報保証責任者補助者（以下この項において「補助者」という。）を指定する場合には、補助者ごとにその業務の内容を明確化するものとする。

(2)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など、指定しようとする者の有する知見を考慮の上行うものとする。

5　情報システム情報保証認証者補助者について（第９条関係）

(1) 情報システム情報保証認証者は、情報システム情報保証認証者補助者（以下この項において「補助者」という。）を指定する場合には、補助者ごとにその業務の内容を明確化するものとする。

(2) 情報システム情報保証認証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など、指定しようとする者の有する知見を考慮の上行うものとする。

6　情報保証対策委員会について（第１２条関係）

(1) 情報保証責任者は、情報保証対策委員会（以下「委員会」という。）

の委員を指定した場合には、委員長に通知するものとする。

(2) 委員長は、委員会の議事内容を情報保証統括責任者、事案対処統括責任者及び事案対処責任者に通知するものとする。

(3) 委員は、委員会における調整、連絡、検討及び審議の結果を情報保証責任者に報告するものとする。

(4) この通達に定めるもののほか、委員会の運営に関し必要な事項は、委員長が定める。

第３　情報システムの整備等に当たっての対策について（第３章第１節関係）

１　認証機能について（第１３条関係）

情報システム情報保証責任者は、情報システムに認証機能を設けるに当たっては、認証機能の実効性を確保するため、次に掲げる機能を情報システムに整備するものとする。

①　情報システムを利用するに先立ち、情報システムの利用者に付与されたユーザ名及びこれに対応する認証情報に基づいて、当該利用者が情報システムの利用に関し正当な権限を有していることを確認できる機能

②　認証情報等の付与等認証機能の設定を行える者を特定の者に限定できる機能

③　認証情報等の不正な使用に対応できる機能

④　その他情報システムの特性に応じ必要な機能

２　アクセス制御機能について（第１４条関係）

(1) 情報システム情報保証責任者は、アクセス可能なネットワーク及びネットワークサービスがある場合には、ネットワークごとにアクセスできる者を限定するよう、情報システムの設定を行うものとする。

(2) 前号に定めるもののほか、情報システム情報保証責任者は、情報システムにアクセス制御機能を設けるに当たっては、アクセス制御機能の実効性を確保するため、次に掲げる機能を情報システムに整備するものとする。

①　電子計算機情報のうち利用を制限すべき情報について、当該情報にアクセスすることに関し正当な権限を有している利用者のみにアクセスを認める機能

②　アクセス制御の設定を行える者を特定の者に限定できる機能

③　その他情報システムの特性に応じ必要な機能

３　証跡管理機能について（第１５条関係）

情報システム情報保証責任者は、情報システムに証跡管理機能を設けるに当たっては、証跡管理機能の実効性を確保するため、次に掲げる機能を情報システムに整備するものとする。

①　証跡として記録すべき事項を適切に選択し、及び記録できる機能

②　証跡を不正な消去、改ざん、アクセス等から保護する機能

③　その他情報システムの特性に応じ必要な機能

４　暗号化機能について（第１６条関係）

情報システム情報保証責任者は、情報システムに暗号化機能を設けるに当たっては、暗号化機能の実効性を確保するため、次に掲げる機能を情報システムに整備するものとする。

①　秘密電子計算機情報、特定秘密電磁的記録又は特別防衛秘密電子計算機情報を取り扱う情報システムについては、秘密電子計算機情報、特定秘密電磁的記録又は特別防衛秘密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暗号化することができる機能

②　注意電子計算機情報又は個人情報電磁的記録を取り扱う情報システムについては、注意電子計算機情報又は個人情報電磁的記録を可搬記憶媒体に格納するに当たり暗号化することができる機能

③　その他情報システムの特性に応じ必要な機能

５　電子署名機能について（第１７条関係）

情報システム情報保証責任者は、情報システムに電子署名機能を設けるに当たっては、電子署名機能の実効性を確保するため、次に掲げる機能を情報システムに整備するものとする。

①　電子署名が付された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し、かつ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機能

②　その他情報システムの特性に応じ必要な機能

６　脆弱性対応のための機能等について（第１８条関係）

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するための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に当たっては、脆弱性対応の実効性を確保するため、次に掲げる措置を講ずるものとする。

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が有する脆弱

性への対応を行うこと
② ウイルス対策ソフトの導入等、コンピュータ・ウイルスその他の不正プログラム（以下「コンピュータ・ウイルス等」という。）への対応を行うこと
③ サーバで使用するソフトウェアについて、不要なソフトウェア及び不要な機能の稼働を停止すること
④ サーバからデータを送信する場合に、サービスの提供に不要なデータを送信しないよう設定すること
⑤ 電子メールサーバが電子メールの不正な中継を行わないよう設定すること
⑥ 情報システムがその利用者から文字列の入力を受ける場合には、当該文字列の入力により情報システムが本来予定していない動作をしないよう設定すること
⑦ 通信プロトコルを利用する通信機能を導入する場合には、本来予定しない通信プロトコルによる通信が行われないよう設定すること
⑧ ウェブサーバ等にサービス不能攻撃に対応するための機能を設けること
⑨ 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

