

平成 24 年 5 月 25 日
総合政策局・海上保安庁

情報流出再発防止対策検討委員会報告書について

今般、情報流出再発防止対策検討委員会報告書が取りまとめられましたので、お知らせいたします。

<資 料>

1. 情報流出再発防止対策検討委員会報告書（概要）
2. 情報流出再発防止対策検討委員会報告書

【問い合わせ先】

海上保安庁総務部情報通信課情報セキュリティ対策官

池田 聡（内線：2905）

海上保安庁総務部政務課課長補佐

福本 拓也（内線：2103）

代表：03-3591-6361

直通：03-3591-9700（情報通信課）

情報流出再発防止対策検討委員会報告書(概要)

1 今般の映像流出事案の概要

平成22年9月7日、尖閣諸島領海内で中国漁船による巡視船への衝突事件が発生した。事件発生の前後をビデオ撮影した映像は、当初より公開しないことが組織の方針であったにもかかわらず、組織としての情報管理が十分でなかったために、同年11月4日、本件事件捜査に直接関係のない神戸海上保安部巡視艇乗組員(当時)が、インターネット上に衝突映像を故意に流出させた。

2 今般の映像流出事案の分析

- (1) 衝突映像については、これを公開しないこととしていた組織の方針に反して、職員が、インターネット上に、故意に映像を流出させたことが最も大きな問題。
- (2) 当該職員等が映像を入手できる状況を招いた背景に、情報セキュリティに対する職員の意識・理解不足、組織の方針の不徹底等海上保安庁の情報管理の不備がある。

3 情報流出再発防止対策検討委員会の設置等

平成22年12月22日、国土交通大臣から海上保安庁に対して、情報流出再発防止対策のあり方について抜本的に見直しを行うよう指示がなされるとともに、情報システム、コンプライアンス、司法プロセスの3分野の有識者により、海上保安庁における情報流出再発防止対策のあり方について抜本的な見直しを行うため情報流出再発防止対策検討委員会が設置された。

当該委員会においては、海上保安庁が国民の信頼を回復し、今後も適確に海上保安業務を遂行していくためには、組織を挙げて再発防止に万全を期す必要があるとの基本認識に立ち、コンプライアンスの向上、情報セキュリティの強化等の再発防止策について平成23年5月までに計4回の会議を開催し、その結果を中間報告書としてとりまとめた。中間報告書における海上保安庁における情報流出再発防止のために必要な改善

策として提言されている事項は以下のとおりである。

(1) 職員の意識に係る改善策

① 職員の意識や理解の促進

職員に必要な国家公務員としての職業倫理を含むコンプライアンスや情報管理に関する意識の促進のため、現行の教育研修内容を再点検し、海上保安官としての服務・規律の必要性や情報管理の必要性についての本質的な理解に重点を置いた教育研修・指導を実施。

② 幹部職員の認識の高揚

組織として情報管理を推進すべき幹部職員の意識を高めるため、情報管理の重要性を意識付ける研修の実施や各組織の長をトップとする情報管理推進のための常設の会議を設置。

③ 組織における方針の徹底

組織内で良好なコミュニケーションを保持、特に社会的関心の高い事案の発生時は、海上保安庁の方針に関し、組織としての認識を共有化。

(2) 規則やマニュアル等に係る改善策

職員の行動の指針として、捜査関係業務等様々な業務に即し、具体的な情報の格付けの基準や取扱い要領を明らかにした規定・マニュアルを整備。

(3) 情報システムに係る改善策

① 海上警察機関として情報管理に万全を期すため、庁内で情報を作成・伝送・共有する業務上の情報システムについては、クローズ系システムとするべきであり、その整備に向けた具体的な方策について早急に検討。

