２０．３．２１
防　衛　省

イージスシステムに係る特別防衛秘密流出事案について

１　はじめに

（１）経緯

平成１９年１月２０日、神奈川県警察が、海上自衛隊第１護衛隊群（横須賀）所属の護衛艦「しらね」の乗組員である２等海曹Ａ（以下、階級は２０年３月１日現在のもの。）の自宅を妻の「出入国管理及び難民認定法」違反の容疑で捜索したところ、秘密の疑いのある情報を記録した外付ＨＤが発見された。

秘密の取扱いに係る法令違反の疑いがあることから、神奈川県警察は捜査を進め、１９年４月４日からは、神奈川県警察と海上自衛隊警務隊が協力して捜査を実施した。その結果、同年１２月１３日、１４年当時海上自衛隊艦艇開発隊（横須賀）に所属していた３等海佐Ｂ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（１９年１２月２８日起訴）されるとともに、同月２５日までに、自衛官４名（３等海佐Ｃ、１等海尉Ｄ、２等海曹Ｅ及び海士長Ｆ）が書類送致（２０年１月１１日起訴猶予）された。

（２）調査の実施

海上自衛隊においては、神奈川県警察と海上自衛隊警務隊が協力して捜査を行うこととなった平成１９年４月４日、海上幕僚監部に海上幕僚副長を長とする調査委員会を設置し、捜査に配意しつつ、事案の全容の解明に向け調査を実施してきたところである。

これまでの調査においては、３等海佐Ｂから２等海曹Ａまでのイージスシステムに係る特別防衛秘密流出の経緯及びそれ以外の者への流出の有無について明らかにするため、隊員への聞き取り調査や隊員が保有する私有ＰＣに保存されているデータの確認・分析等を実施した。

以下は、現時点までに調査が終了した事項についてとりまとめたものを報告するものである。

2　調査結果

（1）プログラム業務隊関連

ア　流出した資料の作成

イージスシステム等のプログラムの作成、維持管理等を担当する部隊であったプログラム業務隊（横須賀）のプログラム第２科に勤務する３等海佐Ｇ、３等海佐Ｈ、３等海佐Ｉは、平成９年頃から１２年頃までにかけて、同部隊への新着任者の教育に使用する目的で、米国留学中に得たイージスシステムの性能等に関する知識や米国から供与された文書等を参考に、「イージス概要」と題するパワーポイント資料等の教育用資料を作成した。

これら資料の中には、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の性能等についての情報が含まれていたことから、「日米相互防衛援助協定等に伴う秘密保護法」に規定する特別防衛秘密（以下「特別防衛秘密」という。）に該当するものがあったが、特別防衛秘密としての登録は行われないなど不適切に取り扱われた。

当該資料は、立入禁止区画であるプログラム業務隊プログラム第２科に置かれた官品ＰＣに保存されていたが、１４年３月、プログラム業務隊が廃止され、新たに艦艇開発隊がイージスシステム担当部隊となったことから、同隊開発部艦艇第２科へ引き継がれた。

イ　流出の経緯

（ア）３等海佐Ｂから３等海佐Ｃへの流出

艦艇開発隊開発部艦艇第２科に勤務していた３等海佐Ｂ及び第１術科学校（江田島。以下「１術校」という。）砲術科に勤務していた３等海佐Ｃは、平成１４年５月から７月までの間、「イージスシステム幹部課程」履修のため米国へ留学することとなった。留学に先立ち、３等海佐Ｂは、上司である３等海佐Ｉから「イージス概要」と題する資料等を用いて教育を受けた。

３等海佐Ｂは、留学中の参考とするため、当該資料をＳＤカードにコピーして自宅に持ち帰り、私有ＰＣにコピーした。当該ＳＤカード内のデータは、その後削除された。

３等海佐Ｂは、留学から帰国後、艦艇開発隊においてイージスシステムの担当とならなかったことから日常的にはイージスシステムに係る特別防衛秘密にアクセスすることはなかったものの、業務上の必要から当該秘密

にアクセスすることを認められていた。また、３等海佐Ｃは、１術校において、「イージスシステムの概要」という教務を担当することとなった。

１４年８月頃、３等海佐Ｃは、この教務で使用する教育用資料を作成するため、３等海佐Ｂに参考となる資料を送付するよう依頼した。

３等海佐Ｂは、ともに留学しイージスシステムに係る教育を受けた者からの依頼であり、特別防衛秘密を含む資料を提供しても問題ないと誤って考え、上司である３等海佐Ｉに送付の了解を求めた。