7 情報システムの特性に応じた機能等について（第１９条関係）
(1) 情報システム情報保証責任者は、情報システムの特性上、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（以下「ＶＰＮ等」という。）を利用して情報システムを整備する場合には、情報保証責任者の許可を得て、ＶＰＮ等経由でアクセスすることが可能な通信回線の範囲の制限、ＶＰＮ等への接続方法をみだりに知られないよう措置すること等必要な措置を講ずるものとする。
(2) 前号に定めるもののほか、情報システム情報保証責任者は、情報保証統括責任者が定めるセキュリティ管理策に従い、情報システムの特性、運用環境等に応じ、情報保証を確保するために必要な機能等を設けるとともに、情報システムの運用、管理等に当たっての措置を講ずるものとする。

8 情報システムの動作確認等について（第２０条関係）
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に当たっては、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を確認するほか、当該ソフトウェアについて次に掲げる事項を確認するものとする。

①　正当なライセンスを有するものであること

②　コンピュータ・ウイルス等が含まれていないこと

9　情報システム間の接続について（第２１条関係）

(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情報システムの情報システム情報保証責任者は、当該情報システムのリスク分析・評価に際して他の情報システムと接続する場合のリスクを含めて評価するとともに、必要に応じて当該情報システムに適用するセキュリティ管理策の見直しを行うものとする。

(2) 他省庁が整備した情報システム（以下「他省庁システム」という。）と接続する情報システムの情報システム情報保証責任者は、当該情報システムのリスク分析・評価に際して他省庁システムと接続する場合のリスクを含めて評価するとともに、必要に応じて当該情報システムに適用するセキュリティ管理策の見直しを行うものとする。

(3) 訓令第２１条第２項第３号に定める防衛大臣の承認は、当該承認に係る情報システムの換装を行ったとき及び当該承認に係る接続における情報保証上の対策の強度に影響を及ぼすと認められる情報システムの変更を行ったときには、再度行われなければならない。

(4) 情報システムを防衛省が保有するその他の情報システムと接続しようとする場合においては、これらの情報システム（これらの情報システムと既に接続している情報システムを含む。以下この項において同じ。）の情報システム情報保証責任者は、あらかじめ、これらの情報システムにおいて取り扱われる秘密電子計算機情報若しくは特定秘密電磁的記録の保全又は注意電子計算機情報若しくは個人情報電磁的記録の取扱いの責任の所在その他の管理に関する必要な事項について、協議により定めるものとする。この場合において、これらの情報システムを異なる情報保証責任者が管理するときは、当該情報保証責任者が協議をして定めるところによるものとする。

(5) 情報システム情報保証責任者は、秘密電子計算機情報、特定秘密電磁的記録、注意電子計算機情報かつ個人情報電磁的記録を扱わない情報システムにおいて、インターネット及び他のネットワークへのアクセスを可能とする仕組みを構築する場合は、情報保証責任者の許可を得なければならない。

１０　外部サービスの利用について（第２１条の２関係）

(1) 外部サービスのうち、事業者によって定義されたインターフェースを

用いた、拡張性及び柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報保証に関する十分な条件設定の余地のあるもの（以下「クラウドサービス」という。）を利用するに当たっては、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和２年１月３０日サイバーセキュリティ戦略本部決定）に基づき運営されている、政府情報システムにおけるセキュリティ評価制度において登録されたサービスから調達することを原則とする。

(2) 情報システム情報保証責任者は、前号の登録がないクラウドサービスを調達する場合は、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示した上で、情報保証責任者を通じて情報保証統括責任者に申請し、承認を得るものとする。

１１　情報システムの設置場所について（第２２条関係）

(1) 情報システム情報保証責任者は、情報システムを情報システム室に設置する場合には、情報システム室への侵入等を防止するため、次に掲げる措置を講ずるものとする。

①　必要に応じ、情報システム室から外部に通ずる全てのドアに、開閉制御装置、開放防止装置を設置すること等により、許可されない者の立入りを防止するための対策を行うこと

②　必要に応じ、情報システム室に防犯カメラ等の監視機能を設置すること

③　必要に応じ、情報システム室に漏えい電磁波対策を行うこと

(2) 情報システム情報保証責任者は、ネットワークの接続口（ハブのポート等）及び通信回線を設置する場合には、床下に配線を設ける等、必要に応じて設置場所を秘匿し、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、情報システムを災害による影響から保護するに当たっては、次に掲げる措置を講ずるものとする。

①　必要に応じ、耐震対策を講じた場所に情報システムを設置すること

②　必要に応じ、防火措置を講じた場所に情報システムを設置すること

③　必要に応じ、情報システムに予備電源を備えること

④　必要に応じ、情報システムを落雷等の過電流から保護すること

⑤　必要に応じ、情報システムを水、埃、振動、落下物等から保護する

こと

⑥　その他情報システムを災害の影響から保護するための措置を必要に応じ行うこと

１２　情報システムセキュリティ台帳の整備について（第２５条関係）

情報システムセキュリティ台帳は、次の事項を含むものとする。

(1) 情報システム名

(2) 情報システム情報保証責任者の氏名及び連絡先

(3) システム構成

(4) 接続する部外回線の種別

(5) 機密性、完全性及び可用性の区分

(6) 適用するセキュリティ管理策

第４　運用承認について（第３章第２節関係）

１　別に定める情報システムについて（第２６条関係）

(1) 訓令第２６条第１項の別に定める情報システムは、次のとおりとする。

①　次に掲げる情報システムであって、他の情報システム又はネットワークと接続しないもの（装備品の維持整備等のために一時的に他の情報システム又はネットワークと接続する情報システムであってリスク管理が適切に行われていると情報保証責任者が認めるものを含む。）

