統幕指企第２５７号
令和５年７月１日

自衛隊サイバー防衛隊司令
統　合　幕　僚　学　校　長
統 合 幕 僚 監 部 各 部 長
統合幕僚監部首席参事官
統 合 幕 僚 監 部 参 事 官　殿
統 合 幕 僚 監 部 報 道 官
統合幕僚監部首席法務官
統合幕僚監部首席後方補給官

統　合　幕　僚　長
（公　印　省　略）

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の運用について（通達）

標記について、別紙のとおり実施されたい。

なお、統合幕僚監部及び自衛隊指揮通信システム隊の情報保証に関する達の運用について（通達）（統幕指企第８２号。令和４年３月１７日）は廃止する。

添付書類：別紙

文書管理者：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
作成年月日：2023.7.1　保存年月日：10年　保存期間満了日：2034.3.31
枚数：27枚　配布先：宛先のとおり。11箇所

別　紙

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（以下「達」という。）の運用について

第１　第１章及び第２章関連

１　達の適用を受ける情報システム及び情報システム情報保証責任者の指定について（達第３条及び第６条関連）

付紙第１のとおり。

２　統合幕僚監部等における部隊等情報保証責任者の指定について（達第７条関連）

付紙第２のとおり。

３　部隊等情報保証責任者の業務について（達第７条関連）

(1)　職員に対する統制

部隊等情報保証責任者は、情報保証の確保に当たり、各課等のシステム利用者を監督するほか、各課等の職員以外に対しても必要な統制を実施するものとする。

(2)　職員以外による機器の持込み

職員以外による説明、展示、講演等に使用するために持ち込まれたパソコン、携帯電話、目的特化型機器及び可搬記憶媒体は、部隊等情報保証責任者により情報保証を確保する上で必要な措置を講じ使用させるものとする。

第２　第３章関連

１　情報システムの管理について

各課等に端末の設置がまたがる情報システムについては、各課等の部隊等情報保証責任者が各課等における端末の設置状況の把握後、各情報システム情報保証責任者（運用）へ掌握状況を通知するものとする。

２　情報システムの施錠について

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、可搬型情報システムの固定ワイヤー又はロッカー等のかぎを管理するものとする。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、かぎの保管、貸出し及び返却に関する管理規則を策定し、当該かぎの保管方法を定めておくものとする。

第３　第５章関連

１　可搬記憶媒体の細部管理要領について（達第３８条関連）

秘密の文書等を起案する場合は、秘密にかかわる業務用データを記録した可搬記憶媒体の管理要領について（通知）（統幕総第７１８号。２７．１０．１）に基づき、秘密の文書等（指定前秘密を含む。）を起案するための可搬記憶媒体の登録、入力記録等を行うものとする。

２　持出時の可搬記憶媒体の準備及び情報漏えい防止の徹底について

部隊等情報保証責任者は、達第３８条第５項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。

３　可搬記憶媒体を使用する場合の責務について

職員は、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ないことを確認し、コンピュータ・ウイルス等の感染が確認された場合には、コンピュータ・ウイルス等が駆除されない限り、当該可搬記憶媒体を使用してはならない。

４　可搬記憶媒体の送達票について

付紙第３のとおり。

５　ファイル暗号化ソフトの適切な使用について

可搬記憶媒体で情報システム内の電子計算機情報を取り扱う場合は、別に示す要領に基づき、適切な暗号化ソフトの設定を行うものとする。

６　可搬記憶媒体等の管理要領について

付紙第４のとおり。

第４　第６章関連

部隊等情報保証責任者は、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（付紙第５）を提出させ、管理するものとする。

第５　第８章関連

１　セキュリティ情報連絡態勢について（達第４２条関連）

(1)　事案対処責任者は、セキュリティ情報連絡網を作成し、情報保証責任者及び各情報システム情報保証責任者（運用）に配布するものとする。

(2)　情報システム情報保証責任者（運用）は、当該情報システムの稼働時間に応じ、連絡態勢をとるものとし、連絡担当者及び連絡先を事案対処責任者に連絡するものとする。