② 情報システムの自動暗号化、証跡管理の強化は、可能なものから順次実施。

(4) 情報管理に関する組織に係る改善策

管区の組織体制の見直しや必要な要員の配置等、本庁から部署、船艇まで、情報セキュリティ対策等を総合的かつ一体的に推進するための体制を整備。

4 中間報告書提言事項に対する海上保安庁の取組み状況

(1) 職員の意識に係る改善策

- ・ 各階層に対する情報管理に関する研修の実施
- ・ 各組織の長をトップとする「情報管理推進会議」の設置

- ・各種会議やテレビ会議の活用でコミュニケーションを保持等を実施することにより、職員の意識や理解の促進、幹部職員の認識の高揚、組織における方針の徹底を図った。

(2) 規則やマニュアル等に係る改善策

- ・捜査書類等の情報システム上の取扱い等に関する内部規則を制定
- ・各種マニュアルやガイドラインの策定

等を実施することにより、情報の取扱いの具体化及び手順の明確化を図った。

(3) 情報システムに係る改善策

- ・行政情報システム等の暗号化の推進
- ・クローズ系システムの導入に向けた調査の実施

等を実施することにより、情報システムのセキュリティ対策の強化を図った。捜査機関である海上保安庁においては、クローズ系システムの整備を早急に進める必要がある。

(4) 情報管理に関する組織に係る改善策

- ・管区本部の事務所であった情報通信管理センターを管区本部の内部組織に改編
- ・情報セキュリティ担当要員の増員

等を実施することにより、情報セキュリティ対策等を総合的かつ一体的に推進するための体制を整備した。

5 おわりに

今後も技術の進展、海上保安庁を取り巻く状況の変化等に応じ、情報管理に関する対策は引き続き見直していかなければならない。また、海上保安庁が今後取り組むべき対策には、定員及び予算上の措置や技術的な検討が必要なものも多いが、対策の推進に積極的に取り組むことを強く期待するものである。

情報流出再発防止対策検討委員会 報告書

平成 24 年 5 月 25 日
情報流出再発防止対策検討委員会

目 次

はじめに

I 今般の映像流出事案

- 1. 本件事案の概要 2
- 2. 本件事案の分析 3

II 海上保安庁における情報流出再発防止のために必要な改善策

- 1. 職員の意識に係る改善策 4
 - (1) 職員の意識や理解 4
 - (2) 幹部職員の認識 6
 - (3) 組織における方針の徹底 6
- 2. 規則やマニュアル等に係る改善策 7
- 3. 情報システムに係る改善策 8
- 4. 情報管理に関する組織に係る改善策 10

III 中間報告書提言事項に対する海上保安庁の取組状況と評価

- 1. 職員の意識に係る改善策 10
- 2. 規則やマニュアル等に係る改善策 11
- 3. 情報システムに係る改善策 11

4. 情報管理に関する組織に係る改善策	11
---------------------	----

おわりに

【資料】

- 情報流出再発防止対策検討委員会開催経緯
- 情報流出再発防止対策検討委員会委員名簿

はじめに

平成22年11月4日、神戸海上保安部の巡視艇乗組員（当時）が、動画サイト「YouTube」に中国漁船衝突事件の映像情報をアップロードし、故意にインターネット上に流出させるという事案が発生した。

同年12月22日、当該乗組員をはじめとする関係者に対する懲戒等の処分が行われ、同時に国土交通大臣から海上保安庁に対して、情報管理に関する当面の緊急対策を講じるとともに、情報流出再発防止対策のあり方について抜本的に見直しを行うよう指示がなされた。

当委員会は、この国土交通大臣の指示を受け、情報システム、コンプライアンス、司法プロセスの3分野の有識者により、海上保安庁における情報流出再発防止対策のあり方について抜本的な見直しを行うため設置された。

当委員会においては、海上保安庁が国民の信頼を回復し、今後も適確に海上保安業務を遂行していくためには、組織を挙げて再発防止に万全を期す必要があるとの基本認識に立ち、コンプライアンスの向上、情報セキュリティの強化等の再発防止策について平成23年5月までに計4回の会議を開催し、その結果を中間報告書としてとりまとめた。

中間報告書には、「政府における情報保全に関する検討委員会」における検討結果を踏まえ、さらに検討すべき事項があれば、最終的な報告として提言を追加することとしていたが、今般政府における検討状況及び海上保安庁の提言事項に対する取組み状況を踏まえ、最終的な報告書としてとりまとめたものである。

I 今般の映像流出事案

1. 本件事案の概要

(1) 平成22年9月7日、尖閣諸島の領海内において、違法操業を行っていた中国漁船が巡視船に船体を衝突させるという公務執行妨害事件が発生し、石垣海上保安部所属の巡視船乗組員が事件発生の前後をビデオ撮影した。

9月8日、石垣海上保安部は、中国漁船船長を公務執行妨害容疑で通常逮捕し、9月9日、那覇地方検察庁に身柄付送致した。

石垣海上保安部は、捜査の過程で、事件発生の前後を撮影したビデオ映像（以下「本件衝突映像」という。）を編集し、事件の説明のための資料（以下「事件説明用映像資料」という。）として那覇地方検察庁及び第十一管区海上保安本部（以下「十一管区本部」という。）に手交した。

(2) その後、海上保安大学校（以下「大学校」という。）に本件衝突映像を鑑定囑託することとなったことを受け、9月17日、十一管区本部は、正式鑑定の前の事前確認のために、事件説明用映像資料を行政情報システムを使用して大学校に伝送することとした。その際、