ア　火器管制装置等に用いられる装備品及びその支援用機材に組み入れられる情報システム

イ　機器の数値制御を行う目的で装備品に組み込まれている情報システム

ウ　装備品の研究開発のための試作品及び装備品の研究開発のため試験的に使用される機材に組み入れられる情報システム

②　前号アからウまでに掲げるもの以外の情報システムであって、業務用データを取り扱わないもの

③　携帯電話（スマートフォンを含む。）

(2) 前号に掲げる情報システムであっても、リスク分析・評価を実施するものとする。仕様検討段階においては、運用承認時リスク評価報告書を作成し情報システム情報保証認証者の評価を経るものとし、情報システム情報保証認証者から改善指示があった場合はリスク評価報告書を見直すものとする。

２　情報システムを新たに整備する場合における運用承認申請文書の作成について（第２６条関係）

(1) 情報システム情報保証責任者は、情報システムを整備する際には、リスク分析・評価（脆弱性検査を含む。）を実施し、その結果を記載した運用承認時リスク評価報告書を作成するものとする。ただし、仕様検討段階においては、情報システムは実装されていないことから、脆弱性検査は行わないものとする。

(2) 情報システム情報保証責任者は、前号の運用承認時リスク評価報告書を踏まえ、当該情報システムを機密性、完全性及び可用性の観点から高、中又は低に分類（以下「セキュリティ分類」という。）するとともに、当該情報システムに適用するセキュリティ管理策を決定し、セキュリティ計画書を作成するものとする。

(3) 情報システム情報保証責任者は、当該情報システムの運用開始後も適用された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に継続監視計画書を作成するものとする。

(4) 情報システム情報保証責任者は、情報システム情報保証認証者が作成するセキュリティ評価文書を踏まえ、当該情報システムに実装しているセキュリティ上の管理項目について、必要な改善策を講じていくために将来対応計画書を作成するものとする。

３　他の情報システムと接続する情報システムの運用承認申請文書の作成について（第２６条関係）

(1) 情報システム情報保証責任者は、運用承認を受けた後に他の情報システムと接続して運用することを予定している情報システム（以下「接続運用する情報システム」という。）について運用承認申請文書を作成する場合には、接続先の情報システムの情報システム情報保証責任者（以下「接続先の情報システム情報保証責任者」という。）に対し、運用承認申請文書の作成に必要な資料の提出を求めることができる。この場合において、接続先の情報システム情報保証責任者は、これに協力しなければならない。

(2) 情報システム情報保証責任者は、接続運用する情報システムについて運用承認申請文書を作成した場合には、情報システム情報保証認証者に提出するに先立ち、接続先の情報システム情報保証責任者に当該運用承認申請文書を送付するものとする。

(3) 前号の規定に基づき運用承認申請文書の送付を受けた接続先の情報シ

ステム情報保証責任者は、運用承認申請文書の内容について、当該運用承認申請文書を作成した情報システム情報保証責任者に意見を提出することができる。この場合において、運用承認申請文書を作成した情報システム情報保証責任者は、意見を提出した接続先の情報システム情報保証責任者と、当該意見に関する対応について協議を行うものとする。

4　運用承認申請文書の認証等について（第２６条関係）

(1) 情報システム情報保証認証者は、情報システムの運用を認証するに当たり、必要に応じて実施する評価の種類に適した情報システム情報保証認証者補助者を選定することができる。

(2) 情報システム情報保証認証者は、情報システムの運用を認証するに当たり、必要に応じて運用承認申請文書の修正を求めることができる。この場合において、情報システム情報保証責任者は、情報システム運用者の意見を聴いた上で、速やかに運用承認申請文書を修正し、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、前号の規定に基づき運用承認申請文書の修正を求めた場合であっても、情報システムの運用に制限を課することにより当該情報システムを暫定的に運用することが可能であると認める場合には、同号の規定に基づき修正された運用承認申請文書が提出されるのを待たずに、修正前の情報システムの運用を暫定的に認証（以下「暫定認証」という。）することができる。この場合において、情報システム情報保証認証者は、認証結果報告書に必要となる運用制限を付記し、実施計画とあわせて情報システム情報保証責任者に提出するものとする。

(4) 情報保証責任者は、前号の規定に基づき暫定認証された段階における運用承認申請文書の提出を受けた場合において、当該暫定認証が適切であると認めるときは、１年以内の暫定運用期間を定めて、情報システムの運用承認を行うことができる。この場合において、情報システム情報保証責任者は、当該暫定運用期間内に、第２号の規定に基づき修正した運用承認申請文書を添えて情報システム情報保証認証者の認証を受けなければならない。