３等海佐Ｉは、送付される資料は留学時の成果をまとめたものであり留学中に得た知識を留学生同士で共有することは特に問題ないと考え、内容を確認することなく、送付を了解した。

３等海佐Ｂは、特別防衛秘密を送付するために必要な手続きを行うことなく、官品ＰＣに保存されていた「イージス概要」と題する資料を含む教育用資料（以下「イージス資料」という。）をＣＤにコピーし、３等海佐Ｃに送付した。

３等海佐Ｃは、当該ＣＤを受領して砲術科教官室内で保管した。

（イ）３等海佐Ｃから１等海尉Ｄへの流出

平成１４年１０月、砲術科教官であった１等海尉Ｄは、イージスシステムに関する知識がないため、担当するイージスシステムに関する教育をどのように実施すべきか３等海佐Ｃに相談した。３等海佐Ｃは、３等海佐Ｂから送付された「イージス概要」と題する資料が参考になると考え、１等海尉Ｄに当該資料を記録するＣＤを貸し出し、私有ＰＣを用いて閲覧させた。

１等海尉Ｄは、資料を勉強したいと考え、３等海佐Ｃが他の業務のために一時的にその場を離れた間に、イージス資料を私有ＰＣにコピーし、その後、当該資料をＣＤにコピーした。

３等海佐Ｃは、返却されたＣＤを他の教官にコピーさせることなく、１術校からの転出時に破棄した。

（ウ）１等海尉Ｄから２等海曹Ｅへの流出

平成１５年９月に護衛艦「しまかぜ」に転出した１等海尉Ｄは、その際、イージス資料を記録したＣＤを艦内に持ち込んだ。

１６年２月末頃、１等海尉Ｄは、同艦乗組みの２等海曹Ｅが近く１術校

「海曹射管課程」に入校予定であることを聞いたことから、今後の勤務の参考に、イージス資料を別のＣＤにコピーした上で、２等海曹Ｅに手渡した。２等海曹Ｅは、「しまかぜ」艦内でＣＤのデータを私有ＰＣにコピーした。

１等海尉Ｄは、１７年３月に「しまかぜ」から転出するまでに、私有ＰＣ内のデータを削除したが、当該資料を記録したＣＤは、その後も自宅で保有していた。

（エ）２等海曹Ｅから海士長Ｆへの流出

平成１６年３月に１術校「海曹射管課程」に入校した２等海曹Ｅは、その際、イージス資料を記録したＣＤ及び私有ＰＣを１術校に持ち込んだ。

同年６月頃、２等海曹Ｅは、「海士射管課程」に入校し居住区が同じであった海士長Ｆから、今後の勤務の参考となる資料を求められたことから、イージス資料をＣＤにコピーし、同居住区において、海士長Ｆに貸し出した。海士長Ｆは、私有ＰＣを使用して当該ＣＤに記録されたイージス資料を外付ＨＤにコピーした。

２等海曹Ｅは、１８年２月の護衛艦「あさゆき」におけるインターネット上への情報流出事案（以下、「あさゆき事案」という。）を契機に、ＣＤ及び私有ＰＣ内のデータを削除した。

（オ）海士長Ｆから２等海曹Ａへの流出

平成１６年８月に護衛艦「はつゆき」に転出した海士長Ｆは、その際、外付ＨＤを同艦に持ち込んだ。

１７年２月頃、海士長Ｆは、居住区が同じであった２等海曹Ａから、海士長Ｆの外付ＨＤ内の動画や画像のデータのコピーを希望されたことから、２等海曹Ａに外付ＨＤを貸し出した。

２等海曹Ａは、艦内において、海士長Ｆの外付ＨＤのデータを私有ＰＣ及び外付ＨＤにコピーし、その後、私有ＰＣ内のデータを削除した。

海士長Ｆは、「はつゆき」退艦直前の１８年１０月頃、外付ＨＤ内のデータをＤＶＤにコピーし、外付ＨＤ内のデータを削除した。また、ＤＶＤは、同月末頃、破棄した。

（カ）２等海曹Ａの外付ＨＤの取扱い

２等海曹Ａは、平成１８年２月の「あさゆき事案」を契機として外付ＨＤを自宅で保有していたところ、１９年１月２０日、神奈川県警察に当該外付ＨＤが押収され、本事案が発覚した。