① 十一管区本部の担当者は、まず、十一管区本部側の行政情報システム端末機のデスクトップ上に作成した共有フォルダに事件説明用映像資料を掲載し、大学校側にアクセス権限を付与する方法で伝送を試みたが、システムの構成上、大学校側からアクセスできなかったため断念した。

② 次に、十一管区本部の担当者は、大学校のパブリックフォルダに事件説明用映像資料を掲載し、大学校側が取り出す方法により伝送することとしたが、大学校側が何度か試みても掲載された映像を取り出すことができなかった。

この際、大学校のパブリックフォルダに掲載された事件説明用映像資料の削除について大学校と十一管区本部の担当者間で確認しなかったため、9月17日から9月22日までの間、事件説明用映像資料が大学校のパブリックフォルダに掲載されたままとなった。また、当該パブリックフォルダにはアクセス制限が付されていなかったため、その間、不特定多数の海上保安庁職員が本件衝突映像を視聴等可能な状態となっていた。

(3) 9月17日から9月22日までの間に、複数の管区の職員が当該パブリックフォルダ内の本件衝突映像を視聴していた。本件衝突映像を後に流出させた職員の同僚職員である神戸海上保安部巡視艇乗組員も9月19日に大学校のパブリックフォルダにアクセスした際、偶然、事件説明用映像資料を発見し、巡視艇内の行政情報システム端末機に保存するとともに、複数の当該巡視艇乗組員に本件衝突映像を視聴させた。

(4) 10月31日、当該巡視艇乗組員の一人が、巡視艇内の行政情報システム端末機から事件説明用映像資料を私有USBメモリに保存して部外に持ち出した。

11月4日、当該職員は、神戸市内のインターネットカフェにおいて、動画サ

イト「You Tube」に本件衝突映像をアップロードし、インターネット上に流出させた。

- (5) 11月10日、しょう戒活動中の当該巡視艇内において、当該職員は同船船長に対し、自分が本件衝突映像を流出させた旨申告した。

2. 本件事案の分析

- (1) 本件事案は、海上保安庁の一職員が業務に係る情報を許可なく私有USBメモリを使用して部外に持ち出し、インターネット上に流出させたものであるが、当該情報を非公開とする組織としての方針に反して故意に流出させた点が最も大きな問題である。

海上保安庁においては、本件衝突映像は、刑事事件の証拠となりうるものであることや海上警備、取締活動の秘匿性等を考慮し、当初から公開しないことが組織の方針であった。他方、本事件は社会的関心が高く、本件衝突映像についても社会に広く公開するべきであるという主張が一部にあることは報道されていた。

このように社会的関心の高い事案が発生した場合には、海上保安官も一般の国民と同様に各種事案に関して様々な個人的な考えを持つことは当然ありうる。しかしながら、流出した本件衝突映像は、業務に係る情報であり、その取扱いについては組織としての方針に従うべきことは言うまでもない。流出させた職員は、海上保安庁という組織の一員である以上、業務に係る情報の取扱いについて、組織としての方針に従うことは、公務員として当然の責務である。

本件事案は、こうした公務員としての基本的な事項に関する意識や理解が十分でなかったことによって引き起こされたものである。

- (2) さらに、流出させた職員のみならず、本事件を担当している部署以外の多数の海上保安官が本件衝突映像を視聴できたことは、海上保安庁の情報管理が十分ではなかったことを示している。

すなわち、十一管区本部から事件説明用映像資料を大学校に伝送する際に、当該映像は「訴訟に関する書類」として非公開であることから慎重な取扱いが必要であったにもかかわらず、情報の内容に応じた格付けがなされず、アクセス制限等も行われていなかった。この点は明らかに規則違反であり、適切な映像伝送手段の選択等情報システムの機能に対する担当職員の理解不足も認められる。

また、実際に本件衝突映像を見た多数の職員が、非公開とする組織としての方針があるにもかかわらず、パブリックフォルダに掲載されていることを知りつつ、また、それを見たことを上司等に報告していなかったことも問題である。

このことから、本件事案を通じて情報セキュリティに対する職員の意識や理解、情報管理に関する組織的なチェック機能が必ずしも十分ではなかったこ

と、業務に関する組織としての方針が組織内に徹底されていなかったこと等がうかがわれる。

Ⅱ 海上保安庁における情報流出再発防止のために必要な改善策

I に述べた本件事案の概要や分析を踏まえれば、海上保安庁における情報管理については、大きく分けて次の四つの分野に関し、必要な改善策を検討することが必要である。

ただし、四つの分野別改善策は、情報流出の再発防止という共通目標に関して、相互に関連性・補完性を有するものである。したがって、その実行にあたっては、全体としてバランスが取れた形で推進するべきである。