(3)　事案対処責任者は、セキュリティ情報連絡態勢に係る事務的事項につい

て、事案対処責任者補助者に実施させるものとする。

(4)　セキュリティ情報連絡態勢概要図は、付紙第６のとおり。

２　サイバー攻撃等対処要領について（達第４１条関連）

付紙第７のとおり。

第６　第９章関連

１　自己点検について（達第４３条関連）

自己点検の実施要領、実施後の報告等については、情報保証統括責任者が自己点検の基本方針を示した場合を除き、以下の要領で実施する。

(1)　基準日

１月１５日

(2)　対象者

ア　情報システム情報保証責任者（運用）

イ　部隊等情報保証責任者

ウ　全職員

(3)　方法

基準日における防衛省の情報保証に関する訓令の遵守状況について、指揮通信システム部長が別に示す自己点検表の質問に回答する。

(4)　結果の取りまとめ

自己点検の結果は、指揮通信システム部長が別に示す報告様式により２月末日までに報告（指揮通信システム部長気付）する。

２　インターネット上への情報流出時における対応要領について（達第４５条関連）

付紙第８のとおり。

第７　リスク管理対応関連

１　運用承認について（第２０条関連）

付紙第９のとおり。

２　リスク分析・評価について（第２２条関連）

付紙第１０のとおり。

３　監査について（第４４条関連）

(1)　情報保証監査責任者補助者の指定

統合幕僚監部等における情報保証監査責任者補助者にサイバー企画室長を充て、次の業務を実施するものとする。

ア　情報保証規則の準拠状況に対する監査における統合幕僚監部等の統制

イ　監査実施計画書の起案に係る業務

ウ　自己点検結果に基づき、情報保証責任者から特に指示された事項

(2)　監査の実施要領について

付紙第１１のとおり。

付紙第１

統合幕僚監部等における情報システム及び情報システム情報保証責任者

番号	情報システム	情報システム情報保証責任者
１	中央指揮システム	整備：指揮通信システム企画課長 運用：指揮通信システム運用課長
２	中央指揮システム専用通信	
３	中央指揮システム緊急伝達装置	
４	防衛情報通信基盤（クローズ系）	
５	防衛情報通信基盤（オープン系）	
６	防衛情報通信基盤（オープン系） ＵＣサービス（防衛省携帯管理機能）	
７	携帯電話用秘匿装置	
８	防衛省携帯電話端末	
９	中継器等管制局	
１０	統合衛星ＮＭＳ	
１１	統合ＮＭＳ	
１２	ＣＥＫＭＳ	
１３	ＧＣＣＳ	
１４	ＣＥＮＴＲＩＸ－Ｊ	
１５	サイバー関連システム	整備、運用： 指揮通信システム企画課長
１６	データ管理装置	整備、運用： 指揮通信システム運用課長
１７	統合訓練支援システム（ＪＥＴＳＳ）	整備、運用：運用第３課長
１８	日米共同分析研究用コンピュータシステム	整備、運用：計画課長
１９	情報収集用端末	整備、運用：総括副報道官
２０	統合幕僚学校ＬＡＮ	整備、運用： 統合幕僚学校総務課長
２１	教育用システム	整備、運用： 統合幕僚学校 国際平和協力センター長

番号	情報システム	情報システム情報保証責任者
２２	研究支援システム	整備、運用： 統合幕僚学校教育課長
２３	スタンドアロン型情報システム	整備、運用： 計画、整備する各課等の長
２４	タブレット型情報システム	
２５	施設設備関連情報システム	

付紙第２

統合幕僚監部等における部隊等情報保証責任者

機　関　名	部　官　名	部隊等情報保証責任者
統合幕僚監部	総　務　部	総務課長
		人事教育課長
	運　用　部	運用第１課長
		運用第２課長
		運用第３課長
	防衛計画部	防衛課長
		計画課長
	指揮通信システム部	指揮通信システム企画課長
		指揮通信システム運用課長
	首席参事官	運用調整官
	参　事　官	
	報　道　官	総括副報道官
	首席法務官	首席法務官付法務官
	首席後方補給官	後方補給室長
統合幕僚学校		企画室長
		総務課長
		教育課長
		国際平和協力センター長
自衛隊サイバー防衛隊	隊本部	隊本部第２科長
	各隊	隊長

付紙第３

可搬記憶媒体送達票

発送元部隊等名称	
発　送　者 職名　階級　氏名	
送達可搬記憶媒体 型式、登録番号及び数量	
発送年月日	
備　考	

-·-·-·-·-·-·-·-·-·-·-·-キリトリ-·-·-·-·-·-·-·-·-·-·-·-

可搬記憶媒体受領票

受領部隊等名称	
部隊等情報保証責任者 職名　階級　氏名	
受領可搬記憶媒体 型式、登録番号及び数量	
受領年月日	
備　考	

※　上記の可搬記憶媒体を受領したならば、「キリトリ」線で切り離し、必要事項を記入の後、速やかに本受領票を返信されたい。

付紙第４

可搬記憶媒体等の管理要領について

１　可搬記憶媒体の管理要領

(1)　部隊等情報保証責任者は、可搬記憶媒体に保存された電子計算機情報の種類、秘密区分等に従い、施錠できるロッカー等へ集中保管するとともに適切に管理を行うものとする。

ア　業務用データを取り扱う可搬記憶媒体

(ｱ)　可搬記憶媒体の包装を開封した段階又は可搬記憶媒体を他の部隊等から接受した段階で、部隊等情報保証責任者は、可搬記憶媒体登録簿へ登録し、管理するものとする。また、当該可搬記憶媒体には、登録されたことが分かるように登録番号を表示する。

なお、秘密以上の情報を取り扱う可搬記憶媒体については、秘密保全に関する達（平成２０年自衛隊統合達第１６号）、特定秘密の保護に関する達（平成２６年自衛隊統合達第１７号）及び特別防衛秘密の保護に関する達（平成２０年自衛隊統合達第１８号）に基づき管理するものとする。

(ｲ)　可搬記憶媒体を集中保管場所から持ち出し、当該部隊等の所在する防衛省が管理する区域内で使用する場合は、可搬記憶媒体使用記録簿に記録し、持ち出すものとする。

(ｳ)　可搬記憶媒体を防衛省が管理する区域外に持ち出す場合は、可搬記憶媒体持出簿に記載し、部隊等情報保証責任者の許可を得て持ち出すものとする。

イ　開示可能データを格納した可搬記憶媒体

開示可能データを可搬記憶媒体に格納する場合は、ＣＤ－Ｒ等の可搬記憶媒体に当該データを格納した後、追記禁止措置を可搬記憶媒体に施し、登録簿に登録して管理するものとする。この際、可搬記憶媒体には登録番号を明記するとともに「開示」と表示する。

