防研総第８４３号
２６．　７．２３
改正　防研総第２２９号
３１．　３．１８
改正　防研総第１８１号
令和４年３月４日

各　　部　　長
戦史研究センター長　殿
図　書　館　長

防衛研究所長
（公印省略）

防衛研究所におけるサイバー攻撃等対処要領について（通達）

標記について、防衛研究所の情報保証に関する達（平成１９年防衛研究所達第８号）第３９条第１項の規定に基づき、別紙のとおり定め、平成２６年７月２３日から実施することとしたので通達する。

なお、防研発総第３６４号（１９．１２．１２）は、平成２６年７月２２日をもって廃止する。

添付書類：別紙
配付区分：副所長、統括研究官、事例研究室長

別紙

1　趣旨

この要領は、防衛研究所における情報保証を確保することを目的とし、防衛研究所情報システム（以下「本システム」という。）へのサイバー攻撃等に対処するために必要な事項を定めるものである。

2　用語の定義

この要領に用いる用語の意義は、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２条、防衛情報通信基盤の維持管理及び運用に関する業務処理について（防官情第２２０９号。１８．３．２４。以下「ＤＩＩ運用通達」という。）第２、防衛情報通信基盤及びこれに接続する情報システムにおけるサイバー攻撃対処要領について（運情第３６６８号。２０．３．２５。以下「ＤＩＩサイバー攻撃等対処要領」という。）第２、防衛情報通信基盤及びこれに接続する情報システムにおけ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「ＤＩＩサイバー攻撃等対処要領」という。）第２及び防衛研究所の情報保証に関する達（平成１９年防衛研究所達第８号。以下「達」という。）第２条に定めるもののほか、次の各号に定めるところによる。

（１）機関等

訓令第６条第１項に規定する機関等をいう。

（２）情報保証責任者

訓令第６条に規定する情報保証責任者をいう。

（３）情報保証責任者補助者

防衛研究所の情報保証に関する細部要領（防研総第８４１号。２６．７．２３。以下「細部要領」という。）第４項第１号アに規定する情報保証責任者の補助者をいう。

（４）事案対処責任者

達第３条第４項に規定する事案対処責任者をいう。

（５）事案対処責任者補助者

細部要領第４項第１号アに規定する事案対処責任者補助者をいう。

（６）システム責任者

達第３条第１項に規定する情報システム情報保証責任者をいう。

（７）システム責任者補助者

細部要領第４項第１号イの規定により、システム責任者が指定するシステム責任者の補助者をいう。

（８）総務課システム責任者補助者（正）

細部要領第４項第１号エに規定する総務課のシステム責任者補助者の正をいう。

（９）情報保証統括責任者

訓令第４条に規定する情報保証統括責任者をいう。

(10) 事案対処統括責任者

訓令第１０条に規定する事案対処統括責任者をいう。

(11) セキュリティ情報
　　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をいう。

3　適用範囲
　この要領は、本システムに適用する。

4　連絡体制
（1）連絡先の把握
　ア　職員等は、所属する各部等のシステム責任者補助者及び総務課システム責任者補助者（正）の連絡先を把握しておくものとする。
　イ　総務課システム責任者補助者（正）は、システム責任者、事案対処責任者補助者及び情報保証責任者補助者の連絡先を把握しておくものとする。
　ウ　システム責任者補助者（総務課システム責任者補助者（正）を除く。）は、総務課システム責任者補助者（正）の連絡先を把握しておくものとする。
　エ　事案対処責任者補助者は、事案対処責任者、情報保証責任者補助者、事案対処統括責任者及び他機関等の事案対処責任者の連絡先を把握しておくものとする。
　オ　情報保証責任者補助者は、事案対処統括責任者、情報保証統括責任者及び総務課システム責任者補助者（正）の連絡先を把握しておくものとする。
（2）連絡要領
　サイバー攻撃等が発生した場合又は発生するおそれがある場合の連絡要領は、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）第９第２項及び第３項並びにＤＩＩ運用通達第５第２項第１号に規定するもののほか、サイバー攻撃等対処連絡網（付紙第１）及び防衛省中央ＯＡネットワーク・システムにおけるサイバー攻撃等発生時の対処の系統図（付紙第２）により行うものとする。

