行政文書開示請求書

2011年7月15日

内閣情報官
~~内閣官房副長官補~~ 殿

氏名又は名称：（法人その他の団体にあっては，その名称及び代表者の氏名）
[redacted]

住所又は居所：（法人その他の団体にあっては，主たる事務所等の所在地）
[redacted]
TEL [redacted]

連　絡　先：（連絡先が上記の本人以外の場合は，連絡担当者の住所・氏名・電話番号）

行政機関の保有する情報の公開に関する法律第４条第１項の規定に基づき，下記のとおり行政文書の開示を請求します。

記

1　請求する行政文書の名称等

（請求する行政文書が特定できるよう行政文書の名称，請求する文書の内容等をできるだけ具体的に記載してください。）
① 平成23年7月開催の「政府における情報保全に関する検討委員会」で配布された資料で、ホームページに掲載されていないもの
② 秘密保全のための法制の在り方に関する有識者会議、情報保全システムに関する有識者会議の配布資料で、ホームページに掲載されていないもの

2　求める開示の実施の方法等（本欄の記載は任意です。）

アまたはイに○印を付してください。アを選択された場合は，その具体的な方法等を記載してください。

ア　事務所における開示の実施を希望する。
＜実施の方法＞　①　閲覧　②　写しの交付　③　その他（　　）
＜実施の希望日＞
イ　写しの送付を希望する。

開示請求手数料（１件３００円）	収入印紙 300円 収入印紙をはってください。	受付 23.7.19 内閣官房 内閣総務官室

＊この欄は記入しないでください。

担当課等	
備　考	H23.7.20　請求人に電話連絡し、あて先を補正する旨を了承記

閣情第３１７号
平成２３年８月１８日

行政文書開示等決定通知書

[redacted]様

内閣情報官

植松　信一

平成２３年７月１５日付け行政文書の開示請求（平成２３年７月１９日付け受付）について、行政機関の保有する情報の公開に関する法律（以下「法」という。）第９条第１項の規定に基づき、下記のとおり開示することとしましたので通知します。

記

１　開示する行政文書の名称

（１）第１回秘密保全のための法制の在り方に関する有識者会議（平成２３年１月１５日）配付資料
（２）第２回秘密保全のための法制の在り方に関する有識者会議（平成２３年２月１８日）配付資料
（３）第３回秘密保全のための法制の在り方に関する有識者会議（平成２３年４月８日）配付資料
（４）第４回秘密保全のための法制の在り方に関する有識者会議（平成２３年４月２２日）配付資料
（５）第５回秘密保全のための法制の在り方に関する有識者会議（平成２３年５月１３日）配付資料
（６）第６回秘密保全のための法制の在り方に関する有識者会議（平成２３年６月１０日）秘密保全のための法制の在り方について（報告書案）
（７）第１回情報保全システムに関する有識者会議（平成２２年１２月１７日）配付資料
（８）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料
（９）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料「中国漁船衝突事件映像情報流出事案の概要について」
（１０）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料「警察における情報保全に関する取組みについて」
（１１）第３回情報保全システムに関する有識者会議（平成２３年３月９日）配付資料

（１２）第３回情報保全システムに関する有識者会議（平成２３年３月９日）配付資料５「将来予想される脅威等に関する各委員の御説明資料」
（１３）第４回情報保全システムに関する有識者会議（平成２３年５月２０日）配付資料「報告書（案）」
（１４）第４回情報保全システムに関する有識者会議（平成２３年５月２０日）配付資料「情報流出再発防止対策検討委員会中間報告書（概要）」
（１５）第２回情報保全に関する検討委員会（平成２３年５月２０日）配付資料「情報保全システムに関する有識者会議報告書（案）」

２　不開示とした部分とその理由

上記（３）中、
我が国や他国におけるセキュリティクリアランス制度の具体的な内容が記載されている部分は、これを公にすることにより、情報提供を受けた当該国との信頼関係が損なわれるおそれがあること、他国機関等から対抗・妨害措置を講じられ、我が国の安全が害されるおそれがあること、当室を含む政府における情報保全事務の適正な遂行に支障を及ぼすおそれがあることから法第５条第３号及び第６号に該当するため不開示とした。