ウ　市販コンテンツを記憶した可搬記憶媒体

(ｱ)　管理簿を必要としない。

(ｲ)　当該可搬記憶媒体に「市販」又は市販コンテンツである旨を表示する。

(ｳ)　市販コンテンツをインターネット等からダウンロードし、可搬記憶媒体へ保存する場合は、業務用データ又は開示可能データとして登録するものとする。

(2)　集中保管場所は、保全責任者等の勤務する執務室及び秘密保全に関する訓令（平成１９年防衛省訓令第３６号。以下「省秘訓令」という。）第４３条に基づき指定された場所を基準とし、部隊等情報保証責任者が指定するものとする。

(3)　同一の可搬記憶媒体に業務用データ、開示可能データ及び市販コンテンツを混在させてはならない。ただし、可搬記憶媒体の保存領域が論理的に分離されており、電子計算機情報がそれぞれの領域間を移動できない場合は、この限りでない。

(4)　部隊等情報保証責任者は、職員等に、暗号化機能が設けられた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保存する場合には、当該電子計算機情報を暗号化して保存させなければならない。ただし、職務の遂行に著しい支障が生じるおそれがあり、やむを得ないと認める場合は、別に定める要領に従い、暗号化機能の無効化及び可搬記憶媒体への電子計算機情報の保存を申請するものとする。

(5)　部隊等情報保証責任者は、業務用データを格納した可搬記憶媒体の破棄について、当該可搬記憶媒体を再利用する場合は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３２６号。令和４年１２月２２日）別紙第３第２項第１４第５項により情報を確実に消去し、可搬記憶媒体そのものを破棄する場合は、省秘訓令第４７条第３項に準じて破棄するものとする。

(6)　職員は、可搬記憶媒体を使用する場合は、安全性を確認し使用するものとする。

２　業務用データの取扱い

防衛省が管理する区域外への業務用データの持ち出しを禁止する。ただし、業務上の理由により、防衛省が管理する他の区域に携行する場合又は防衛省が管理する区域外で業務用データを使用する場合については、携行する可搬記憶媒体、情報システムの持ち出しに必要な手続の後、携行するものとする。

３　持ち出しを前提とした情報システムの取扱い

内部に業務用データを保存しないよう設計された持ち出しを前提とした情報システムを持ち出す場合には、情報システム情報保証責任者（運用）の許可を得るほか、次の項目を実施するものとする。

(1)　端末の管理

情報システム情報保証責任者（運用）は、端末を部外へ持ち出すことを許可した場合については、持ち出し先、持ち出し期間等を記録するものとする。また、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。

(2)　使用場所の制限

システム利用者は端末を持ち出す場合には、盗難防止のために必要な措置を講じるとともに、使用場所は、当該システム利用者以外の者により不正な操作や情報の窃取が行われることのないと認められる場所に限るものとする。

(3)　無線ＬＡＮの制限

システム利用者は無線ＬＡＮを使用する必要がある場合には、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（通達）（防防調第６５２１号。令和４年４月１日）第１７による秘匿化措置を講じたもののみ接続することができる。

(4)　周辺機器の接続

システム利用者は外部での端末使用時、情報システム情報保証責任者（運用）に認められた周辺機器を除き、端末に接続してはならない。

(5)　端末の紛失

システム利用者は端末の破損、紛失を確認した場合には、速やかに情報保証担当者を通じて、情報システム情報保証責任者（運用）に通報し、指示を仰ぐとともに防衛省所管物品管理取扱規則（平成１８年防衛庁訓令第１１５号）第３４条に基づき適切な処置を行う。

１３
付紙第５

統合幕僚長　殿

誓　約　書

私は、現在、私有機器により、業務用データを取り扱っていません。

また、防衛省職員としての職務を自覚し、その役割を果たすとともに、情報保証に関する規則を遵守し、情報流出防止のための措置をとることに努め、決して業務用データの流出を起こさないことを誓います。