5　処置要領
（1）応急処置
　ア　システム責任者は、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、本システムの全部又は一部を停止し、使用の統制をして被害の拡大を防ぐものとする。
　イ　システム責任者は、職員等が行うことが適当な応急処置について、当該職員等が所属する各部等のシステム責任者補助者又は当該職員等に連絡し、対処させるものとする。
（2）原因探求及び排除
　ア　システム責任者は、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し、これを排除するものとする。
　イ　事案対処責任者は、原因探求及び排除に関して、システム責任者に対し技術的支援を行い、協力して対処するものとする。
（3）証拠保全
　ア　職員等は、サイバー攻撃等が発生した場合又はそのおそれがある場合は、第４

項第２号の連絡要領に従い、直ちに通報するとともに、自ら処置することなく、その指示を受けるものとする。

イ　システム責任者は、サイバー攻撃等が発生した場合又はそのおそれがある場合は、必要に応じ事案対処責任者の技術的支援を受け、速やかにサイバー攻撃等の影響範囲、被害状況を特定するために必要な各種証拠の保全措置を行うものとする。

（４）復旧処置

ア　システム責任者は、サイバー攻撃等による障害原因の排除後、本システムを運用可能な状態に復旧させるものとし、復旧処置に関して必要な事項を職員等に連絡するものとする。

イ　事案対処責任者は、復旧処置に関して、システム責任者に対し技術的支援を行い、協力して対処するものとする。

ウ　システム責任者は、本システムの復旧が終了した場合には、情報保証責任者に報告するものとする。

（５）再発防止

システム責任者は、サイバー攻撃等が発生した原因を第３号で収集した各種証拠により分析するとともに、再発防止策を策定し、情報保証責任者に報告するものとする。

６　情報収集、分析及び配布要領

（１）情報収集

ア　システム責任者は、サイバー攻撃等により本システムに不正な変更等が行われていないことを定期的に確認するものとする。

イ　システム責任者及び事案対処責任者は、常に最新のセキュリティ情報の収集に努めるものとする。

（２）分析

事案対処責任者は、サイバー攻撃等の未然防止のため、収集したセキュリティ情報を分析するものとする。

（３）配布

ア　システム責任者は、収集したセキュリティ情報のうち、必要に応じ情報保証責任者に報告するものとする。

イ　情報保証責任者は、この号アの報告を受けたセキュリティ情報のうち、必要と思われるものを職員等に配布するものとする。

７　その他

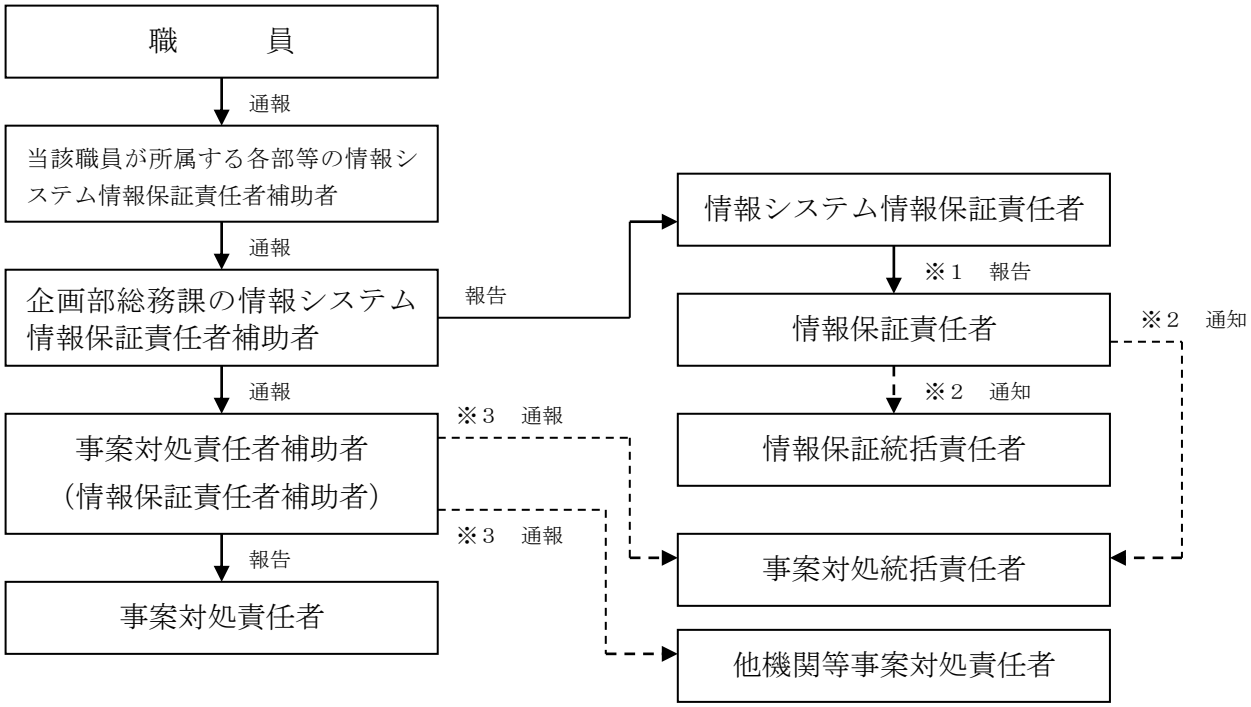
（１）　この要領の実施に関し必要な事項は、システム責任者及び事案対処責任者が定めることができるものとする。