上記（８）、（１１）、（１３）及び（１５）中、
我が国行政機関の情報保全システムに関する具体的な内容が記載されている部分は、これを公にすることにより、他国機関等から対抗・妨害措置を講じられ、我が国の安全が害されるおそれがあること、不当な目的を持った者の働きかけにより秘密の漏えいを引き起こすなど、犯罪の予防その他公共の安全と秩序の維持に支障を及ぼすおそれがあること、当室を含む政府における情報保全事務の適正な遂行に支障を及ぼすおそれがあることから法第５条第３号、第４号及び第６号に該当するため不開示とした。

上記（１２）中、
有識者の説明資料については、
○　公表前の研究内容等の研究成果が含まれており、これは公にすることにより、個人の権利利益を侵害するおそれがあることから法第５条第１号に該当する
○　外部に内容を公開しない前提で任意に提供されたものが含まれており、これは公にすることにより、有識者が属する法人の正当な利益を害するおそれがあり、法第５条第２号に該当する
○　また、これらは公にすることにより、
・　他国機関等から対抗・妨害措置を講じられ、我が国の安全が害されるおそれがあることから法第５条第３号に該当する
・　不当な目的を持った者等の働きかけにより秘密の漏えいを引き起こすなど、犯罪の予防その他公共の安全と秩序の維持に支障を及ぼすおそれがあることから法第５条第４号に該当する
・　他国機関等からの対抗・妨害措置あるいは不当な目的を持った者等の働きかけによる秘密の漏えい等により、当室を含む政府における情報保全事務の適正な遂行に支障を及ぼすおそれがあることから法第５条第６号に該当する
・　今後同様の検討を行う場合に有識者の間で情報等の提供を躊躇することが懸念

されるなど、当室の行う事務の適切な遂行に支障を及ぼすおそれがあり、ひいては我が国の安全が害されるおそれがあることから法第５条第３号及び第６号に該当する
ため不開示とした。

＊　この決定に不服がある場合は、行政不服審査法（昭和３７年法律第１６０号）第５条の規定により、この決定があったことを知った日の翌日から起算して６０日以内に、内閣総理大臣に対して審査請求をすることができます（なお、決定があったことを知った日の翌日から起算して６０日以内であっても、決定の日の翌日から起算して１年を経過した場合には審査請求をすることができなくなります。）。
また、この決定の取消しを求める訴訟を提起する場合は、行政事件訴訟法（昭和３７年法律第１３９号）の規定により、この決定があったことを知った日から６か月以内に、国を被告として（訴訟において国を代表する者は法務大臣となります。）、東京地方裁判所に処分の取消しの訴えを提起することができます（なお、決定があったことを知った日から６か月以内であっても、決定の日から１年を経過した場合には処分の取消しの訴えを提起することができなくなります。）。

３　開示の実施の方法等

（１）開示の実施の方法等　　＊同封の説明事項をお読みください。

下表に記載した方法の中から、希望する方法で開示の実施を受けられます。

行政文書の種類・数量等	開示の実施の方法	開示実施手数料の額（算定基準）	行政文書全体について開示の実施を受けた場合の基本額	実際にお支払いいただく開示実施手数料（※）
Ａ４判文書 ２９８枚 （内訳） 白黒　190枚 カラー　108枚	①閲覧	１００枚までにつき １００円	３００円	０円
	②複写機により白黒で複写したものの交付	用紙１枚につき １０円	２９８０円	２６８０円
	③複写機によりカラーで複写したものの交付	カラー１枚につき ２０円	４０６０円	３７６０円
	③スキャナにより電子化しCD-Rに複写したものの交付（ＰＤＦファイル）	CD-R１枚につき１００円に、文書１枚ごとに１０円を加えた額	３０８０円	２７８０円