- ① 職員の意識に係る改善策（国家公務員としての職業倫理、職員全般のサービスや情報管理に関する意識、情報管理の重要性に関する幹部職員の認識、組織としての方針の徹底等）
- ② 情報の格付けや取扱制限に関する規則やマニュアル等に係る改善策
- ③ 情報システムに係る改善策
- ④ 情報管理に関する組織に係る改善策

1. 職員の意識に係る改善策

(1) 職員の意識や理解

【現状と問題点】

イ 海上保安庁に対する国民の信頼は、警備、救難、航行安全といった日々の海上保安業務を遂行することによって培われてきたものである。また、業務遂行に必要な国家公務員としての倫理やサービスをはじめとする海上保安官として必要な知識、能力、使命感等は、専門の教育機関における初任教育のみならず巡視船艇や航空機における日々の業務遂行や現場研修の中で教育が行われてきた。

ロ 行政機関である以上、業務遂行を適切に行うべきことは言うまでもないが、現場執行機関である海上保安庁においては、日々の業務を組織としての方針に従って一体となって実施していくことが何よりも重要である。

ハ 最近、海上保安庁の業務がますます重要になっており、社会的関心の的となることも多い。その場合、個々の職員が海上保安庁が行っている業務遂行の方針に関して様々な考えを持つことはありうる。今回、本件衝突映像を流出させた職員も公開しないという組織としての方針を知りつつ、個人の信条としてやらなければならないことを行ったとその動機を述べている。

ニ しかしながら、組織としての方針よりも職員個人の思いを優先して、組織の方針に反したことが対外活動として行われることになれば、海上保安庁の組織・機能を全体として見た場合、その適切な業務の実施に多大な支障を生じ、その

結果として、国民の海上保安庁に対する要請にも応えられないこととなるのは明らかである。組織としての方針に従って業務を行うことは、海上保安官として最も基本的な事項であり、これまでの服務に関する教育研修をはじめとする国家公務員としての職業倫理を含むコンプライアンスに関する意識向上のための取組みが実効的でなかったといわざるを得ず、点検のうえ再構築する必要がある。

ホ また、情報セキュリティに関する教育研修が学校教育や現場赴任後の各組織において行われているが、船艇勤務職員が多いこと等から必ずしも全員が受講できていないほか、研修内容がセキュリティ対策の技術的事項に偏りがちであり、情報管理が海上保安庁において如何に重要であるかといった職員の意識に係る教育研修が必ずしも十分ではない。さらには各職員のそれぞれの業務に即した理解しやすい研修資料の整備も十分ではなく、情報システムの機能に対する担当職員の理解不足も認められる。

【改善策】

イ 国の行政機関である海上保安庁の一員として、組織としての方針に従って職務に従事しなければ、真にその職責を果たしたことにはならないという基本を各職員に再度徹底するため、大学校及び海上保安学校における初任教育、現場赴任後の初任者研修や階層別研修等、各教育研修のカリキュラムを再点検し、国家公務員としてのコンプライアンスや情報管理に関する意識強化のための教育研修を適確に実施するべきである。

コンプライアンスに関する教育研修は、対象者の経験、年齢構成等に応じ、ケーススタディを活用する等効果的手法について検討するとともに、海上保安官としての服務や規律の必要性についての本質的な理解に重点を置くよう努めるべきである。

ロ また、日々の業務遂行の中において、各級幹部が部下に対し、公務員としての自覚を促すとともに、コンプライアンスのあり方等を適確に指導していくことが重要である。

ハ 全職員に対して情報セキュリティに関する研修を毎年度確実に実施するため、それぞれの年度における研修の重点項目を明らかにするとともに、各部署はそれぞれの業務の実情に応じて研修の実施時期、手法等を検討するべきである。また、研修後の小テストの実施、研修履歴管理等、研修効果について組織的な把握が可能な仕組みを検討するべきである。

ニ 情報セキュリティに関する研修については、それぞれの業務の実態を反映したわかりやすい研修資料を作成することが重要であるが、その場合においても技術的事項に偏ることなく、情報管理の必要性についての本質的理解に重点を置くとともに、情報管理の基本である「Need to Knowの原則」（情報は知る必要のある者のみに伝え、知る必要のない者には伝えないという原則）の意識付けやカウンターインテリジェンス対策等についても、総合的に理解させるよう努めるべきである。

