第3節　情報流出防止のための取組

防衛省の取り扱う情報の中には、漏えいすればわが国の防衛に重大かつ深刻な影響を及ぼすものがあり、このような秘密を保全することは、国の防衛を全うし、安全を保持する上で不可欠な基盤である。したがって、防衛省においては、日米相互防衛援助協定等に基づき米国から供与された装備品等に関する事項を内容とする「特別防衛秘密」、自衛隊の運用や防衛力整備等に関する一定の事項のうち、わが国の防衛上特に秘匿することが必要であるとして防衛大臣が指定する「防衛秘密」、およびこれら以外の防衛省の業務に関する秘密であるいわゆる「省秘」の３種類の秘密について、関係者以外の者がみだりに触れることのないよう、秘密の指定手続、秘密の厳正な伝達、保管、廃棄等の取扱い手続を定めるなど、その保全に努めている。

こうした中、防衛省・自衛隊においては、次に説明するような情報流出事案が発生した。

このことから、本節では、発生した事案の問題点およびそれを踏まえた取組などを説明する。

1 最近の事案

1　インターネットを通じた情報流出事案

防衛省・自衛隊においては、06（平成18）年２月、護衛艦「あさゆき」の秘密情報が、私有パソコンからファイル共有ソフトを介して流出したことが判明するなど、一連のインターネットを通じた情報流出事案が発生した。

このような情報流出事案の発生の背景には、近年の急速なIT化の流れに、防衛省・自衛隊における情報管理体制・意識が追いつかなかったことが挙げられる。

2　イージスシステムに係る特別防衛秘密流出事案

昨年１月、護衛艦「しらね」乗組員の自宅から、秘密の疑いのある情報を記録した外付ハードディスクが発見され、捜査の結果、昨年12月、海上自衛官がイージスシステムに係る特別防衛秘密を漏えいした容疑で逮捕されるとともに、海上自衛官４名が書類送致された。

本事案発生の背景にある問題点としては、①規則違反や秘密資料の安易な複製など、隊員の保全意識が欠如、②秘密にかかわる教育の無許可での実施など、秘密保全態勢が不備、③前述のインターネットを通じた情報流出事案を受けた再発防止に係る抜本的対策の実施以前であり、パソコンなどの管理態勢が不備、④管理者及び保全責任者の指揮監督などが不十分、といったことが考えられる。

本事案については調査の結果、特別防衛秘密の自衛隊外への流出は確認されなかったものの、イージスシステムにかかわる秘密情報が多数の隊員へ流出するなど外部流出のおそれも否定できない状況が存在していたことは、情報保全にかかわる極めて重大な問題であり、海上自衛隊、ひいては防衛省全体としての情報保全態勢に対する国民の大きな不信を招くとともに、日米安全保障体制や関係国との関係にも影響を及ぼしかねないものであった。また、自衛隊内においても、隊員の士気に多大な影響を与えることとなった。

防衛省においては、本事案の事実関係などにつき調査を行い、本年３月、公表した[1]ところである。

1）<http://www.mod.go.jp/j/sankou/report/2008/pdf/080321a.pdf>

2 防衛省における取組

06（平成18）年２月、インターネットを通じた情報流出事案の発生を受け、防衛省では、業務に使用したことのある私有パソコンからのファイル共有ソフトの削除、秘密の情報および必要のない業務用データの削除、私有パソコンによる秘密情報の取扱いの全面禁止などからなる緊急対策を実施した。

この緊急対策の実施に加え、06（同18）年２月、防衛庁長官政務官（当時）を委員長とする「秘密電子計算機情報流出等再発防止に係る抜本的対策に関する検討会」を設置し、再発防止に係る抜本的対策の具体的措置を取りまとめ、同年４月に公表した。その後、同月に防衛庁長官政務官（当時）を長とする「秘密電子計算機情報流出等再発防止に係る対策実施委員会」を設置して、この抜本的対策の実施に取り組んできた。