（２）　防衛研究所ＤＩＩオープン系システム（防衛研究所が加入した防衛情報通信基盤のオープン系統合ルータに接続している情報システムをいう。）のサイバー攻撃等対処要領については、この要領に定めるもののほか、ＤＩＩサイバー攻撃等対処要領に定めるところによるものとする。

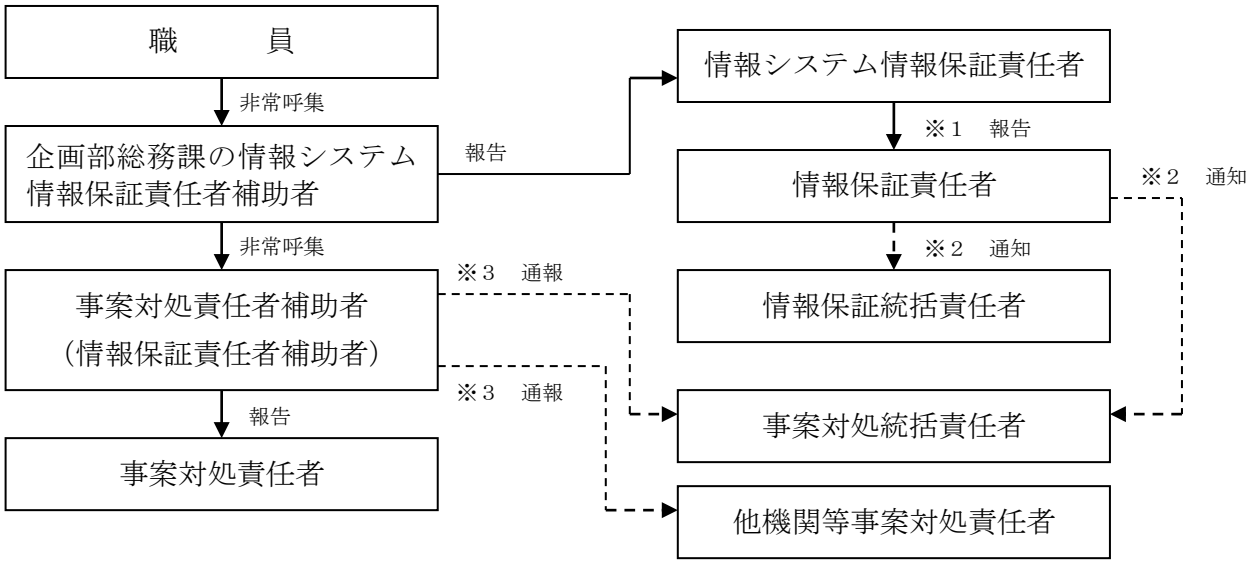
付紙第１

サイバー攻撃等対処連絡網

【課業中】



【課業外】



※１　重大な被害が生じた場合又は重大な被害が生じるおそれがある場合
※２　必要に応じて
※３　次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
（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）コンピュータウィ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、漏えい又は改ざん

→ 防研内　　- - -▶ 防研外

防衛省中央ネットワーク・システムにおけるサイバー攻撃等発生時の対処の系統図