ホ 情報管理強化のための取組みが各組織において継続的に実施されることを確保するため、各組織に対する効果的な情報セキュリティ監査を定期的を実施すべきである。また、様々な周知啓発活動等を定期的、かつ、確実に実施していくことも、職員の情報管理意識の向上を図るうえで有効である。

(2) 幹部職員の認識

【現状と問題点】

個々の職員の意識、業務内容等に応じて指導育成を図り、規則やシステムの整備を推進する等、各組織において情報管理の実効性を高めるうえでは、幹部職員の情報管理の重要性に関する認識とリーダーシップによるところが大きい。しかしながら、幹部職員への登用前に行われる研修等において情報管理に関する事項は必ずしも最重要事項とはみなされていない等、幹部職員の情報管理に関する認識を高める取組みは十分なものではない。

【改善策】

イ 幹部職員への登用の際の情報管理に関する研修を充実させるとともに、幹部職員を召集した会議等あらゆる機会を活用して、情報管理の重要性に関する認識を高めていくべきである。また、幹部職員は、個々の部下職員の情報管理やコンプライアンスに関する意識等を適確に把握して、そのレベルに応じて適確に指導育成を図るべきである。

そのためには、適切な情報管理及び部下職員の指導育成は組織としてのコンプライアンスの確保の上で極めて重要であるといった意識を幹部職員に徹底させなければならず、研修資料をはじめとする各種資料を専門家の意見も参考としつつ早急に作成することが必要である。また、情報管理に関する講演会等への幹部職員の積極的参加も有効である。

ロ また、情報管理について幹部職員のリーダーシップの下、組織をあげて推進するために各組織の長をトップとする情報管理に関する常設の会議をそれぞれの組織で設置することを検討するべきである。

(3) 組織における方針の徹底

【現状と問題点】

本件事案は、一職員が個人の思いから当該情報を非公開とする組織としての方針に反する形で情報を故意に流出させたものである。また、本事件を担当していない職員であって本件衝突映像を見た者も、そうした組織としての方針があるにもかかわらず、誰もが視聴できるパブリックフォルダで映像を見たことについて上司等への報告を行っていない。

このように、本件衝突映像を公開しないという方針を決定していたにもかかわらず

らず、その方針が組織全体に共有、徹底されていない等、重要な事案の対処に関する方針の組織的な共有が不十分であった。

【改善策】

- イ 社会的関心の高い重要な事案の発生時には、当該事案に直接関係する管区本部だけでなく、本庁幹部と各管区本部幹部の間で、当該事案に関する認識等を共有し、現場の各職員に対しても各管区本部幹部から必要な範囲で当該事案の重要性等について説明する等、組織として情報を共有する努力が必要である。
- ロ そのためには、様々な単位でのミーティングや各組織間の連絡会議等あらゆる機会を活用して、組織内で良好なコミュニケーションを保持するよう努めることが必要である。特に社会的関心の高い事案の発生時においては、職員一般の意識や世論等の動向も十分に踏まえた上で海上保安庁としての方針等に関し、積極的に情報の共有を行っていくべきである。

2. 規則やマニュアル等に係る改善策

【現状と問題点】

- (1) 一般に国の機関においては、文書管理規則によって秘密文書の指定等が、情報セキュリティポリシーによって機密性の格付けや取扱制限の実施等が定められている。また、捜査機関の一つである海上保安庁においては、これらの規則に加えて捜査関係規則において捜査書類や証拠物を施錠可能な書庫等で保管する等の厳格な取扱いが定められている。

捜査関係事務等について適切に業務を実施するためには秘密文書の指定や情報の格付けや取扱制限等について、どの段階で誰が判断し、どのように明示すべきか、情報システム上で実際にどのように扱うべきか等に関し具体的な手順が明確にされているべきであったが、こうした点が関連する各種規則において十分ではなかった。

この場合、捜査関係事務において作成される書面等は、刑事訴訟法上の「訴訟に関する書類」として公にしてはならないものであり、一般的な行政文書以上に厳格な取扱いがなされるべきである。その意味では、秘密文書としての指定の有無や機密性の如何にかかわらず、本来クローズ系のシステムで扱うべきものであるが、海上保安庁の現状としては、捜査関係事務において作成される書面についても情報管理に関する必要な措置を講じたうえで、オープン系のシステムで扱わざるを得ない。

- (2) 現行の海上保安庁情報セキュリティポリシー実施手順書は、すべての業務を網羅しているため大部であり、かつ、その表現が難解との指摘がある。また、文書管理規則や捜査関係規則は、電子的処理を前提とした規定となっていない。捜査関係事務以外にも様々な業務に従事する海上保安庁職員のためには、個々