（２）第１術科学校関連

ア　第１術科学校における特別防衛秘密の取扱い

１術校においては、平成１２年８月から「イージスシステムの概要」を含む「誘導武器システム」という教務が開始された。

この教務においては、イージスシステムに係る特別防衛秘密を用いることとはされていなかったにもかかわらず、個々の教官の判断により、それを用いた教育が事実上行われていた。

特に、１１年８月から１２年１２月にかけて砲術科教官（射撃班長）としてイージスシステムの教育を担当していた２等海佐Ｊは、「イージスシステム幹部課程」履修のため１１年９月から１２月まで米国留学した際に習得した知識を利用して、１２年８月頃、イージスシステムに係る特別防衛秘密に該当する「誘導武器システム」と題するパワーポイント資料を作成した。

当該資料は、特別防衛秘密に該当するものであったが、特別防衛秘密として登録を行うなどの管理が行われず、１２年１２月の２等海佐Ｊの転出後は、ＭＯに記録され、歴代教官（射撃班長）５名（１等海尉K1、３等海佐K2、１等海尉K3、２等海佐K4及び３等海佐K5）に引き継がれた。また、１３年８月から１５年９月まで砲術科教官であった１等海尉Ｄ及び１４年３月から１５年７月まで同教官であった３等海佐Ｃにも当該資料が渡された。

２等海佐Ｊは、１７年１月、護衛艦「きりしま」に転出した際、当該資料をＭＯに記録して同艦に持ち込んだが、同年３月頃、削除した。

イ　資料の流出

イージス資料又は「誘導武器システム」と題する資料は、次の課程においても学生に流出していたことが判明した。

（ア）第１４０２期幹部中級一般課程

平成１５年３月頃、「第１４０２期幹部中級一般課程」担当教官であった１等海尉Ｄは、同課程学生であった３等海佐Ｌに艦艇武器について質問

されたことから、「誘導武器システム」と題する資料の一部を３等海佐Ｌの私有ＵＳＢメモリにコピーした。

その後、３等海佐Ｌは、当該資料を外付ＨＤにコピーして自宅で保有し、当該ＵＳＢメモリ内のデータを削除した。

（イ）第１４０３期幹部任務射撃課程

平成１５年１月、「第１４０３期幹部任務射撃課程」担当教官であった１等海尉Ｄは、同課程学生であった１等海尉Ｍに、教育参考資料として、イージス資料、「誘導武器システム」と題する資料等を記録したＣＤを貸し出した。１等海尉Ｍは、これを私有ＰＣにコピーするとともに、同期学生であった１等海尉Ｎに手渡し、１等海尉Ｎは、私有ＰＣ、ＣＤ及び外付ＨＤにコピーした。

１等海尉Ｍは、１５年頃、私有ＰＣ内のデータを削除し、１等海尉Ｎは、１８年２月の「あさゆき事案」を契機に、私有ＰＣ、ＣＤ及び外付ＨＤ内のデータを削除した。

（ウ）第１５０１期幹部任務射撃課程

平成１５年４月、「第１５０１期幹部任務射撃課程」担当教官（射管班長）であった３等海佐Ｃは、イージス資料に含まれる「イージス概要」と題するパワーポイント資料に一部変更を加え、新たに「イージスシステム」と題するパワーポイント資料を作成した。

同年５月頃、３等海佐Ｃは、資料の一部を同課程の教務で使用したところ、同課程の学生であった２等海尉Ｏは、休憩時間中に当該資料を私有ＵＳＢメモリにコピーした。

２等海尉Ｏは、その後、同資料を他の参考資料とまとめてＣＤにコピーし、希望する同期学生４名（２等海尉P1、２等海尉P2、３等海佐P3及び２等海尉P4）に配布した。

このうち２等海尉Ｏ、２等海尉P1及び２等海尉P2は、１８年２月の「あさゆき」事案を契機に当該資料を削除したが、３等海佐P3及び２等海尉P4はその後も自宅で保有した。

