沖縄防衛局達第４６号

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）第４７条の規定に基づき、沖縄防衛局におけるサイバー攻撃等対処要領を次のとおり定める。

平成１９年１２月２８日

改正　平成２０年４月１日沖縄防衛局達第３号
平成２７年１０月１日沖縄防衛局達第６号

沖縄防衛局長　鎌田　昭良

沖縄防衛局におけるサイバー攻撃等対処要領

１　セキュリティ情報の連絡等

（１）　情報システム情報保証責任者は、最新のセキュリティ情報の把握に努めるものとする。

（２）　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。

（３）　情報システム情報保証責任者は、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９第２項第６号による重要性の指標に従って、次のとおり通報するとともに、情報システムに与える影響を考慮し、情報システムに対する措置を行うものとする。

ア　各情報システム情報保証責任者に対しては、すべて

イ　事案対処責任者に対しては、「注意喚起」及び「警報」を付したもの

ウ　情報保証責任者に対しては、「警報」を付したもの

２　サイバー攻撃等による被害を認知したときの連絡等

（１）　情報システム情報保証責任者は、運用通達第９第２項第４号の①から⑥までに掲げる被害のいずれかを認知したときは、事案対処責任者に通報しなければならない。

（２）　連絡要領は、運用通達第９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。（別図１及び別図２参照）

ア　運用通達第９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９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、次に掲げる被害のいずれか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。

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　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　具体的処置

（１）　応急処置

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は、サイバー攻撃等による被害が拡大するおそ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は、被害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し、被害の拡大を防がなければならない。

イ　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

ことが適当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。

（２）　原因探求

ア　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とともに、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に通報しなければならない。

イ　事案対処責任者及びシステム管理担当者は、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は、速やかに全ての情報システム情報保証責任者に通報するもとともに必要に応じ対策を講じさせるものとする。

（３）　復旧処置

ア　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を要すると判断した場合は、その旨を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、システム復旧の計画を作成し、事案対処責任者及び情報保証担当者に報告しなければならない。

イ　情報システム情報保証責任者は、被害に対処する方策を確立した場合は、次のとおり対処しなければならない。

（ア）サーバ側のみの対処で復旧する場合は、復旧処置後に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。

ウ　情報システム情報保証責任者は、情報システムの復旧が完了した場合には、事案対処責任者に報告しなければならない。

エ　情報システム情報保証責任者は、情報システムへの被害が極めて重大であった場合には、各種情報保証対策の改善等再発防止に必要な事項について、事案対処責任者に報告しなければならない。