令和　　年　　月　　日

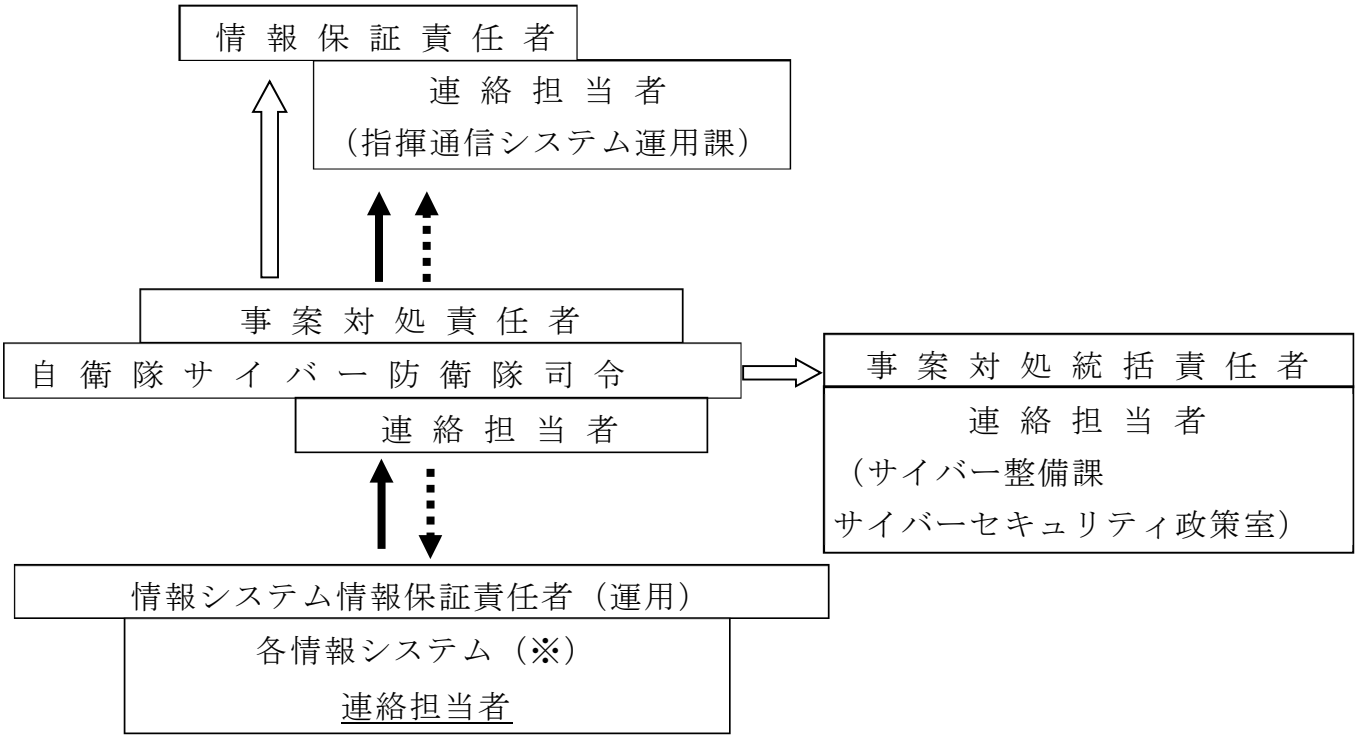
（所　属）

（官職名）

（氏　名）

付紙第６

セキュリティ情報連絡態勢概要図



※：付紙第１に定める各情報システム

凡例

：各情報システムに係るセキュリティ情報

：事案対処責任者が収集するセキュリティ情報（整備計画局情報通信課から連絡される他機関等のセキュリティ情報を含む。）

：セキュリティ情報のうち、情報システムに重大な影響を及ぼすおそれのあるものについては、情報保証責任者及び事案対処統括責任者に報告

付紙第７

サイバー攻撃等対処要領

１　サイバー攻撃等対処のための連絡態勢

セキュリティ情報連絡態勢を活用する。

２　対処要領

(1)　未然防止措置

ア　事案対処責任者は、セキュリティ情報連絡態勢を活用し、サイバー攻撃等に関する情報を努めて早期に収集・分析し、必要な措置について、各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。

イ　情報システム情報保証責任者（運用）は、自ら収集するセキュリティ情報及び事案対処責任者から連絡されるセキュリティ情報に基づき、管理する情報システムの脆弱性等を発見した場合、脆弱性を改善するための措置をとるものとする。

ウ　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上の理由により、修正プログラム等を当該情報システムに適用できない場合、脆弱性を無効化し得る他の対策を講じるものとする。

エ　事案対処責任者は、脆弱性の改善に関する事項及びコンピュータ・ウイルスの定義ファイル更新に関し､情報システム情報保証責任者(運用)を統制するものとする。

オ　情報システム情報保証責任者（運用）は、システムの形態管理情報、アクセス制御情報及びアクセス記録の整理収集を行い、異状の有無を定期的に点検するものとする。

(2)　サイバー攻撃等を認知した場合の対処措置

ア　情報システムの利用者は、情報システム内にウイルス等を発見した場合又はデータの消失、データの改ざん等、情報システムの異常を発見した場合、速やかに情報システム情報保証責任者（運用）に報告又は通報するものとする。

イ　情報システム情報保証責任者（運用）は、アの報告又は通報を受けた場合、速やかに事案対処責任者に通報するものとする。

ウ　事案対処責任者は、情報システム情報保証責任者（運用）からイの通報を受けた場合、情報保証責任者に報告するとともに、事案対処統括責任者に通報するものとする。

(3)　対処措置

ア　応急処置

情報システム情報保証責任者（運用）は、サイバー攻撃等が情報シス

テムに与える影響を局限するため、被攻撃等部位（端末等）の情報システムからの切断等の応急処置を実施する。この際、事案対処責任者は、情報システム情報保証責任者（運用）に対する必要な技術的支援を実施するものとする。また、他の機関の情報システムに影響を及ぼすおそれがある場合は、事案対処統括責任者及び他の機関の事案対処責任者と連携して対処するものとする。