また、３等海佐Ｃは、「イージスシステム」と題する資料をＭＯに記録し、後任の歴代教官（射管班長）２名（３等海佐Q1及び３等海佐Q2）に引き継いだ。

（エ）第１５０１期幹部中級射撃課程

「第１５０１期幹部中級射撃課程」学生であった３等海佐Ｒは、入校期間中の平成１５年８月から１６年７月までの間、過去にプログラム業務隊での勤務経験があったことから、教官を補佐してイージスシステムに係る教務を実施した。その際、３等海佐Ｒは、教官であった３等海佐K2から「誘導武器システム」と題する資料を記録したＭＯを借り受け、当該資料の一部を私有ＰＣにコピーしたが、その後削除した。

（オ）第１６０１期海曹射管課程及び第１６０１期海士射管課程

「第１６０１期海曹射管課程」学生であった２等海曹Ｅは、平成１６年６月頃、１等海尉Ｄから入手したイージス資料をＣＤにコピーして、「第１６０１期海曹射管課程」に入校していた同期学生のうち希望した２名（１等海曹S1及び２等海曹S2）及び「第１６０１期海士射管課程」に入校していた同期学生のうち希望した３等海曹Ｔに配布した。

また、同時期、「第１６０１期海士射管課程」に入校中の海士長Ｆは、２等海曹Ｅから入手したイージス資料を同期学生であった海士長Ｕの私有ＵＳＢメモリにコピーした。

資料を受領した学生は、１８年２月の「あさゆき事案」等を契機にデータを削除した。

（カ）第１７０１期幹部中級船務課程

「第１７０１期幹部中級船務課程」学生であった３等海佐Ｖは、平成１７年８月から１８年７月までの間、過去にプログラム業務隊での勤務経験があったことから、教官を補佐してイージスシステムに係る教務を実施した。その際、３等海佐Ｖは、「イージスシステム」と題する資料を保存したＭＯを借り受け、当該資料に変更を加えた上で私有ＰＣに保存したが、その後削除した。

（キ）第１７０１期海曹射管課程等

「第１７０１期海曹射管課程」学生であった３等海尉Ｗは、平成１７年５～７月頃、「誘導武器システム」と題する資料を入手した。

その後、３等海尉Ｗは、１８年５月頃、第１輸送隊（呉）で同僚だった

海曹長Ｘが幹部候補生学校（江田島）に入校することとなったことから、教育の参考として、海曹長Ｘに当該資料を記録したＤＶＤを譲り渡した。海曹長Ｘは、当該ＤＶＤを職場で保有した。

（３）その他

上記以外にも次の事案が判明した。

ア　３等海佐Ｇから１等海尉Ｙへの流出

３等海佐Ｇは、平成１２年３月、プログラム業務隊から護衛艦「みょうこう」に転出する際、今後の業務の参考とするため、プログラム業務隊で使用していたイージス資料及びこれに一部修正を加えたパワーポイント資料を保存した私有ＰＣを同艦に持ち込み、資料の一部を士官室の官品ＰＣにコピーした。

１３年３月、３等海佐Ｇは、官品ＰＣにコピーした資料を削除することなく、「みょうこう」から転出し、その後も、資料を保存した私有ＰＣを自宅で保有した。

同年３月、「みょうこう」に転入した１等海尉Ｙは、同年７月頃、士官室の官品ＰＣに当該資料を発見し、今後の勤務の参考とするため、私有ＰＣにコピーして職場で保有していた。その後、１等海尉Ｙは、１８年２月の「あさゆき事案」を契機に、私有ＰＣを自宅に持ち帰ったが、その際、データを削除しなかった。

イ　３等海佐Ｈによる持ち出し

プログラム業務隊に勤務していた３等海佐Ｈは、平成１３年頃、職場に官品ＰＣが整備されたことに伴い、イージス資料及びこれに一部修正を加えた資料を記録した私有ＰＣを自宅に持ち帰った。

その後、３等海佐Ｈは、１８年２月の「あさゆき事案」を契機に、当時勤務していた護衛艦「いそゆき」艦内の外付ＨＤに私有ＰＣのデータをコピーし、私有ＰＣ内のデータを削除した。

ウ　１等海尉Ｄから１等海曹Ｚへの流出

平成１５年９月、護衛艦「しまかぜ」に転出した１等海尉Ｄは、同年１１月頃、同艦乗組員である１等海曹Ｚから、業務上参考になる資料がないか相

談され、同艦に持ち込んでいたイージス資料が記録されたＣＤを１等海曹Ｚに貸し出した。

１等海曹Ｚは、射撃管制室の官品ＰＣに当該資料をコピーした。

１５年１１～１２月頃、当該官品ＰＣにアクセスした射撃管制員３名（３等海曹ａ1、３等海曹a2及び３等海曹a3）が、今後の業務の参考になると考え、私有ＰＣに当該資料の一部をコピーした。

