運情第３６６８号
２０．３．２５

情報保証責任者
　施設等機関の長
　各　幕　僚　長
　情 報 本 部 長
　技術研究本部長　殿
　装備施設本部長
　防 衛 監 察 監
　各地方防衛局長

情報保証統括責任者
運 用 企 画 局 長

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(通達)

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条第２項の規定に基づき、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に対する対処要領について別紙のとおり定め、平成２０年３月２６日から適用することとしたので、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。

添付書類：別紙

別紙

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

第１　趣旨

この「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」（以下「要領」という。）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４７条第２項の規定に基づき、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への対処に関し統一的な基準を設けるため、必要な事項を定めるものとする。

第２　定義

この要領に掲げる用語の定義は、訓令に定めるもののほか、次の各号に定めるとおりとする。

(1) 防衛情報通信基盤

自衛隊が共通に使用する音声通信網及びデータ通信網で、固定の通信回線(専ら音声通信に使用するものにあっては多重伝送路を使用するものに限る。)及び衛星可搬局により構成される通信回線並びに音声通信用機器及びデータ通信用機器で構成されるものをいう。

(2) 未然防止措置

サイバー攻撃等が発生するおそれがある場合又は発生した場合においてサイバー攻撃等による被害を未然に防止するための措置及びサイバー攻撃等が発生した場合に再発を防止するための措置をいう。

(3) 対処措置

サイバー攻撃等が発生した場合に講ずる証拠保全、被害拡大防止、復旧等の措置をいう。

(4) ＩＮＦＯＣＯＮ

防衛情報通信基盤及びこれに接続する情報システム（以下「防衛情報通信基盤等」という。）に対しサイバー攻撃等が発生するおそれがある場合又は発生した場合において、サイバー攻撃等の脅威の状態に応じて５段階で未然防止措置又は防衛情報通信基盤における対処措置を講ずることによりサイバー攻撃等に対処する態勢をいう。

(5) 統幕事案対処責任者

統合幕僚長により置かれた事案対処責任者をいう。

第３　統幕事案対処責任者の責務

統幕事案対処責任者は、防衛情報通信基盤等に対するサイバー攻撃等への対処として、以下の措置を講ずるものとする。

(1) セキュリティ情報の収集及び防衛情報通信基盤等に与える影響等の分析並びに機関

等の事案対処責任者への当該セキュリティ情報及び分析結果の通報

(2) ＩＮＦＯＣＯＮの設定又は変更並びに機関等の事案対処責任者へのＩＮＦＯＣＯＮの設定又は変更の通報

(3) 前号のＩＮＦＯＣＯＮの設定又は変更に際しては、必要に応じて行う機関等の事案対処責任者との調整

(4) 第２号によりＩＮＦＯＣＯＮの設定又は変更をした場合には、事案対処統括責任者への報告

(5) サイバー攻撃等が発生した場合における防衛情報通信基盤等の被攻撃箇所又は被害箇所の特定及び第２号のＩＮＦＯＣＯＮの変更に係る通報に併せて行う当該被攻撃箇所又は被害箇所の通報

(6) 機関等の事案対処責任者が実施する未然防止措置及び対処措置に対する技術的支援

(7) 必要に応じて、機関等の事案対処責任者と調整の上行う、防衛情報通信基盤からの情報システムの切断等、防衛情報通信基盤の全部又は一部の運用を停止又は制限する措置

第４　機関等の事案対処責任者の責務

機関等の事案対処責任者は、防衛情報通信基盤等に対するサイバー攻撃等への対処として、以下の措置を講ずるものとする。

(1) セキュリティ情報の収集及び統幕事案対処責任者への当該セキュリティ情報の通報

(2) サイバー攻撃等が発生した場合における防衛情報通信基盤に接続する情報システムの被攻撃箇所又は被害箇所の特定及び統幕事案対処責任者への当該被攻撃箇所又は被害箇所の通報

(3) 第６で示すＩＮＦＯＣＯＮの各段階における未然防止措置の基準に基づく必要な未然防止措置

(4) 機関等の情報保証責任者が定める対処要領に基づく対処措置

第５　ＩＮＦＯＣＯＮの各段階における脅威の状態

ＩＮＦＯＣＯＮの各段階における脅威の状態は、以下のとおりとする。

(1) ＩＮＦＯＣＯＮ５

防衛情報通信基盤等に対するサイバー攻撃等が発生するおそれがある場合又は発生した場合であって、業務の遂行又は部隊の運用への影響がないか、影響がないと予測される状態をいう。

(2) ＩＮＦＯＣＯＮ４

防衛情報通信基盤等に対するサイバー攻撃等が発生するおそれがある場合又は発生した場合であって、業務の遂行又は部隊の運用への影響の可能性があると予測される状態をいう。

(3) ＩＮＦＯＣＯＮ３

防衛情報通信基盤等に対するサイバー攻撃等が発生した場合であって、業務の遂行又は部隊の運用への影響が一部に見られる状態をいう。

⑷　ＩＮＦＯＣＯＮ２

防衛情報通信基盤等に対するサイバー攻撃等が発生した場合であって、業務の遂行又は部隊の運用に相当程度の影響が見られる状態をいう。

⑸　ＩＮＦＯＣＯＮ１

防衛情報通信基盤等に対するサイバー攻撃等が発生した場合であって、業務の遂行又は部隊の運用に深刻な影響が見られる状態をいう。

第６　ＩＮＦＯＣＯＮの各段階における未然防止措置の基準

機関等の事案対処責任者が講ずるＩＮＦＯＣＯＮの各段階における未然防止措置の基準は、以下のとおりとする。

⑴　ＩＮＦＯＣＯＮ５

１８０日周期で未然防止措置を講ずる。

⑵　ＩＮＦＯＣＯＮ４

９０日周期で未然防止措置を講ずる。

⑶　ＩＮＦＯＣＯＮ３

６０日周期で未然防止措置を講ずる。

⑷　ＩＮＦＯＣＯＮ２

３０日周期で未然防止措置を講ずる。

⑸　ＩＮＦＯＣＯＮ１

１５日周期で未然防止措置を講ずる。

第７　報告等

機関等の事案対処責任者、情報システム情報保証責任者等の報告等は、この要領で定めるもののほか、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）によるものとする。

第８　雑則

１　この要領の実施に関して必要な事項は、統合幕僚長が定めるものとする。

２　この要領の施行後１年以内に、施行の状況について検討を実施し、その結果に基づき必要があると認められる場合は、この要領の見直しを行うものとする。