イ　原因探求及び排除

情報システム情報保証責任者（運用）は、応急処置を実施した後、サイバー攻撃等による障害の原因探求を行い、障害の原因を排除するものとする。この際、事案対処責任者は、情報システム情報保証責任者（運用）に対する必要な技術的支援を実施するものとする。また、サイバー攻撃等が他の機関の情報システムに影響を及ぼしている場合は、他の機関の事案対処責任者と連携して対処するものとする。

ウ　復旧処置

情報システム情報保証責任者（運用）は、サイバー攻撃等による障害原因の排除後、情報システムを通常運用に復旧させるものとする。

エ　その他

中央指揮システム及び防衛情報通信基盤に対するサイバー攻撃等の場合、当該情報システムの情報システム情報保証責任者（運用）は、それぞれの関連規則に従い、連接システム及び加入システムの情報システム情報保証責任者と連携して対処するものとする。

３　情報収集、分析及び配布要領

事案対処責任者は、セキュリティ情報連絡態勢により、収集したセキュリティ情報を分析し、各情報システム情報保証責任者（運用）に配布するものとする。また、分析結果については、セキュリティ情報連絡態勢を活用し、他機関とも情報共有を図るものとする。

４　その他

サイバー攻撃等対処に関し、その他必要な事項については、各情報システム情報保証責任者（運用）が定めるものとし、情報システム情報保証責任者（運用）から依頼があった場合、事案対処責任者は、情報システム情報保証責任者（運用）を支援するものとする。

付紙第８

インターネット上への情報流出時における対応要領

１　連絡態勢

インターネット上への情報流出事案対応を行う情報通信担当課及び秘密保全担当課は次のとおりとする。

(1)　情報通信担当課

指揮通信システム部指揮通信システム企画課

連絡先　サイバー企画室情報保証係

（課業外　指揮通信システム部運用当直）

(2)　秘密保全担当課

総務部総務課

連絡先　総務班保全係

（課業外　総務部当直）

２　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、速やかに前項の情報通信担当課及び秘密保全担当課に連絡するものとする。

(2)　事案対処責任者は流出元情報システムを特定するとともに、情報システム情報保証責任者（運用）及び情報通信担当課又は秘密保全担当課に対し技術的支援を行うものとする。

(3)　当該情報システム情報保証責任者（運用）は情報システムのネットワークからの切断又は隔離を行うとともに、情報通信担当課（当該情報流出事案が秘密保全事案の場合は、秘密保全担当課）と協力し、流出情報の詳細、流出原因等の整理を行う。

(4)　関係する部等は、事案対処責任者に協力するものとする。

付紙第９

運用承認の実施について

１　情報システム情報保証責任者（整備）は、情報システムの整備、換装に際し、適切にリスク管理が行われることについて、情報システム情報保証認証者による評価及び認証を得た上で、定められた時期までに情報保証責任者の運用承認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（整備）は、運用承認を受ける場合、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（以下「運用承認申請文書」という。）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、情報システム情報保証責任者（整備）より前項の提出を受けた場合には、セキュリティ評価計画書及びセキュリティ評価報告書を作成し、情報システム情報保証責任者（整備）に提出するものとする。

４　情報システム情報保証責任者（整備）は、評価結果を踏まえ、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、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（整備）は、運用承認申請文書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、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（整備）に提出するものとする。

７　情報システム情報保証責任者（整備）は、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。

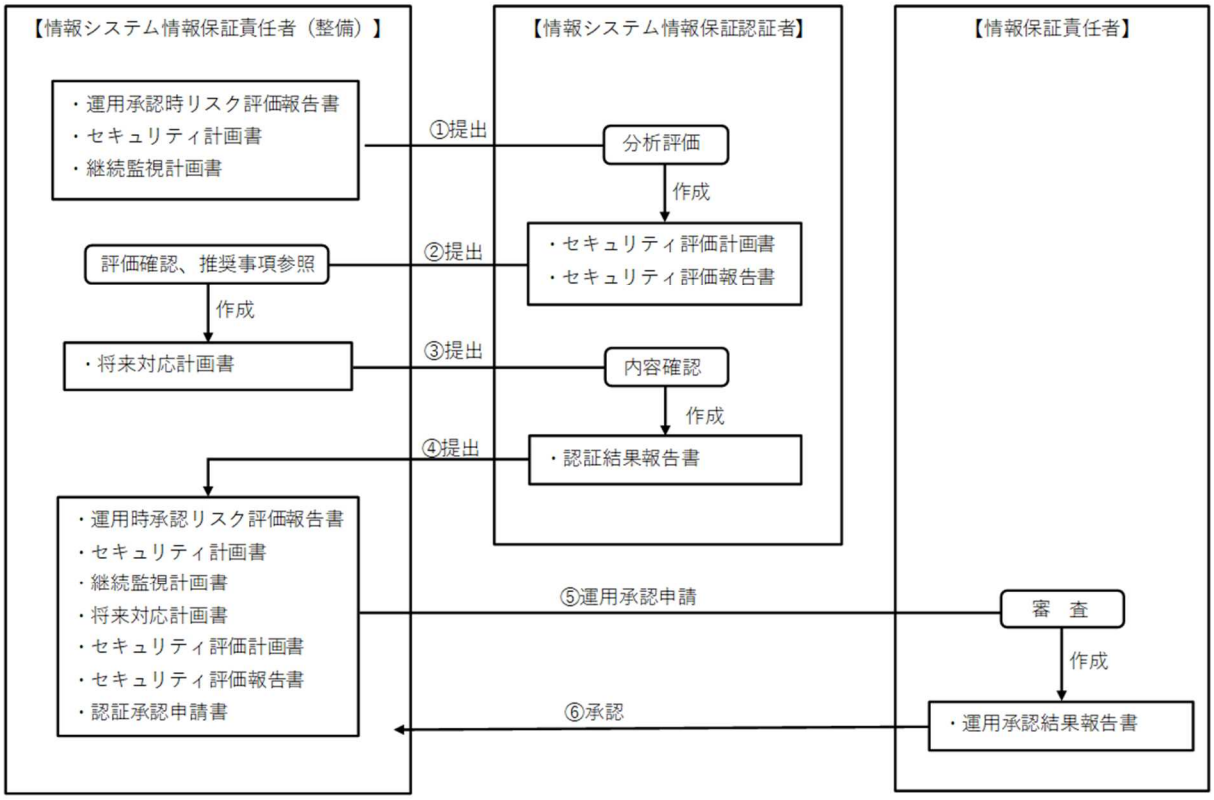
８　情報保証責任者は、運用承認の申請を受けた場合には、これを審査し、情報システムを運用することが可能と認める場合には、当該情報システムの運用承認を行い、その結果を情報システム情報保証責任者（整備）及び情報システム情報保証認証者に通知するものとする。