(5) 情報システム情報保証責任者は、やむを得ない事情により前号の暫定運用期間内に運用承認申請文書を修正できない場合には、情報システム情報保証認証者を経由して、情報保証責任者に対し、暫定運用期間の延長を申請することができる。

(6) 情報保証責任者は、前号の申請があった場合には、１年以内の期間を定めて、暫定運用期間を延長することができる。この場合において、暫定運用期間の延長は、２回を超えて行うことはできない。
(7) 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の様式は、情報保証統括責任者が定める。

５　運用承認実績の報告等について（第２６条の２関係）
(1) 訓令第２６条の２の報告及び提出は、毎年度１回、５月末日までに行うものとする。
(2) 訓令第２６条の２の運用承認結果報告書の様式は、情報保証統括責任者が定める。

６　情報保証統括責任者への報告等について（第２６条の２関係）
情報保証統括責任者は、運用承認前の各情報システムのリスク管理を一元的に行うことを目的として、情報保証責任者に対し、管理する情報システムの運用承認申請文書及びセキュリティ評価文書について、随時提出することを求めることができるものとする。

第５　情報システムの運用、管理等に当たっての対策について（第３章第３節関係）

１　リスク分析・評価について（第２７条の２関係）
(1) 情報システム情報保証責任者は、運用承認を必要とする情報システムを対象とし、情報システムの製造が完了し実際の運用環境と同等の環境となってから運用開始後１年を経過するまでの間に、少なくとも１回はリスク分析・評価の一環として脆弱性検査を実施するものとする。また、１回目の脆弱性検査から２年を経過した後に再度脆弱性検査を実施するものとする。
(2) 情報保証統括責任者は運用中の各情報システムのリスク管理を一元的に行うことを目的として、情報保証責任者に対し、管理する情報システムのリスク評価報告書について、随時提出することを求めることができるものとする。

２　認証情報等の管理について（第２８条関係）
(1) 情報システム情報保証責任者は、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（以下「認証情報等」という。）を

付与するに当たっては、認証が有効に行われるよう、次に掲げる措置を講ずるものとする。

① 認証情報等を付与すべき相手方を特定すること

② 認証情報等の付与を行える者を特定の者に限定すること

③ 認証情報等を付与すべき相手方に対してのみ確実に付与するとともに、認証情報等の管理を適切に行うこと

④ 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) 情報システム情報保証責任者は、認証情報等が不正に使用され、又はそのおそれがあると認めたときは、直ちに必要な措置を講じなければならない。

(3) 職員は、認証情報等の管理を行うに当たっては、次に掲げる措置を講ずるものとする。

① 認証情報等を不正に使用しないこと

② 認証情報等を他人に不正に使用されないようにすること

③ その他情報システム情報保証責任者が定める事項を遵守すること

(4) 職員は、認証情報等が不正に使用され、又はそのおそ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に届け出なければならない。

3 アクセス制御について（第２９条関係）

(1) 情報システム情報保証責任者は、部外からのアクセスを許可する場合には、情報保証責任者の許可を得るとともに、次に掲げる事項を遵守しなければならない

① アクセスの許可は、部外からのアクセスを処理するサーバに対してのみとし、直接部内のネットワークに対する接続の許可をしてはならないこと

② 部外からアクセスする者の真正性の確保ができなければならないこと

③ 遠隔地に情報システムがある場合には、安全なアクセスが可能となる制御を施さなければならないこと

④ 職員以外の者が情報システムの保守のために部外からアクセスすることを許可してはならないこと

(2) 前号に定めるもののほか、情報システム情報保証責任者は、アクセス制御機能を設けた場合には、アクセス制御が有効に行われるよう、次に掲げる措置を講ずるものとする。

① アクセス制御の対象となる防衛省の電子計算機情報及び当該情報にアクセスできる者を特定すること
② アクセス制御に関する設定を行える者を特定の者に限定すること
③ アクセス制御の対象となる防衛省の電子計算機情報について、当該情報にアクセスすべき者に対してのみ当該情報にアクセスする権限を付与すること
④ 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

(3) 職員は、アクセス制御に関し、次に掲げる措置を講ずるものとする。
① 防衛省の電子計算機情報のうち利用を制限すべき情報について、情報システムに設けられたアクセス制御機能によりアクセス制御を行うこと
② その他情報システム情報保証責任者が定める事項を遵守すること

4 証跡管理について（第３０条関係）

(1) 情報システム情報保証責任者は、証跡管理機能を設けた場合には、証跡管理が有効に行われるよう、次に掲げる措置を講ずるものとする。
① 証跡として記録すべき事項を適切に選択し、及び記録すること
② 証跡についてアクセス制御を行うこと
③ 証跡の分析を円滑に行えるよう情報システム内での時刻を同期すること
④ 証跡の保存期間を定め、当該期間が満了するまでの間はこれを適切に管理すること。また、保存期間が満了した後は証跡を確実に消去すること
⑤ 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) 情報システム情報保証責任者は、必要に応じてアクセス状況を監視するものとする。

(3) 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事項が明らかとなった場合には、必要な措置を講じなければならない。