の業務に即した秘密文書の指定、機密性の格付け及び取扱制限に関する基準、具体的なシステム上の取扱いに関し、規則やマニュアル等が理解しやすい形で整備されるべきであるが、現状は十分ではない。

【改善策】

- (1) 捜査関係資料については、本来、クローズ系のシステムで取り扱われるべきであるが、そうしたクローズ系システムの環境が確保されるまでの間においても、捜査関係業務に従事する職員が、現在のオープン系のシステム上、適確に情報を取り扱うことができるよう、捜査関係規則において文書管理規則や海上保安庁情報セキュリティポリシー実施手順書との整合を図りつつ、具体的な取扱い要領を明らかにした規定を整備すべきである。
- (2) 捜査以外の業務についても、業務毎に職員が適確に情報を取り扱うことができるよう、また、組織的に情報の取扱い状況をチェックすることができるよう、秘密文書の指定や機密性の格付け・取扱制限についてポジティブリスト化する等の文書管理規則や海上保安庁情報セキュリティポリシー実施手順書の規定の明確化を図るべきである。
- (3) さらに、各業務や各ポスト毎等、様々な現場の業務に即した理解しやすいマニュアルや指導資料を早急に作成するべきである。

3. 情報システムに係る改善策

【現状と問題点】

- (1) 情報管理の徹底のためには、すでに述べた職員のコンプライアンス等に関する意識を高め、規則やマニュアルを整備する等の必要な措置を取った上で、職員の故意や過失があっても直ちには情報の流出につながらないような、あるいは故意の流出を抑止するような情報システム上の対策も重要である。
- (2) 海上保安庁は、広範な管轄海域における様々な事案に組織全体として迅速適確に対処しなければならないという業務の特質から、部内外における「情報共有」の必要性が高い。また、電子申請の受付や府省共通システムの運用等による一般行政事務の遂行も必要不可欠である。このため、オープン系の行政情報システムを主要なシステムとして整備してきた。
- (3) ファイアウォール等の必要なセキュリティ対策は、現在のオープン系の行政情報システムにおいても講じているが、例えば私有USBメモリはシステム上使用できなくする、あるいは情報システムから持ち出す情報は自動暗号化する等、職員が規則の適用を誤ったり、規則が遵守されなかった場合でも、フェイルセーフ機能が働くような情報システム上の対策が十分ではない。
- (4) また、そもそも意図的な部外への情報送信等の情報流出を確実に防止し、コンピューターウィルスの感染、不審メール、サイバー攻撃等の外部からの脅威に対してより適確に対応する観点からは、オープン系システムはクローズ系シ

システムに比べ万全ではない。さらには職員が常にオープン系のシステム環境の中で業務に係る情報を取り扱ってきたことも、情報管理に注意すべき情報を扱っているという意識が希薄になってしまった一因である。

【改善策】

- (1) 海上保安庁内で情報を作成、伝送、共有する業務上の情報システムについては、インターネットを介した外部からの脅威に対して万全な対策をとるとともに、内部からの情報流出の危険性を排除することにより情報管理に万全を期する必要がある。この場合、オープン系システムでは、ファイアウォール等の必要なセキュリティ対策を講じたとしても、過失による情報流出の可能性を否定できず、海上保安庁内で業務に常用するシステムはクローズ系システムとすべきである。なお、他の捜査機関や治安機関においては、組織内で情報を作成、伝送、共有する業務上の情報システムにはクローズ系を使用しており、業務に常用するシステムをクローズ系とすることで、職員の情報管理に関する意識の向上にも資する効果が期待できる。したがって、クローズ系システムを業務に常用するシステムとする場合の規模、時期等、その整備に向けた具体的な方策について早急に検討するべきである。
- (2) クローズ系システムを業務に常用するシステムとする場合にあっても、オープン系システムは、内外の情勢等に関する幅広い情報収集、外部機関との連絡調整、電子申請の受理等、一定の業務には引き続き必要であり、その範囲内でセキュリティ対策を強化したうえで維持する必要がある。
- (3) また、クローズ系システムを整備していくとしても、以下のようなシステム上のセキュリティ対策を、クローズ系システムの整備を待つことなく、可能なものから実施すべきである。
 - ① データの持出しや流出があった場合にも被害を最小限にとどめるため情報システムを自動暗号化すること。
 - ② 問題発生時の迅速な原因究明等のため証跡管理を強化すること。
 - ③ 無許可USBメモリ等の使用制限のためシステム上の認証を導入すること。
 - ④ 機密性の高い情報を扱う課室、システム上重要な機器管理場所等の入退室の管理等監視体制を強化すること。
 - ⑤ 外部からの不正アクセスや異常なデータ流出の監視、ルール遵守のためのシステム上のサポート、その他のシステム上の対策について費用対効果や技術の動向を勘案しつつ、強化すること。
- (4) なお、システムの構築に当たっては、適確な情報の共有による効率的な業務の遂行が可能となるよう十分な配慮が必要であるが、ネットワーク回線の容量等についてもコンピュータ処理能力等の進展に応じて十分に確保することが必要である。