これらの射撃管制員は、１８年２月の「あさゆき事案」を契機に、私有ＰＣ内のデータを削除した。

３　問題点

（１）隊員の保全意識の欠如

関係当事者は、特に幹部を中心として、取り扱う情報が秘密と知りながら、関係規則を遵守することなく、無許可で特別防衛秘密を複製、送付、保有するなど、自衛隊において取り扱う情報の重要性の認識や情報保全の意識が著しく欠如していた。特に、プログラム業務隊及び艦艇開発隊においては、特別防衛秘密を取り扱う部署であるにもかかわらず、隊員に対する規則の遵守の徹底がなされず、無許可の特別防衛秘密の送付等秘密の不適切な取扱いがなされていた。

また、関係当事者の中には、秘密にアクセスする業務上の必要性について適切に上司の判断を仰ぐことなく、教育の向上又は勤務の参考といった理由を単独で判断し、秘密を広範に配布するなどしており、「Need to Know の原則」（情報は知る必要のある者にのみ伝え、知る必要のない者には伝えない」という原則）の不徹底がみられた。

さらにＰＣ等の普及や可搬記憶媒体の大容量化に伴い、膨大な量の情報を容易に保存、コピー又は携帯することが可能となった状況下、曹士クラスを中心とした関係当事者間において、教育用資料等の業務用データの必要性の有無を深く考えず、又は秘密が含まれているとの認識のないまま、安易に資料を収集し、保存する傾向にあったことも、秘密の拡散を招いた。

加えて、平成１８年４月に取りまとめられた「秘密電子計算機情報流出等再発防止に係る抜本的対策の具体的措置」（以下、「抜本的対策」という。）の実施以降は私有ＰＣ等での業務用データの取扱いが禁止されたにもかかわらず、依然として私有ＰＣ等において業務用データを保有していた者がおり、「抜本

的対策」が未だ全ての隊員に浸透していなかったことが明らかとなった。

（２）秘密保全態勢の不備

１術校は、イージスシステムに関する特別防衛秘密を使用して教育を行うこととはされていなかったにもかかわらず、かかる教育が個々の教官の判断で事実上行われていた。そのため、特別防衛秘密の取扱いに必要な関係規定に基づく秘密保全態勢が構築されず、特別防衛秘密の適切な取扱いもなされていなかった。

また、同校砲術科教官室においては、教育用資料が砲術科内に限り使用されることを前提に作成され、教務内容の充実を目的として各教官が日常的に修正等を行っていた状況の下、教育用資料が秘密を含むものであっても、秘密文書等としての登録がなされなかった。

（３）ＰＣ等の管理態勢の不備

「抜本的対策」の実施以前の当時においては、各部隊等において使用するＰＣ及び可搬記憶媒体の管理態勢が不十分であり、業務用データの外部持出しに対するチェックも行われていなかったなど、秘密も含め業務用データの取扱いに問題があった。

例えば、当時の１術校においては、教官及び学生は、私有ＰＣ及び可搬記憶媒体の教官室及び居住区への持込みを許可されていたが、転出等に伴い私有ＰＣ等を持ち帰る際の業務用データの削除等について、確認も指導も十分になされていなかった。また、教官室においてさえ、秘密を含む可搬記憶媒体が登録もされないまま各教官の机の中で保有されていたなど、基本的な管理がなされていなかった。

（４）管理者及び保全責任者の注意義務違反及び指揮監督不十分

プログラム業務隊及び艦艇開発隊においては、秘密の管理者及び保全責任者（以下「管理者等」という。）による秘密の管理、指導が徹底されず、無許可の持出しや他部隊への送付を防止できなかった。