5 暗号化について（第３１条関係）

(1) 情報システム情報保証責任者は、暗号化機能を設けた場合には、暗号化が有効に行われるよう、次に掲げる措置を講ずるものとする。
① 秘密電子計算機情報、特定秘密電磁的記録又は特別防衛秘密電子計算機情報を取り扱う情報システムについては、別に定めるところによ

り、秘密電子計算機情報、特定秘密電磁的記録又は特別防衛秘密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暗号化することができるよう設定すること

② 注意電子計算機情報又は個人情報電磁的記録を取り扱う情報システムについては、別に定めるところにより、注意電子計算機情報又は個人情報電磁的記録を可搬記憶媒体に格納するに当たり暗号化することができるよう設定すること

③ 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) 職員は、暗号化に関し、次に掲げる措置を講ずるものとする。

① 秘密電子計算機情報、特定秘密電磁的記録又は特別防衛秘密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、別に定めるところにより暗号化する場合には、情報システムに設けられた暗号化機能により暗号化すること

② 注意電子計算機情報又は個人情報電磁的記録を可搬記憶媒体に格納するに当たり、別に定めるところにより暗号化する場合には、情報システムに設けられた暗号化機能により暗号化すること

③ その他情報システム情報保証責任者が定める事項を遵守すること

6 電子署名について（第３２条関係）

(1) 情報システム情報保証責任者は、電子署名機能を設けた場合には、電子署名が有効に行われるよう、次に掲げる措置を講ずるものとする。

① 必要に応じて電子署名を付することができるよう設定すること

② 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すること

③ 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) 職員は、電子署名に関し、次に掲げる措置を講ずるものとする。

① 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、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こと

② その他情報システム情報保証責任者が定める事項を遵守すること

7 脆弱性対応について（第３３条関係）

(1) 情報システム情報保証責任者は、情報システムの脆弱性対応が有効に行われるよう、次に掲げる措置を講ずるものとする。

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 ①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他の情報システム情報保証責任者等と共有すること

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) 職員は、情報システムの脆弱性対応に関し、次に掲げる措置を講ずるものとする。

① 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すること

② 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・ウイルス等の感染防止に努めること

③ その他情報システム情報保証責任者が定める事項を遵守すること

8 情報システム室の入退室管理について（第３４条関係）

情報システム情報保証責任者は、情報システム室の入退室管理が適切に行われるよう、次に掲げる措置を講ずるものとする。

① 情報システム室の入退室を許可された者に限定すること

② 情報システム室内で身分証明書を装着させること等により、入退室を許可された者であることが外見上明らかとなる措置を講ずること

③ 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

9 情報システムの盗難防止について（第３５条関係）

(1) 情報システム情報保証責任者は、可搬型の情報システム（次項により許可を得て持ち出されているものを除く。）については、ワイヤーで机

等に固定の上当該ワイヤーを施錠し、又はワイヤーで机等に固定することが困難な場合には、情報システムを使用しないときにロッカー等に保管の上これを施錠するものとする。

(2) 前号において使用するワイヤー又はロッカー等のかぎは、情報システム情報保証責任者が指定する者が管理するものとする。

(3) 前２号に規定するもののほか、情報システム情報保証責任者は、情報システムを設置している事務室等に職員がいない場合には事務室等を施錠すること等により、情報システムの盗難を防止するための措置を講じなければならない。

１０　情報システムの持ち出しについて（第３５条関係）

(1) 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、持ち出しの都度、情報システム情報保証責任者の許可を得なければならない。ただし、あらかじめ期間を定めて許可を得た場合を除く。

(2) 職員は、持ち出し先において情報システム情報保証責任者が定めた方法以外で外部ネットワークに接続してはならない。

(3) 情報システム情報保証責任者は、情報システムの持ち出しを許可した場合には、情報システムの管理のための文書に持ち出し先、持ち出し期間等を記録することにより、適切に管理しなければならない。

(4) 職員は、情報システムの持ち出し先で盗難防止に努めなければならない。

１１　情報システムの変更について（第３６条関係）

情報システム情報保証責任者は、職員から、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について許可を求められた場合には、情報システムの情報保証を確保する上で問題がないことを確認しない限り、これを許可してはならない。

１２　職員以外の者による情報システムの利用について（第３９条関係）

情報システム情報保証責任者は、職員以外の者が情報システムを使用する場合においては、情報保証を確保するため職員に監督させるなど必要な措置を講じなければならない。

１３　情報システムの障害発生時の措置等について（第４０条関係）

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おいて当該障害の記録を作成するに当たっては、職員から報告のあった情

報、情報システムの障害に対する処理、処置上の問題点等についての記録を行うものとする。

第６　情報システムの廃棄等に当たっての対策について（第３章第４節関係）

情報システム情報保証責任者は、情報システムの廃棄、返却等を行う場合には、必要に応じ当該情報システムに保存された防衛省の電子計算機情報の複製を作成するとともに、物理的な破壊その他の方法により情報システムに保存された防衛省の電子計算機情報を復元不可能な状態にしなければならない。

第７　防衛省の目的特化型機器に係る対策について（第４章関係）

(1) 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、機器ごとに名称、設置場所、使用者名等を記載した管理簿を設け、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の特性に応じて、以下を含む対策を講ずることとする。ただし、使用している目的特化型機器の機能上の制約により講ずることができない対策を除く。