６　その他

（１）　他の機関が設置する情報システムについては、当該機関が定める要領等を優先に適用する。

（２）　他の機関が設置する情報システムの管理者は、前記（１）による対処を実施するとともに、事案対処責任者へ適宜報告するものとする。

附　則

１　この要領は、平成２０年１月１日から施行する。

２　沖縄防衛局におけるサイバー攻撃等対処要領（平成１９年沖縄防衛局達第２４号）は廃止する。

附　則（平成２０年４月１日沖縄防衛局達第３号）

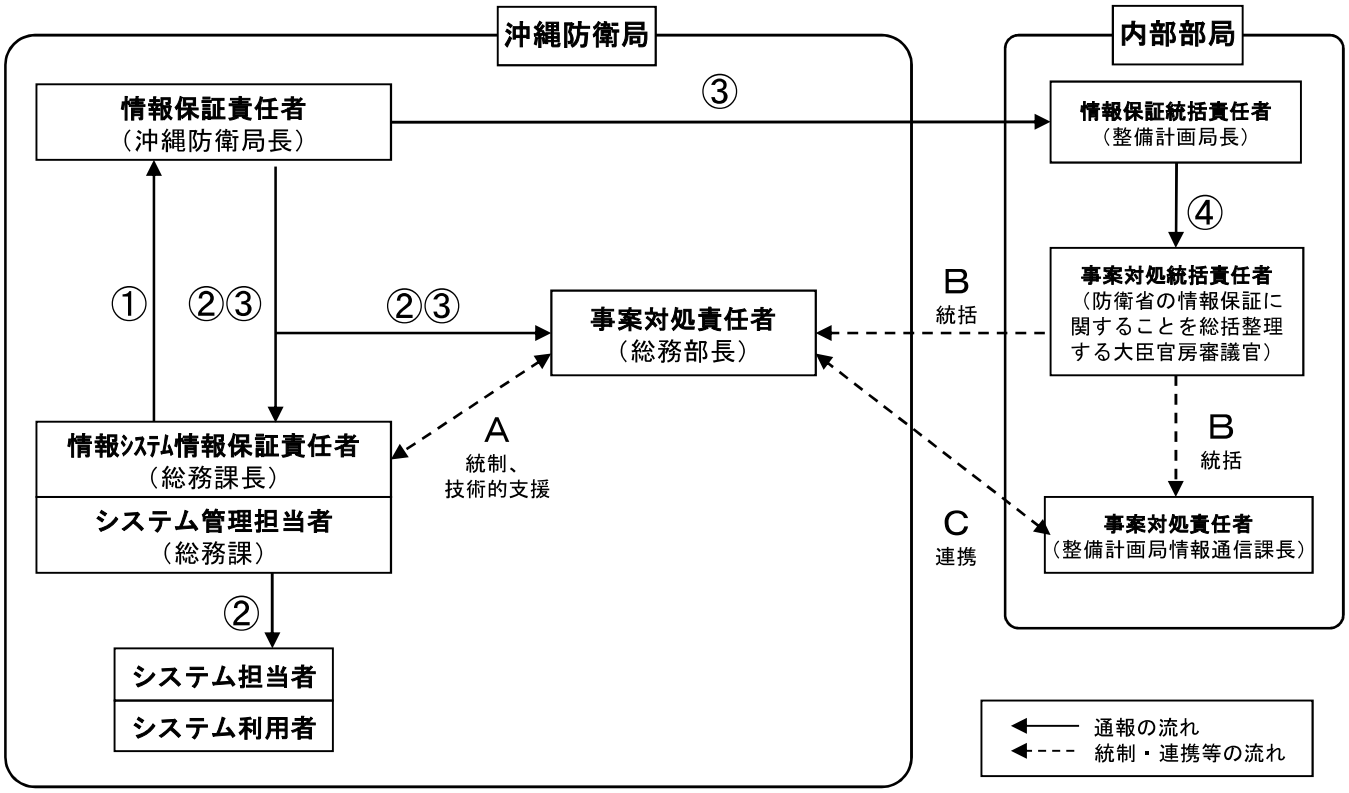
この達は、平成２０年４月１日から施行する。

附　則（平成２７年１０月１日沖縄防衛局達第６号）

この達は、平成２７年１０月１日から施行する。

別図１

事案対処系統図（未然防止のための措置）



通報の流れ

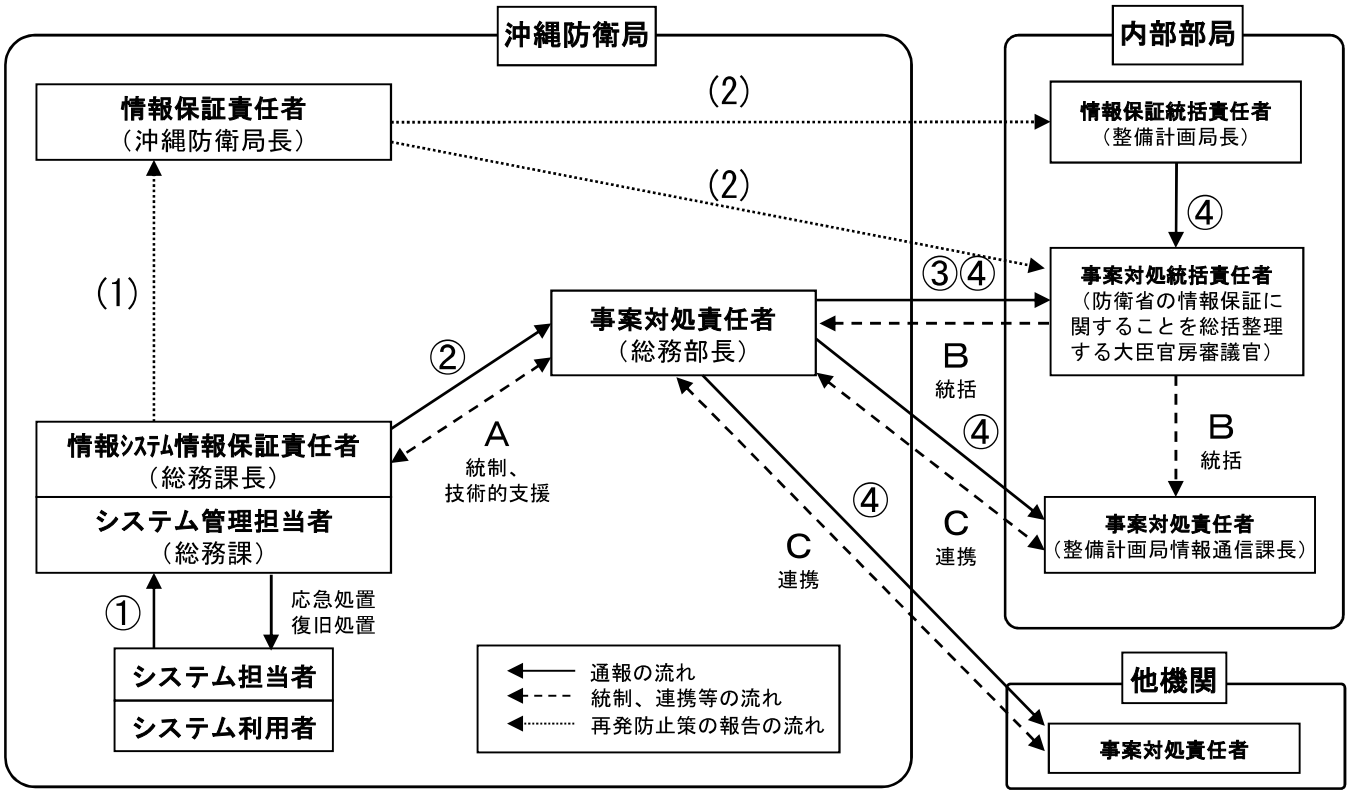
①運用通達第９第２項第２号
　情報システム情報保証責任者は、セキュリティ情報を入手した場合には、情報保証責任者に通報するものとする。
②運用通達第９第２項第３号
　情報保証責任者は、セキュリティ情報を入手した場合又は前号の通報を受けた場合には、必要に応じ、情報システム情報保証責任者、事案対処責任者その他の関係職員に周知するものとする。
③運用通達第９第２項第４号
　情報保証責任者は、セキュリティ情報のうち、次に掲げる被害のいずれかの兆候を認知した場合又は他の機関等の情報システムに影響を及ぼすおそれがあると認めるセキュリティ情報を入手した場合には、情報システム情報保証責任者及び事案対処責任者に通報するとともに、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、漏えい又は改ざん　・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９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括するものとする。
Ｃ 運用通達第９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。

別図２

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９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９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９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９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括するものとする。
Ｃ 運用通達第９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。

再発防止策の報告の流れ

(1) 運用通達第９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９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。