このような中、イージスシステムに係る特別防衛秘密流出事案が発生したことから、昨年４月、「秘密電子計算機情報流出等再発防止に係る対策実施委員会」を廃止の上、新たに防衛大臣を長とする「情報流出対策会議」を設置し、情報管理の重要性や抜本的対策が末端隊員まで十分浸透していないとの問題意識の下、対策を検討・実施してきた。

これまで防衛省・自衛隊が講じてきた主な情報流出防止対策は、図表Ⅳ-3-1のとおりである。

さらに、本年７月に示された「防衛省改革会議」の報告書の内容を踏まえ、取組を進めていきたいと考えている。

COLUMN

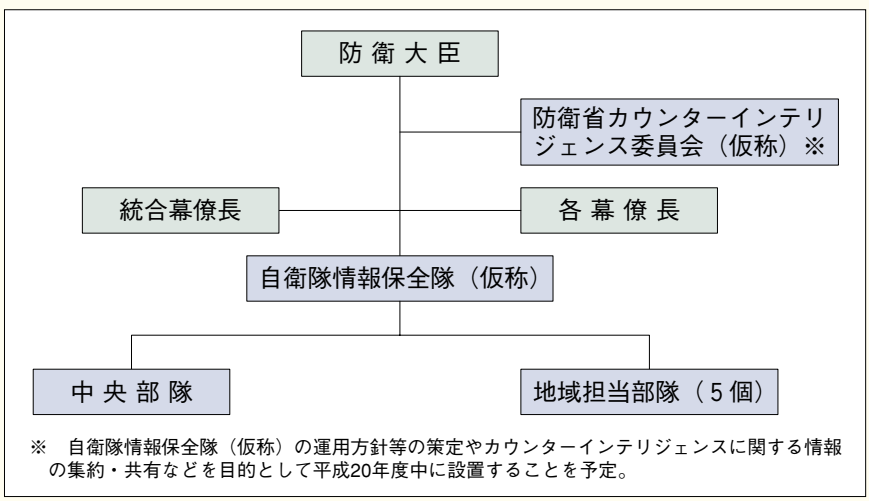
VOICE　解説　Q&A

「自衛隊情報保全隊（仮称）」の新編

情報保全隊は、部隊などの情報保全業務の実施に必要な資料および情報の収集整理などを行うことを任務として、陸・海・空自に設置されている部隊である。

一連の情報流出事案を受け、防衛省における情報保全態勢の強化は極めて重要になっている。防衛省としては、外国による自衛隊への諜報活動から自衛隊が保有する重要な情報を防護する必要性が一層高まっていることを踏まえ、本年度予算においてこれまで陸・海・空自に設置されていた情報保全隊を統合し、共同の部隊として、自衛隊情報保全隊（仮称）を新編するとともに所要の増員を行うことを予定している。

この新編により、自衛隊への諜報活動に関する情報の効率的な収集・集約・分析・共有が可能となり、カウンターインテリジェンスに関する情報保全態勢を強化することができるものと考えている。



※　自衛隊情報保全隊（仮称）の運用方針等の策定やカウンターインテリジェンスに関する情報の集約・共有などを目的として平成20年度中に設置することを予定。

図表Ⅳ－3－1　主な情報流出防止対策について

・人に係る対策

秘密保全のために必要な事項	防衛省として講じた事項
○秘密に接する者を制限	○秘密の取扱者は管理者が「ふさわしい者」を指定 （本人の身上や平素の勤務状況等個別具体の状況を総合的に勘案して判断） ○「need to knowの原則」（※）の下、必要最小限の範囲で指定
○情報管理の重要性を認識	◎秘密保全に係る重い責任を自覚するための「誓約書」の提出 ◎秘密の管理者等の責任の明確化 □情報流出防止に係る全隊員に対する個別指導の実施 □内局幹部を長とする特別行動チームの部隊への派遣
○秘密を扱う者が取扱いのルールを熟知	○全職員を対象に定期的に階級、取扱い情報に応じた保全等の教育を実施 ◎事例集の作成配布・理解度の確認及び情報セキュリティ月間の設定 ◎分散化していた秘密保全関係規則を整理・統合し一覧性のある体系を構築
○秘密漏えいに対する抑止力の強化	◎「省秘（機密・極秘）」について、内容を精査の上、より重い罰則で担保される。「防衛秘密」に移行 （平成13年、自衛隊法を改正して防衛秘密制度を創設し、罰則強化。平成14年施行。） ◎情報漏えいに関する処分基準の明確化 □公益通報制度の活用 □防衛監察本部による監察
○カウンターインテリジェンス	○情報保全隊による保全に必要な情報の収集整理等 ○各国駐在武官等との接触について、保全責任者等の了解を得ることとし、接触状況を報告
○個人的弱点の把握と解消	◎部外者から不自然な働き掛けを受けた場合は保全責任者等へ報告 ○金銭感覚や家庭事情等について個別に身上把握を行い指導を実施