4. 情報管理に関する組織に係る改善策

【現状と問題点】

情報管理に万全を期していくためには、適時適切な対策を企画立案し、推進していくしっかりとした組織が必要である。

本庁においては、総務部情報通信課が中心となって情報セキュリティ対策を実施しており、管区においては情報通信管理センターが情報セキュリティ対策を実施している。しかしながら、情報通信管理センターは、管区本部の下部組織である事務所のひとつであり、管区本部には情報管理に関し管区本部長のリーダーシップの下、積極的に対策を推進していく組織がない。また、各部署等においても、情報管理を実践、推進する要員が配置されていない等の問題がある。

【改善策】

- イ 管区における情報通信管理センターの位置付けを見直し、管区本部長の指揮の下に、管区全体の情報セキュリティ対策を推進する体制を整備することを検討するべきである。これによって、組織の長をトップとする情報管理の推進のための会議の設置と相まって、幹部職員のリーダーシップの下、本庁から管区本部、部署、現場船艇に至るまで、情報管理のための諸施策を総合的、かつ、一体的に推進するための体制が整備されることとなる。
- ロ 部署を含む各組織に、日常的な情報管理の実践、指導の中核となる要員を配置するとともに、情報システム上のセキュリティ対策の強化に応じ、必要なシステム担当要員を確保することを検討するべきである。
- ハ 情報システムや情報セキュリティに係る専門的知識経験を有する人材を継続的に確保、育成するべきである。
- ニ 情報セキュリティ対策上の職員の疑問に24時間対応し、適切な対策について助言できる体制を整備するべきである。

Ⅲ 中間報告書提言事項に対する海上保安庁の取組状況と評価

1. 職員の意識に係る改善策

- (1) 海上保安大学校及び海上保安学校における初任教育並びに現場赴任後の初任者研修及び階層別研修等、あらゆる機会を捉えて、国家公務員としてのコンプライアンスや情報管理に関する意識強化のための教育研修や注意喚起が行われており、また、情報管理に関する総合的な研修資料の作成のほか、研修後の小テストの導入などにより、職員の意識や理解が促進されている。
- (2) 平成23年度の情報セキュリティ監査については、上記のとおり職員の意識や理解の促進が図られたことにより、結果は概ね良好であったと思料する。
- (3) 幹部職員に対する情報管理の責任者としての研修を実施したほか、本庁、管区本部、部署に至るまで、組織のトップを議長とする情報管理推進会議を設置

したことにより、幹部職員の情報管理に対する認識の高揚が図られている。

- (4) 重要事案等発生時には、本庁から各管区等幹部に対し一元的な情報提供を行うとともに、各種会議やテレビ会議の活用を通じて良好なコミュニケーションを保持し、組織内における方針の徹底が図られている。
- (5) 今後は、各職員の情報管理に関する意識の風化が懸念されることや、情報セキュリティに対する脅威や対策の変化に伴い、各職員に付与すべき知識等も変化することから、引き続き、最新の状況を踏まえた研修等を実施していく必要がある。

2. 規則やマニュアル等に係る改善策

- (1) 捜査関係業務に従事する職員が、適確に捜査情報を取り扱うことができるよう、内部規則を制定するとともに、人事関係情報の取扱いに関するガイドライン等、個別の業務に関するマニュアルが必要に応じて作成されており、情報の取り扱いの具体的手順が明確化されている。
- (2) 今後は、それら新たなルールの日々の業務遂行への浸透をはかりつつ、併せて、その業務への適合性、効果等を適宜検証し、必要に応じて、所要の見直しを講じる必要がある。

3. 情報システムに係る改善策

- (1) 海上保安庁内で業務で常用する情報システムをクローズ系システムとするため、一部で既に運用されているクローズ系システムの脆弱性やその改善に必要な機器構成等の調査を開始するとともに、行政情報システム等に対し内部情報を暗号化するソフトを順次導入し、データの持ち出しや流出があった場合の被害を最小限に止める措置を講ずるなど、情報システムにおけるセキュリティ対策の強化が進められている。
- (2) 捜査情報は、関係者のプライバシーの保護や適切な法執行等の観点から厳格な取扱いがなされるべきであるところ、捜査機関等においては、クローズ系システムを整備して運用することは今や常識となっている。海上保安庁においても、情報流出の再発防止の観点のみならず、取り扱う業務や情報の性質上、クローズ系システムによる業務の運営が不可欠である。このため、現在進めているクローズ化のための調査に基づき、クローズ系システムを整備を早急に進める必要がある。また、問題発生時の迅速な原因究明等のため証跡管理を強化することや無許可USBメモリ等の使用制限のためシステム上の認証等を実施していく必要がある。