①　認証情報を初期設定から変更した上で、適切に管理する。

②　目的特化型機器にアクセスする主体に応じて必要な権限を割り当て、管理する。

③　目的特化型機器が備える機能のうち利用しない機能を停止する。

④　インターネットと通信を行う必要のない目的特化型機器については、当該目的特化型機器をインターネット及びインターネットに接点を有する情報システムに接続しない。

⑤　目的特化型機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。

⑥　目的特化型機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップ、セキュリティパッチの適用、アクセス制御等の対策を講ずる。

⑦　目的特化型機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。

⑧　目的特化型機器を廃棄する場合は、目的特化型機器に保存されているデータを抹消する。

第８　防衛省の可搬記憶媒体に係る対策について（第５章関係）

(1) 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、情報システムに挿入又は接続する場合及び業務用データを取り扱う場合については、使用者名等を記載した管理簿を設け、管理し、集中保管するものとする。ただし、次に掲げる条件のいずれかに該当する場合は、適切に管理するものとし管理簿へ記載する必要はない。

①　第１２号の規定に基づき管理を行う可搬記憶媒体

②　業務用データが保存されておらずかつ新たに電子計算機情報を保存できないことを部隊等情報保証責任者が確認した可搬記憶媒体

③　電子計算機情報を追記可能で未使用の可搬記憶媒体

(2) 部隊等情報保証責任者は、管理簿に記載した防衛省の可搬記憶媒体について、管理簿に記載された可搬記憶媒体であることが分かるように表示をしなければならない。

(3) 部隊等情報保証責任者は、第１号の管理簿に記載した可搬記憶媒体を保管する容器を原則１か所に設置し適切に管理するものとする。ただし、部隊等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、別に保管する容器を設置することができる。その際、部隊等情報保証責任者は、部隊等情報保証責任者補助者を指定し、管理を分任するものとする。

(4) 職員は、防衛省の可搬記憶媒体を使用する場合は、コンピュータ・ウイルス等の感染の無いことを確認し、コンピュータ・ウイルス等の感染が確認されたときは、コンピュータ・ウイルス等が駆除されない限り使用してはならない。

(5) 職員は、管理簿に登録された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、持ち出しの都度、管理簿に記録しなければならない。

(6) 職員は、管理簿に登録された可搬記憶媒体を職場から持ち出す場合には、その都度、部隊等情報保証責任者の許可を得なければならない。

(7) 情報保証責任者は、業務上必要と認める場合、防衛省が管理する区域内において、第５号に示す記録をもって職員が管理簿に登録された可搬記憶媒体を職場から持ち出すことができる区域を定めることができる。

(8) 職員は、前号で定められた区域に管理簿に登録された可搬記憶媒体を持ち出す場合、第５号に示す記録をもって足りる。

(9) 部隊等情報保証責任者は、第６号の許可を求められた場合には、当該

可搬記憶媒体に持ち出し先で業務上必要となる電子計算機情報以外の電子計算機情報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目的以外に複製しないことを指導すること等により、情報保証を確保するために必要な措置の実施を確認しない限り、当該可搬記憶媒体の持ち出しを許可してはならない。

(10)部隊等情報保証責任者は、第１号の管理簿に持ち出し先、持ち出し期間等を記録することにより、可搬記憶媒体の持ち出しを適切に管理しなければならない。

(11)部隊等情報保証責任者は、可搬記憶媒体にコンピュータ・ウイルス等の感染が確認されたときは、コンピュータ・ウイルス等の駆除をした後に使用するものとする。また、コンピュータ・ウイルス等の駆除が不可能な場合、当該可搬記憶媒体にコンピュータ・ウイルス等に感染したことが分かるように表示するなど感染防止の措置を講ずるものとする。

(12)防衛省の可搬記憶媒体が、秘密保全に関する訓令の解釈及び運用について（防防調第４６０７号。１９．４．２７）第２７若しくは第１１７の規定により登録されたものであるとき、又は特別防衛秘密の保護に関する訓令の解釈及び運用について（防防調（事）第３号。２７．１０．１）第１９の規定により取扱いの経過について記録されたものであるときは、秘密保全に関する訓令、特定秘密の保護に関する訓令又は特別防衛秘密の保護に関する訓令に基づき管理することで足りる。

第９　私有機器の取扱いについて（第６章関係）

１　訓令第４４条に規定する私有パソコンとは、各種ソフトウェアを用い、画面の大きさや液晶キーボードを備えるなどの操作性の高さから、資料作成を容易に行うことができる多用途なコンピュータであって、防衛省が管理していないものをいう。

２　防衛大学校及び防衛医科大学校の学生による私有パソコンの取扱いは以下のとおりとする。

(1) 防衛大学校及び防衛医科大学校の情報保証責任者は、学生が私有パソコンを使用することにより学修の効率化が図られ、かつ、学生が私有パソコンを持ち込んでも業務用データに接することがないと認められる場所については、私有パソコンを持ち込める学修場所として指定することができる。

(2) 学生は私有パソコンを学修場所に持ち込む必要がある場合は、部隊等

情報保証責任者の許可を受けるものとする。

(3) 部隊等情報保証責任者は、前号の許可を求められた場合には、当該私有パソコンに業務用データが保存されていないことを確認するとともに、情報流出防止に関する教育等により、情報保証を確保するために必要な措置の実施を確認しない限り、私有パソコンの持ち込みを許可してはならない。