９　訓令第２６条第１項に定める情報システムについては、情報システム情報保証責任者（整備）は、情報保証責任者に承認を得た上で、運用承認を不要とすることができるものとする。

１０　運用承認に係る概要図を属図に示す。

属　図

運用承認概要図



作成文書	概　要
リスク評価報告書	セキュリティ上のリスクを特定し、想定し得る被害や影響を記載
セキュリティ計画書	情報システムを機密性、完全性、可用性の観点から分類 分類に基づく情報システムに導入するセキュリティ管理策を選択 セキュリティ管理策の実装状況を記載
継続監視計画書	セキュリティ管理策の有効性を監視する評価要領を記載
セキュリティ評価計画書	セキュリティ管理策の分析・評価を記載
セキュリティ評価報告書	分析評価を通じて発見された問題、推奨事項を記載
将来対応計画書	セキュリティ評価に基づく非準拠項目及び脆弱性に対する対応計画

付紙第１０

リスク分析・評価の実施について

１　情報システム情報保証責任者（整備）は、リスク分析・評価の実施に当たり別に示す基本方針に従いリスク評価報告書、セキュリティ計画書、継続監視計画書を更新した後、情報システム情報保証責任者（運用）に情報提供するものとする。

２　情報システム情報保証責任者（運用）は、事案対処責任者又はリスク管理支援役務と調整した上で、脆弱性検査を統制し実施させるものとする。また、脆弱性検査終了後、判明した脆弱性及び統制する情報システムの運用状況に基づきリスク評価報告書、セキュリティ計画書、継続監視計画書を更新し、情報システム情報保証責任者（整備）に提出するものとする。

３　情報システム情報保証責任者（整備）は、前項により提出された文書を確認し、情報システム情報保証認証者に提出するものとする。

４　情報システム情報保証認証者は、前項によ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（整備）に提出するとともに必要に応じて改善指示を与えるものとする。

５　情報システム情報保証責任者（整備）は、セキュリティ評価文書の提出を受けた場合には、評価及び推奨事項を参照し、将来対応計画書を更新し、情報システム情報保証責任者（運用）に情報提供するものとする。

６　情報システム情報保証責任者（運用）は、前項による情報提供を受けた場合には、セキュリティ評価文書の評価及び推奨事項を参照し、運用所掌のセキュリティ管理策を更新し、情報システム情報保証責任者（整備）に提出するものとする。

７　情報システム情報保証責任者（整備）は、前項により提出された文書を確認し、情報システム情報保証認証者に提出するものとする。

８　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提出された文書を審査し、情報保証責任者に報告するものとする。