※　実際にお支払いいただく開示実施手数料は、選択された開示の実施の方法に応じて、定められた算定方法に従って基本額（複数の実施の方法を選択した場合はそれぞれの合算額）を計算し、その額が３００円までは無料、３００円を超える場合は当該額から３００円を差し引いた額となります。

（注）　ＣＤ－Ｒによる開示の実施を希望される場合は、所要枚数が異なることにより開示実施手数料が変動することがありますので、開示の実施方法の申出をする前に、あらかじめ、担当課まで御連

絡ください。

（2）事務所における開示を実施することができる日時、場所

事務所における開示の実施を希望する場合には、下記に記した日時の中から、希望する日時を選択してください。

日：平成２３年８月２４日から平成２３年１０月３１日まで（行政機関の休日を除く。）

時：１０：００から１７：００まで（１２：００～１３：００を除く。）

場所：内閣府庁舎１階情報公開窓口　東京都千代田区永田町１－６－１

（3）写しの送付を希望する場合の準備日数、郵送料（見込み額）

日数：「開示の実施の方法等に係る申出書」が提出された日から１週間後までに発送予定

郵送料：５００円（ゆうパック）

＊　担当課等

内閣官房内閣情報調査室（情報公開担当）

〒100-8968

東京都千代田区永田町１－６－１

電話：０３－５２５３－２１１１（内線８３４０６）

保存期間	30年・10年・5年・3年・1年

（文書処理上の記事）

文書番号	閣情　第３１７号
受付	平成２３年　７月１９日
起案	平成２３年　８月１１日
決裁・~~供覧~~	平成 23 年 8 月 18 日
施行	平成 23 年 8 月 18 日
専決番号	別表　――

内閣情報官

次長

内閣審議官

内閣参事官（総務部主幹）

内閣参事官

調査官

内閣事務官

[redacted]

起案者

氏名 [redacted]

（件　名）　行政文書開示等決定通知書の発出について

（伺い）

標記の件、平成23年7月19日受付けの情報公開請求について、別紙案のとおり、行政文書開示等決定通知書を発出してよろしいか伺います。※請求書別添

内　閣

決　裁　要　旨

所属	本室・総務・[redacted]	氏名	[redacted]	内線	[redacted]
内容	情報公開請求	期限	平成23年8月18日		

◎[redacted]からの情報公開請求について

○「情報保全に関する検討委員会」、「秘密保全のための法制の在り方に関する有識者会議」、「情報保全システムに関する有識者会議」の配付資料に関し、官邸HPに掲載していないものについて、7月19日受付で情報公開請求がありました。※請求書別添

○対象文書の中には、不開示とすべき箇所があります。

・フランスにおけるセキュリティクリアランス制度のうち、公開情報と判断できないもの

・有識者からの提供資料につき、個人の権利利益を害するおそれ（５条１号）、法人の事業に関する情報（５条２号）に該当する箇所

・我が国政府における情報保全システムの現状や対応策に関する文書のうち、国の安全が害されるおそれ（５条３号）、犯罪予防とその他公共の安全と秩序の維持に支障を及ぼすおそれ（５条４号）、事務の適正な遂行に支障を及ぼすおそれ（５条６号）に該当する箇所

○ついては、別紙案のとおり、行政文書開示等通知書を提出してよろしいか伺います。

行政文書開示請求書

2011年7月15日

内閣情報官
~~内閣官房副長官補~~ 殿

氏名又は名称：（法人その他の団体にあっては，その名称及び代表者の氏名）
[redacted]

住所又は居所：（法人その他の団体にあっては，主たる事務所等の所在地）
[redacted]
TEL [redacted]