第１０　教育及び訓練について（第７章関係）

情報保証責任者は、職員に対する教育及び訓練を行うに当たっては、次に掲げる事項に留意しなければならない。

①　対象となる職員の職務に応じた教育及び訓練（情報システム情報保証責任者、情報システムの利用者の区分等）を実施すること

②　計画に基づく定期的な教育及び訓練を実施すること

③　適切な資料を活用した教育及び訓練を実施すること

第１１　サイバー攻撃等への対処について（第８章関係）

１　対処要領の策定について（第４７条関係）

情報保証責任者は、サイバー攻撃等に対処するための要領を定めるに当たっては、次に掲げる事項を定めるとともに、更新する都度関係する職員に周知するものとする。

①　機関等内での連絡体制

②　処置要領（情報システムや電子計算機をネットワークから切断すること等の応急処置、原因探求及び排除、証拠保全、復旧処置等）

③　情報収集、分析、配布要領

④　その他必要な事項

２　サイバー攻撃等の未然防止のための措置について（第４８条関係）

(1) 情報システム情報保証責任者は、サイバー攻撃等により情報システムに不正な変更等が行われていないかを定期的に確認するものとする。

(2) 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。

(3) 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。

(4) 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。

① 不正アクセス

② ホームページの改ざん

③ サービス不能攻撃

④ 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

⑤ 情報システムに係る情報の窃盗、流出又は改ざん

⑥ その他情報システムに係る犯罪、不正行為等

(5) 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。

(6) 情報保証統括責任者は、前号により通報する情報に、次の表の左欄に掲げる基準に従い同表右欄に掲げる重要性の指標を付記するものとする。

基　　準	重要性の指標
機関等におけるセキュリティ対策の参考となる情報	情　　報
機関等において適切な措置を講ずることが強く推奨される情報	注意喚起
機関等において直ちに適切な措置を講ずる必要がある情報	警　　報

(7) 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。

3　サイバー攻撃等の発生時の措置について（第４９条関係）

(1) 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) 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) 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) 事案対処責任者は、第２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ときは、前号の規定により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し、連携して対処するものとする。

(5) 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。

(6) 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。

(7) 訓令第４９条第３項の措置に関し、機関等の事案対処責任者は、事案対処統括責任者から助言、資料の提供等を求められた場合には、これに協力しなければならない。

４　連絡体制の整備について（第４８条及び第４９条関係）

整備計画局サイバー整備課長は、前２項に規定する各種措置に係る調整が円滑に行われるよう、機関等の担当者間の連絡体制を整備するものとする。

第１２　対策の実施状況の確認等について（第９章関係）

１　自己点検について（第５１条関係）

情報保証責任者は、職員に自己点検を行わせるに当たっては、自己点検の計画、点検項目、実施要領その他必要な事項を定め、職員に周知するものとする。

２　監査について（第５２条関係）

(1) 情報保証監査責任者は、次の区分により監査を行うものとする。

①　定期監査 監査実施計画書及び自己点検等の結果に基づいて、毎年度１回以上行う。

②　臨時監査 情報保証に関する問題点等を考慮の上、必要に応じて行う。

(2) 情報保証監査責任者は、監査を行うに当たっては、監査の対象となる部署とは異なる部署の職員に監査を行わせること等により、第三者的観点を確保するとともに監査の実効性を確保するための措置を講ずるものとする。

(3) 情報保証監査責任者は、運用承認の対象となる情報システムのうち、セキュリティ分類の完全性「高」に該当する情報システム及び情報システム情報保証責任者又は情報保証監査責任者が必要と認める情報システムを対象とし、情報システムの製造が完了し実際の運用環境と同等の環境となってから運用開始後１年を経過するまでの間に、少なくとも１回は侵入試験を実施するものとする。また、１回目の侵入試験から２年を経過した後に、再度侵入試験を実施するものとする。

(4) 情報保証統括責任者は、運用中の各情報システムのリスク管理を一元的に行うことを目的として、情報保証監査責任者に対し、管理する情報システムの監査結果報告書について、随時提出することを求めることができるものとする。

３　職員の私有パソコン等について（第５２条関係）

情報保証責任者は、職員から、私有機器で業務用データを取り扱っていない旨の誓約書を提出させるものとする。

４　特別監査について（第５３条関係）

(1) 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、特別監査の計画、特別監査の項目その他必要な事項を定めるものとする。

(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、特別監査の対象となる機関等とは異なる機関等の職員に特別監査を行わせること等により、第三者的観点を確保するとともに特別監査の実効性を確保するための措置を講ずるものとする。

(3) 情報保証監査責任者は、情報保証監査統括責任者から、特別監査を行う体制の整備、特別監査の実施日時の調整その他特別監査の円滑な実施に関し協力を求められた場合には、これに協力しなければならない。