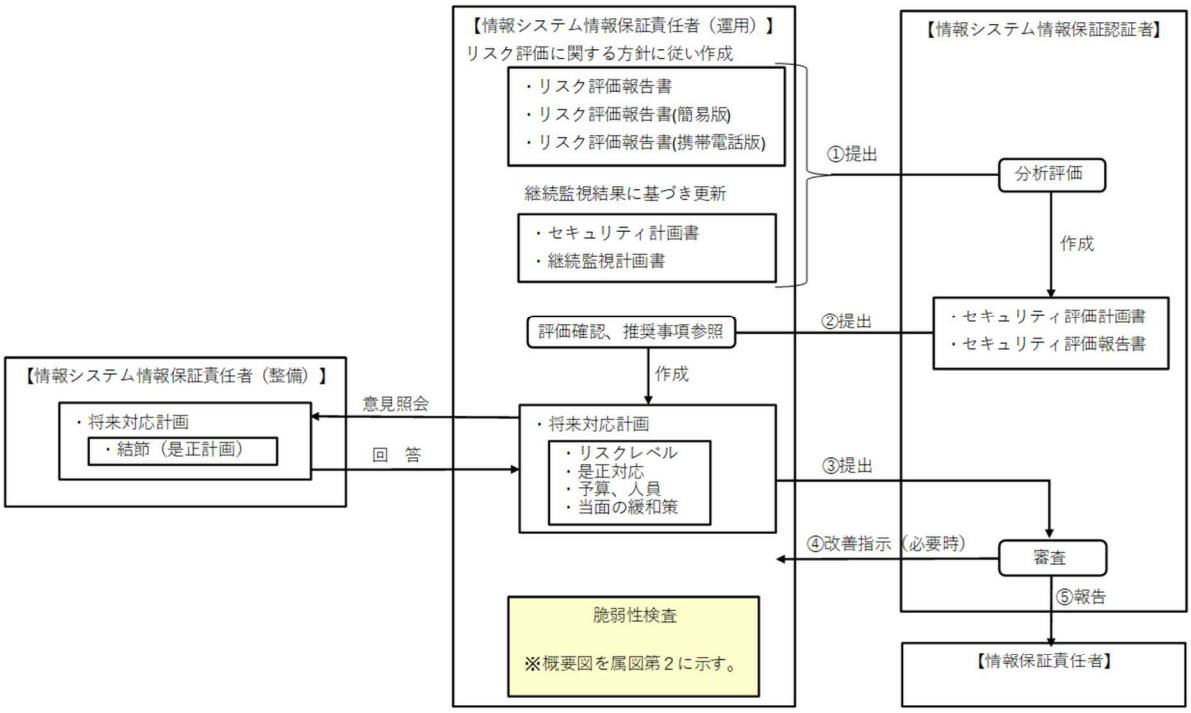
９　リスク分析・評価の一環として行う脆弱性検査については、運用承認を必要とする情報システムを対象とし、定められた頻度で実施する。脆弱性検査で判明した脆弱性については、将来対応計画に記載するものとする。

１０　指揮通信システム企画課は、付紙第１に定める情報システムに対し、事案対処責任者の支援を要する脆弱性検査を実施する場合は、必要事項を定めた脆弱性検査実施計画を作成し、脆弱性検査を受検する情報システム情報保証責任者（運用）及び事案対処責任者に通知するものとする。

１１　リスク分析・評価に係る概要図を属図第１及び属図第２に示す。

属図第１

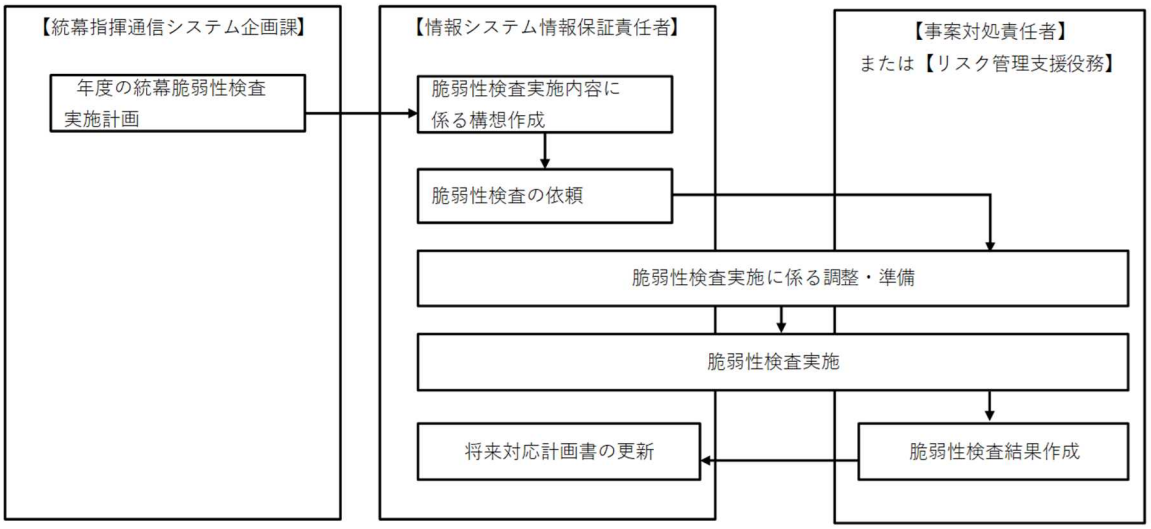
リスク分析・評価概要図



作成文書	概　要
脆弱性検査	リスク分析評価の一環として定められた頻度で実施、判明した脆弱性を将来対応計画に記載
リスク評価報告書	運用承認後、運用中の情報システムのリスク分析評価を記載
リスク評価報告書（簡易版）	運用承認を要しない情報システム及び規則改正後の運用承認を取得していないシステムがリスク分析評価時に使用する。
リスク評価報告書（携帯電話版）	運用承認を要しないとされた情報システム（携帯電話）がリスク分析評価時に使用する。