１術校においては、管理者等によるイージスシステムに関する教育用資料の取扱い状況の把握がなされず、当該資料の不適切な取扱い及び学生への配布を防止できなかった。

また、関係当事者が勤務していた部隊等全般にわたり、業務で使用した私有

ＰＣ等を持ち帰る際の管理者等による確認、指導が徹底されず、隊員が秘密の資料を不適切に取り扱っていたことを把握できなかった。

さらに、一部の部隊等においては、「抜本的対策」以降に実施した私有ＰＣ等の検査が徹底されず、例えば２等海曹Ａが私有ＰＣ等を保有していないとの虚偽の申告をしたため、特別防衛秘密を自宅に保有していることを発見できなかったなど、隊員が私有ＰＣ等に秘密の業務用データを保有していたことを把握できなかった。

4　事案が与えた影響

本調査において、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係る秘密情報が、海上自衛隊内において多数の隊員へ流出し、また、一部隊員はそれを自宅で保有していた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、情報保全に係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。

5　再発防止対策

かかる事態を深刻に受け止め、情報流出の防止については、引き続き、平成１８年４月の「抜本的対策」や本事案を受けて設置された防衛大臣を長とする「情報流出対策会議」のもとで講じられた対策等を徹底的に推進していくとともに、今後、官邸に設置された「防衛省改革会議」の議論を踏まえて講じられる対策も通じ、信頼回復に全力を尽くして行く。

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（実施予定のものを含む。）は別紙のとおりである。また、海上自衛隊における１８年以降の新たな対策について、本事案の問題点ごとに整理すれば以下のとおりである。

（１）保全意識に係る対策

- 情報セキュリティ及び秘密保全に係る教育の充実
- 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

・　可搬記憶媒体による秘密情報の持出し等を防ぐための抜打ち所持品検査等の実施
・　情報漏えいに関する処分基準の明確化
・　内局の課室長をチーム長とする特別行動チームの地方派遣
・　全隊員に対する個別面談指導の実施
・　全隊員の自宅私有ＰＣ等の業務用データの有無の確認
・　業務用データの不正持ち出しに対する処分の厳罰化
・　情報セキュリティ月間の設定
・　情報保全マニュアルの作成配布による規則等の周知徹底
・　「Need to Know」の原則を徹底するため「知る必要のある者」の範囲の更なる明確化（今後実施予定）

（２）秘密保全態勢に係る対策
・　海上幕僚監部による部隊等に対する秘密保全態勢の点検の計画的実施
・　１術校における教育でイージスシステムに係る特別防衛秘密を取り扱う必要性を精査し、必要最小限の範囲で関係職員を指定するなど保全態勢の確立
・　１術校における施設の出入り、ＰＣへのアクセス等に対する個人認証による管理機能の強化

（３）ＰＣ等の管理態勢に係る対策
・　官品ＰＣの整備及び私有ＰＣの職場への持込み全面禁止
・　私有ＰＣ及び私有可搬記憶媒体による業務用データの取扱禁止
・　官品可搬記憶媒体の集中管理
・　情報セキュリティに関する制度の遵守状況調査の実施
・　ファイル暗号化ソフト（強制的にファイルを暗号化）の導入
・　特別防衛秘密を扱う部隊等の教育用ＬＡＮ等について、端末でのコピーを不可能とするシンクライアントシステムの導入

（４）管理者等の指揮監督責任等に係る対策
・　管理者等の階級に応じた教育の充実
・　管理者等の責任及び処分基準の明確化

別　紙

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 ＊「知る必要のある者」の範囲の明確化
○　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 □　全隊員に対する個別面談指導の実施 □　特別行動チームの部隊への派遣 ＊　誓約内容の強化、啓発活動
○　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等	◎　「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 □　業務用データ不正持出しに対する処分の厳罰化 □　公益通報制度の活用 □　防衛監察本部による監察 ＊　情報保全の観点から捜査能力の強化等を目的とした警務隊の統合
○　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 ◎　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 ＊　自衛隊情報保全隊(仮称)の新編
○　個人的弱点の把握と解消	○　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

◎：１８年４月の「秘密電子計算機情報流出等再発防止に係る抜本的対策」以降実施した対策
□：１９年４月の「情報流出対策会議」設置以降実施した対策
＊：今後実施予定の対策

・　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

・電子データに係る対策

秘密保全のために必要な事項	防衛省として講じた事項
○　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） ・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 ◎　データの不正持出し防止 ・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 ◎　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 □　所要部隊へのシンクライアントシステムの導入
○　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
○　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月の「秘密電子計算機情報流出等再発防止に係る抜本的対策」以降実施した対策
□：１９年４月の「情報流出対策会議」設置以降実施した対策