4. 情報管理に関する組織に係る改善策

- (1) 管区本部の事務所であった情報通信管理センターを管区本部の内部組織に改編するとともに、管区全体の情報セキュリティ対策を推進し、情報の管理に関する重要事項について企画及び立案を行う「情報管理官」を設置して、管区全体の情報管理対策を総合的、一体的に推進する体制が整備されている。
- (2) 本庁及び管区本部に情報保全対策係の増員が図られるとともに、情報セキュリティに関する問合せ窓口を設置、運用することにより、情報セキュリティ上の職員の疑問に対応する体制が整備されている。
- (3) 今後も、引き続き部署を含む各組織に、日常的な情報管理の実践、指導の中核となる要員を確保していくことを検討するとともに、様々な業務を行う海上保安官の中から情報システムやセキュリティに係る専門的人材を確保・育成し、他の業務との両立も含め、有効に活用していく方策について検討していく必要がある。

おわりに

「政府における情報保全に関する検討委員会」の現段階までの検討結果の内容については、すでに当委員会の中間報告書の提言の中で網羅されており、新たに追加的記載を必要とする事項は認められないことから、今般、当委員会としての最終的な取りまとめを行うものであるが、今後も技術の進展、海上保安庁を取り巻く状況の変化等に応じ、情報管理に関する対策は引き続き見直していかなければならない。また、海上保安庁が今後取組むべき対策には、定員及び予算上の措置や技術的な検討が必要なものも多いが、対策の推進に積極的に取り組むことを強く期待するものである。

情報流出再発防止対策検討委員会開催経緯

○ 第1回

日時：平成23年1月19日（水）1400～1600

場所：国土交通省（3号館）4階特別会議室

- ・国土交通大臣挨拶
- ・事務局から、「海上保安庁における文書、情報管理ルール の現状」、「海上保安庁の情報システムの現状」、「海上保安庁における情報セキュリティ対策の経緯」、「中国漁船衝突事件映像流出事案の概要及び問題点」、「緊急対策として講じた措置」、「海上保安庁の業務及び取り扱う情報の特質」等について順次説明を行ったのち、討議を行った。

○ 第2回

日時：平成23年2月7日（月）1000～1150

場所：国土交通省（3号館）11階海上保安庁会議室

- ・事務局から、「海上保安庁における情報システムの現状」、「海上保安庁における教育研修の現状」、「海上保安庁における捜査書類等の管理の現状」及び「情報管理体制の見直しに係る緊急対策の進捗状況」について順次説明を行ったのち、海上保安庁の情報管理のために考えられる改善策等について討議を行った。

○ 第3回

日時：平成23年3月3日（木）1000～1200

場所：国土交通省（3号館）11階海上保安庁会議室

- ・海上保安庁の情報管理に関する具体的な改善策の方向性について、過去2回の委員会での討議を踏まえつつ自由討議を行い、
 - 職員等の意識・理解の問題と改善策
 - 規則・マニュアル等の問題と改善策
 - 情報システム上の問題と改善策
 - 組織管理上の問題と改善策などの観点から、各委員の専門的知見に基づく意見・提言がなされた。
- ・情報管理の見直しに係る緊急対策の実施状況及び政府における情報保全に関する検討状況等について事務局から報告された。

○ 第4回

日時：平成23年5月16日（月）1630～1800

場所：国土交通省（3号館）11階海上保安庁会議室

- ・ 中間とりまとめとして「情報流出再発防止対策検討委員会中間報告書(案)」を審議・作成した。

○ 第5回

日時：平成24年5月8日(火) 1330～1500

場所：国土交通省(3号館)11階海上保安庁会議室

- ・ 最終的なとりまとめとして「情報流出再発防止対策検討委員会報告書(案)」を審議・作成した。

情報流出再発防止対策検討委員会委員名簿
(五十音順、敬称略)

赤松 幸夫 弁護士

有田 知徳 弁護士

五味 祐子 弁護士

田中 利幸 法政大学法学部 教授

林 紘一郎 情報セキュリティ大学院大学 教授 (座長)

舟橋 信 (財) 未来工学研究所 研究参与