(4) 情報保証監査統括責任者は、特別監査の結果について、情報保証統括責任者に通知するものとする。

５　職員による報告等について（第５４条関係）

(1) 情報保証責任者は、訓令第５４条第１項の報告を受けた場合には、遅滞なく情報保証統括責任者に通知するものとする。

(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の細部については、別紙のとおりとする。

第１３　委任規定

この通達の実施に関し必要な事項は、情報保証責任者が定める。

第１４　経過措置

１　この通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は、第３の規定は、この通達の施行の後に訓令別表第３の左欄に掲げる場合に該当することとなる場合に適用するものとし、それまでの間、なお従前の例による。

２　この通達の施行の際現に設計が終了している情報システムについては、第３の規定は、当該情報システムの運用を開始した後に訓令別表第３の左欄に掲げる場合に該当することとなる場合に適用するものとし、それまでの間、なお従前の例による。

３　第５第１項第１号及び第１２第２項第３号に定める脆弱性検査及び侵入試験の頻度について、この通達の施行の後から令和９年度末までの間において機関等における態勢整備の状況等により実施が困難である場合は、当該期間中に少なくとも１回は脆弱性検査及び侵入試験を実施するものとする。

４　この通達の施行の際現に運用している情報システムについては、脆弱性検査について、この通達の施行の後から３年以内に少なくとも１回は実施するものとする。

別紙

インターネット上への情報流出事案対応要領

１　目的

本要領は、インターネット上への情報流出事案判明時の対応を迅速かつ的確に行うため、全省的な対応要領について必要な事項を定めるものである。

２　連絡体制

(1) 各機関の長（防衛省本省の内部部局にあっては整備計画局長。以下同じ。）は、各機関において、この要領に従って事案対応を行う情報通信担当課及び秘密保全担当課を指定しておくものとする。

(2) 整備計画局サイバー整備課、防衛政策局調査課、各機関の情報通信担当課及び秘密保全担当課は、相互の連絡先を把握しておくものとする。

(3) 各機関の長は、職員に対し、第１号で指定した情報通信担当課及び秘密保全担当課の連絡先を周知徹底するものとする。

３　初動対応

(1) 職員は、インターネット上に業務関連情報が流出している事実を把握した場合、速やかに自己の所属する機関の情報通信担当課及び秘密保全担当課に通報するものとする。

(2) 通報を受けた情報通信担当課及び秘密保全担当課は、当該情報流出事案が自己の機関とは異なる機関で処理すべきと思慮する場合は、処理すべきと思慮する機関の情報通信担当課及び秘密保全担当課に通報し、その後、引き続き事案の処理に協力するものとする。

(3) 事案を担当する情報通信担当課（以下この要領において「情報通信事案担当課」という。）及び事案を担当する秘密保全担当課（以下この要領において「秘密保全事案担当課」という。）は、相互に連携し、流出した情報の把握を行うとともに、これと並行して、整備計画局サイバー整備課及び防衛政策局調査課に通報するものとする。

(4) 整備計画局サイバー整備課及び防衛政策局調査課は、前号の通報を受けた場合には、必要に応じ、情報通信事案担当課及び秘密保全事案担当課が属する機関以外の機関の情報通信担当課及び秘密保全担当課に、流出した情報の把握等について協力を依頼することができる。

(5) 情報通信事案担当課は、流出元の電子計算機を速やかに特定し、当該電子計算機をネットワークから切断又は隔離するものとする。
(6) 防衛政策局調査課及び秘密保全事案担当課は、秘密の情報の流出の有無を特定するものとする。
(7) 整備計画局サイバー整備課及び防衛政策局調査課は、相互に連携し、前各号までの結果を踏まえ、事案について、順序を経て防衛大臣に報告するものとする。

４　詳細把握、原因究明等

(1) 情報通信事案担当課（秘密の情報が流出した場合（秘密の情報が流出したおそれがある場合を含む。）は秘密保全事案担当課）は、流出情報の詳細、流出原因等を速やかに整理するとともに、必要に応じ関係課の協力を得てリスク分析、ダメージコントロール等を実施し、その内容を整備計画局サイバー整備課（秘密の情報が流出した場合（秘密の情報が流出したおそれがある場合を含む。）は防衛政策局調査課。次号及び第３号において同じ。）に通報するものとする。
(2) 整備計画局サイバー整備課は、前号により報告があった内容について、防衛省本省の内部部局の関係課に確認を依頼するものとする。
(3) 整備計画局サイバー整備課は、第１号により通報があった内容、前号により防衛省本省の内部部局の関係課が確認した結果等を取りまとめ、順序を経て防衛大臣に報告するものとする。
(4) 事案の詳細把握、原因究明等を行うに当たっては、整備計画局サイバー整備課及び防衛政策局調査課並びに情報通信事案担当課及び秘密保全事案担当課は、相互に情報を共有すること等により連携を図るものとする。

５　再発防止

(1) 情報通信事案担当課（秘密の情報が流出した場合は秘密保全事案担当課）は、事案に対処する方策を検討し、整備計画局サイバー整備課（秘密の情報が流出した場合は防衛政策局調査課）と調整の後、再発防止策を策定する。
(2) 再発防止策を策定するに当たっては、整備計画局サイバー整備課及び防衛政策局調査課並びに情報通信事案担当課及び秘密保全事案担当課は、相互に検討内容を調整する等により、連携を図るものとする。