※：「情報は知る必要がある者のみに伝え、知る必要のない者には伝えない。」という原則
◎：18年４月に取りまとめた「秘密電子計算機情報流出等再発防止に係る抜本的対策」以降の対策
□：19年４月から実施している海上自衛隊情報持ち出し事案以降の対策

・秘密の文書に係る対策

秘密保全のために必要な事項	防衛省として講じた事項
○秘密文書の持ち出しの禁止	○秘密文書の保管は、各課等におかれた保全責任者が一元的に実施 ○秘密文書は、簿冊に登録して管理し、三段式文字盤かぎの金庫等に保管 ○一部の庁舎の出入口には、秘密文書の持ち出しを感知し、警報を発する装置を導入
○外部への送達時の漏えい防止	○秘密文書を外部へ送達し又は貸出すには、管理者等の許可が必要であり、その都度簿冊に記録 ○秘密情報の伝達には、内容を暗号化する秘匿電話、秘匿ファックスを使用
○秘密を取り扱う施設への立入の制限	○秘密が取り扱われる主な施設は、立入を禁止。立入禁止の場所等の入出は、ICカード、パスワード又は生体認証により管理
○秘密文書の削減	◎秘密指定の厳格化措置などを講ずることにより、過剰な秘密指定を防止するとともに、秘密文書を削減

◎：18年４月に取りまとめた「秘密電子計算機情報流出等再発防止に係る抜本的対策」以降の対策

・電子データによる対策

秘密保全のために必要な事項	防衛省として講じた事項
○業務用データの職場外への無断持ち出しの禁止	◎職場から私有パソコンを一掃 ・官品パソコンの緊急調達（約56,000台、約40億円） ・私有パソコンの職場への持ち込みを全面禁止 ◎官品パソコンでの私有可搬記憶媒体の使用禁止 ◎規則に違反したデータの持ち出し防止 ・登退庁時、課業時間中の抜き打ち所持品検査の実施 ・ファイル暗号化ソフトの導入により、業務用データの持ち出しを防止 ◎官品可搬記憶媒体の明瞭な標記及び集中管理 ◎官品可搬記憶媒体の管理簿の点検など情報保証に関する対策の遵守状況を調査（定期調査年１回、臨時調査年１回以上、その際第三者性を確保した特別検査チームを派遣）
○自宅のパソコン等での業務用データの取扱いの禁止等	◇職務上使用したことのある私有パソコンからファイル共有ソフト、秘密・必要のないデータを削除 ◎ファイル共有ソフトによる情報流出の危険性等について教育を行い、ファイル共有ソフトの削除を促進 ◎業務用データを私有パソコン等で取り扱っていない旨の誓約書を提出させた上で、本人の同意を得て自宅の私有パソコンの業務用データの有無を「確認」 □上記「確認」については、昨年７月末までに全職員を一巡し、以降は厳罰化
○情報保証の管理体制の強化	◎管理者の補助者について単に役職指定することなく、パソコンの取り扱い等の知見を考慮して指定

◇：18年２月に実施した緊急対策
◎：18年４月に取りまとめた「秘密電子計算機情報流出等再発防止に係る抜本的対策」以降の対策
□：19年４月から実施している海上自衛隊情報持ち出し事案以降の対策