連　絡　先：　（連絡先が上記の本人以外の場合は，連絡担当者の住所・氏名・電話番号）

行政機関の保有する情報の公開に関する法律第４条第１項の規定に基づき，下記のとおり行政文書の開示を請求します。

記

1　請求する行政文書の名称等

（請求する行政文書が特定できるよう行政文書の名称，請求する文書の内容等をできるだけ具体的に記載してください。）
① 平成23年7月開催の「政府における情報保全に関する検討委員会」で配布された資料で、ホームページに掲載されていないもの
② 秘密保全のための法制の在り方に関する有識者会議、情報保全システムに関する有識者会議の配布資料で、ホームページに掲載されていないもの

2　求める開示の実施の方法等　（本欄の記載は任意です。）

ア又はイに○印を付してください。アを選択された場合は，その具体的な方法等を記載してください。

ア　事務所における開示の実施を希望する。
<実施の方法>　① 閲覧　② 写しの交付　③ その他（　　）
<実施の希望日>
イ　写しの送付を希望する。

開示請求手数料（1件300円）	収入印紙 300円 収入印紙をはってください。	受付 (受付印) 23.7.19 内閣官房 内閣総務官室

＊この欄は記入しないでください。

担当課等	
備　考	H23.7.20　請求人に電話連絡し、あて先を補正する旨を確認

閣情第３１７号
平成２３年８月１８日

行政文書開示等決定通知書

[redacted] 様

内閣情報官

植松　信一

平成２３年７月１５日付け行政文書の開示請求（平成２３年７月１９日付け受付）について、行政機関の保有する情報の公開に関する法律（以下「法」という。）第９条第１項の規定に基づき、下記のとおり開示することとしましたので通知します。

記

１　開示する行政文書の名称

（１）第１回秘密保全のための法制の在り方に関する有識者会議（平成２３年１月１５日）配付資料
（２）第２回秘密保全のための法制の在り方に関する有識者会議（平成２３年２月１８日）配付資料
（３）第３回秘密保全のための法制の在り方に関する有識者会議（平成２３年４月８日）配付資料
（４）第４回秘密保全のための法制の在り方に関する有識者会議（平成２３年４月２２日）配付資料
（５）第５回秘密保全のための法制の在り方に関する有識者会議（平成２３年５月１３日）配付資料
（６）第６回秘密保全のための法制の在り方に関する有識者会議（平成２３年６月１０日）秘密保全のための法制の在り方について（報告書案）
（７）第１回情報保全システムに関する有識者会議（平成２２年１２月１７日）配付資料
（８）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料
（９）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料「中国漁船衝突事件映像情報流出事案の概要について」
（１０）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料「警察における情報保全に関する取組みについて」
（１１）第３回情報保全システムに関する有識者会議（平成２３年３月９日）配付資料

（１２）第３回情報保全システムに関する有識者会議（平成２３年３月９日）配付資料５「将来予想される脅威等に関する各委員の御説明資料」
（１３）第４回情報保全システムに関する有識者会議（平成２３年５月２０日）配付資料「報告書（案）」
（１４）第４回情報保全システムに関する有識者会議（平成２３年５月２０日）配付資料「情報流出再発防止対策検討委員会中間報告書（概要）」
（１５）第２回情報保全に関する検討委員会（平成２３年５月２０日）配付資料「情報保全システムに関する有識者会議報告書（案）」