属図第２

脆弱性検査概要図



付紙第１１

監査の実施について

１　監査の概要

情報保証監査責任者は、防衛省の情報保証規則の遵守状況及び情報システムに対するセキュリティ管理策の適用状況について検証するため、監査を実施するものとする。

２　監査の区分

(1)　定期監査（情報保証監査責任者が定期的に実施する監査）

(2)　臨時監査（情報保証監査責任者が必要に応じて実施する監査）

(3)　特別監査（情報保証監査統括責任者の命により特別に実施する監査）

３　定期監査の実施について

定期監査について、監査実施計画書に基づき次を基準として実施する。

(1)　情報保証規則の遵守状況に関する監査要領

情報保証監査責任者は、別に示される監査の基本方針に示される事項を基準とするほか、各課等の自己点検の結果を踏まえ必要と認める事項について、情報保証規則の遵守状況を検証するものとする。

(2)　情報システムに対する監査の観点

ア　準拠性評価

情報システムにおけるセキュリティ管理策の準拠状況を評価

イ　要件評価

運用承認時に行った認証結果の妥当性を評価

ウ　プロセス評価

運用承認時に行った認証手順の妥当性を評価

(3)　情報システムに対する監査要領

ア　情報保証監査責任者は、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、監査を受検する情報システム情報保証責任者（運用）に通知するものとする。

イ　情報保証監査責任者は監査結果について監査結果通知書を作成し、情報システム情報保証責任者（運用）に通知し、是正勧告及び助言を行うものとする。

ウ　情報システム情報保証責任者（運用）は、監査の結果、整備段階の措置が必要となった場合については、情報システム情報保証責任者（整備）に通報するものとする。

エ　情報システム情報保証責任者（整備・運用）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。

オ　監査の一環として実施される侵入試験については、別に定める侵入試験の実施項目を基準としてシナリオを作成し実施するものとする。また、実施するに当たり、可能な限り情報システム内のデータ書き換え及び運用への支障が生じない範囲で実施するものとする。

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

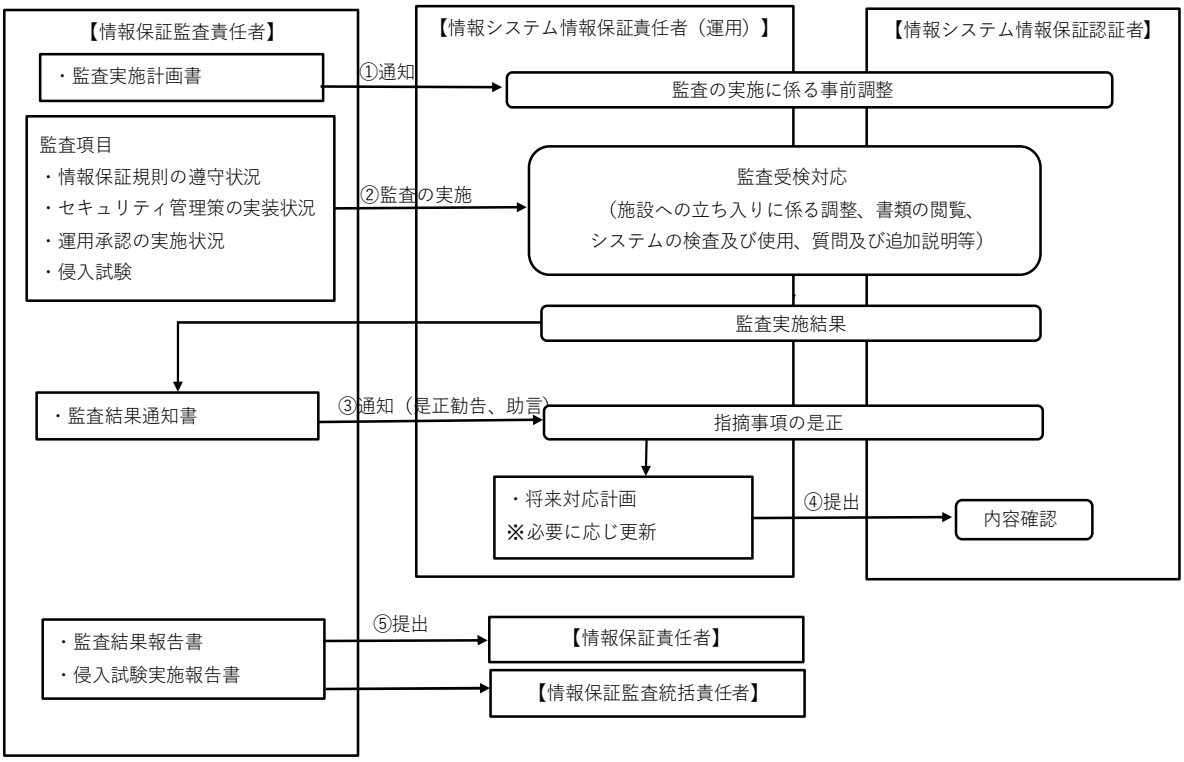
４　臨時監査及び特別監査の実施について

情報保証監査責任者は臨時監査及び特別監査の実施について、その都度別に示すものとする。

５　監査に係る概要図を属図第１及び属図第２に示す。

属図第１

監査概要図



監査作成書類	概　要
監査実施計画書	別途示される監査の基本方針に基づき、情報保証監査責任者が作成
監査結果通知書	監査の結果を通知し、是正勧告及び助言を行う。
将来対応計画書	監査での指摘事項に基づく将来の対応計画
監査結果報告書	監査結果を取りまとめたもの。

２７」

属図第２

侵入試験概要図