２　不開示とした部分とその理由

上記（３）中、
我が国や他国におけるセキュリティクリアランス制度の具体的な内容が記載されている部分は、これを公にすることにより、情報提供を受けた当該国との信頼関係が損なわれるおそれがあること、他国機関等から対抗・妨害措置を講じられ、我が国の安全が害されるおそれがあること、当室を含む政府における情報保全事務の適正な遂行に支障を及ぼすおそれがあることから法第５条第３号及び第６号に該当するため不開示とした。
上記（8）、（１１）、（１３）及び（１５）中、
我が国行政機関の情報保全システムに関する具体的な内容が記載されている部分は、これを公にすることにより、他国機関等から対抗・妨害措置を講じられ、我が国の安全が害されるおそれがあること、不当な目的を持った者の働きかけにより秘密の漏えいを引き起こすなど、犯罪の予防その他公共の安全と秩序の維持に支障を及ぼすおそれがあること、当室を含む政府における情報保全事務の適正な遂行に支障を及ぼすおそれがあることから法第５条第３号、第４号及び第６号に該当するため不開示とした。
上記（１２）中、
有識者の説明資料については、
○　公表前の研究内容等の研究成果が含まれており、これは公にすることにより、個人の権利利益を侵害するおそれがあることから法第５条第１号に該当する
○　外部に内容を公開しない前提で任意に提供されたものが含まれており、これは公にすることにより、有識者が属する法人の正当な利益を害するおそれがあり、法第５条第２号に該当する
○　また、これらは公にすることにより、
・　他国機関等から対抗・妨害措置を講じられ、我が国の安全が害されるおそれがあることから法第５条第３号に該当する
・　不当な目的を持った者等の働きかけにより秘密の漏えいを引き起こすなど、犯罪の予防その他公共の安全と秩序の維持に支障を及ぼすおそれがあることから法第５条第４号に該当する
・　他国機関等からの対抗・妨害措置あるいは不当な目的を持った者等の働きかけによる秘密の漏えい等により、当室を含む政府における情報保全事務の適正な遂行に支障を及ぼすおそれがあることから法第５条第６号に該当する
・　今後同様の検討を行う場合に有識者の間で情報等の提供を躊躇することが懸念

されるなど、当室の行う事務の適切な遂行に支障を及ぼすおそれがあり、ひいては我が国の安全が害されるおそれがあることから法第５条第３号及び第６号に該当する
ため不開示とした。

＊　この決定に不服がある場合は、行政不服審査法（昭和３７年法律第１６０号）第５条の規定により、この決定があったことを知った日の翌日から起算して６０日以内に、内閣総理大臣に対して審査請求をすることができます（なお、決定があったことを知った日の翌日から起算して６０日以内であっても、決定の日の翌日から起算して１年を経過した場合には審査請求をすることができなくなります。）。
また、この決定の取消しを求める訴訟を提起する場合は、行政事件訴訟法（昭和３７年法律第１３９号）の規定により、この決定があったことを知った日から６か月以内に、国を被告として（訴訟において国を代表する者は法務大臣となります。）、東京地方裁判所に処分の取消しの訴えを提起することができます（なお、決定があったことを知った日から６か月以内であっても、決定の日から１年を経過した場合には処分の取消しの訴えを提起することができなくなります。）。

３　開示の実施の方法等

（１）開示の実施の方法等　　＊同封の説明事項をお読みください。

下表に記載した方法の中から、希望する方法で開示の実施を受けられます。

行政文書の種類・数量等	開示の実施の方法	開示実施手数料の額（算定基準）	行政文書全体について開示の実施を受けた場合の基本額	実際にお支払いいただく開示実施手数料（※）
Ａ４判文書 ２９８枚 （内訳） 白黒　190枚 カラー　108枚	①閲覧	１００枚までにつき １００円	３００円	０円
	②複写機により白黒で複写したものの交付	用紙１枚につき １０円	２９８０円	２６８０円
	③複写機によりカラーで複写したものの交付	カラー１枚につき ２０円	４０６０円	３７６０円
	③スキャナにより電子化しCD-Rに複写したものの交付（ＰＤＦファイル）	CD-R１枚につき１００円に、文書１枚ごとに１０円を加えた額	３０８０円	２７８０円

※　実際にお支払いいただく開示実施手数料は、選択された開示の実施の方法に応じて、定められた算定方法に従って基本額（複数の実施の方法を選択した場合はそれぞれの合算額）を計算し、その額が３００円までは無料、３００円を超える場合は当該額から３００円を差し引いた額となります。

（注）　ＣＤ－Ｒによる開示の実施を希望される場合は、所要枚数が異なることにより開示実施手数料が変動することがありますので、開示の実施方法の申出をする前に、あらかじめ、担当課まで御連

絡ください。

（2）事務所における開示を実施することができる日時、場所

事務所における開示の実施を希望する場合には、下記に記した日時の中から、希望する日時を選択してください。

日：平成２３年８月２４日から平成２３年１０月３１日まで（行政機関の休日を除く。）

時：１０：００から１７：００まで（１２：００～１３：００を除く。）

場所：内閣府庁舎１階情報公開窓口　東京都千代田区永田町１－６－１

（3）写しの送付を希望する場合の準備日数、郵送料（見込み額）

日数：「開示の実施の方法等に係る申出書」が提出された日から１週間後までに発送予定

郵送料：５００円（ゆうパック）

＊　担当課等

内閣官房内閣情報調査室（情報公開担当）

〒100-8968

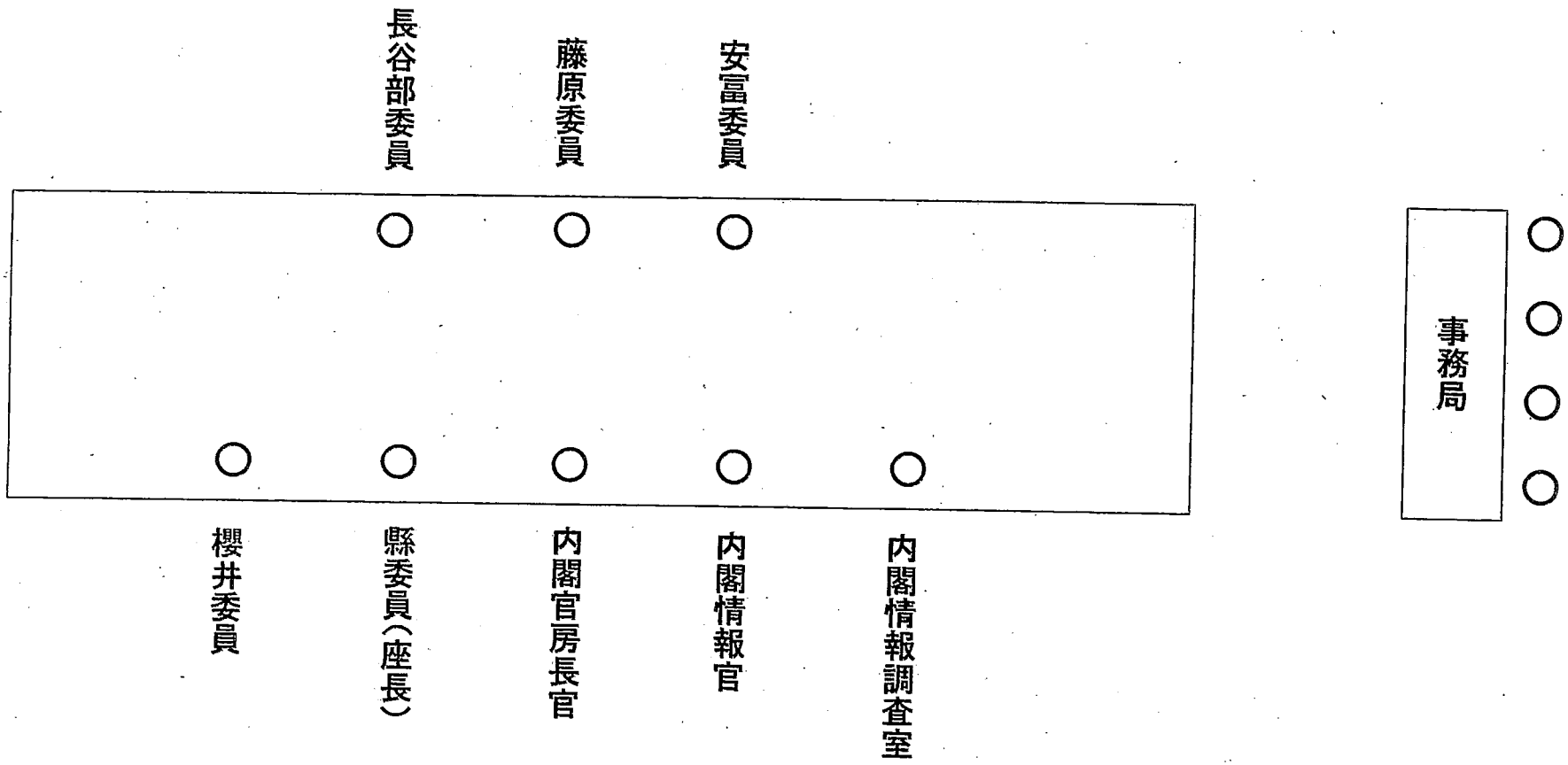
東京都千代田区永田町１－６－１

電話：０３－５２５３－２１１１（内線８３４０６）

第1回秘密保全のための法制の在り方に関する有識者会議　座席表

平成23年1月5日（水）午前9時30分～午前11時　於：官邸4階大会議室

（出入口）



配付資料

資料１　政府における情報保全に関する検討委員会の開催について

資料２　秘密保全のための法制の在り方に関する有識者会議の開催について

資料３　秘密保全のための法制の在り方に関する有識者会議の運営について（案）

資料４　秘密保全法制の検討スケジュール（案）

資料５　秘密保全法制の意義

資料６　主要な漏えい事件等の概要

資料７　我が国の秘密保全に関する現行法制

対外非公表　取扱注意

機密性２情報

配付資料３

（案）

秘密保全のための法制の在り方に関する有識者会議の運営について

平成２３年１月５日
秘密保全のための法制の在り方に関する有識者会議決定

秘密保全のための法制の在り方に関する有識者会議（以下「会議」という。）の運営については、以下のとおりとする。

1　議事の非公開について

会議は、非公開とする。

2　議事要旨の公開について

会議の議事要旨は、原則として、会議終了後、発言者名を付さない形で、速やかに公開する。

3　配付資料の公開について

会議における配付資料の公開については、内容に応じて可否を判断する。

4　記者ブリーフについて

会議の内容については、会議終了後、事務局が記者ブリーフを実施する。

（了）

第1回　秘密保全のための法制の在り方に関する有識者会議

情報漏えい事案発生の原因及び具体的対応

防　衛　省

３等海佐による秘密漏えい事案

①　事案の概要

○　防衛庁防衛研究所所属のＨ３等海佐（「Ｈ３佐」）は、平成１１年１月、都内で開催された安全保障国際シンポジウムの会場で在日ロシア大使館駐在武官のＢ海軍大佐（「Ｂ大佐」）と知り合った。

同年９月、Ｈ３佐が通訳を務めたロシア海軍駆逐艦の横須賀寄港関連行事でＢ大佐と再会して話をするなどしたところ、後日、Ｂ大佐から食事に招待され、２人で食事を共にした。

○　以後、Ｈ３佐は、自己の研究に役立てるため、旧ソ連海軍関係の資料をＢ大佐から入手することを期待して同人との接触を十数回にわたって続け、その過程で、難病を患っていたＨ３佐の長男に対する見舞金等の名称でＢ大佐から現金等を受け取った。

○　こうして接触を続けていく中で、Ｂ大佐から海上自衛隊に関する資料を求められたが、旧ソ連海軍関係資料を入手したいという一心と、同大佐から種々の名目で現金の提供を受けたことへの負い目から、Ｈ３佐が過去に不正に複写し保有していた秘密文書の写しを、平成１２年６月、Ｂ大佐に渡したもの。

○　平成１２年９月、警視庁と神奈川県警の合同捜査本部は、Ｈ３佐を自衛隊法第５９条（秘密を守る義務）違反容疑で逮捕した。平成１３年３月７日、東京地裁において懲役１０ヶ月(求刑：懲役１年)の判決。

○　なお、Ｈ３佐は秘密保全義務違反として懲戒免職処分とされるとともに、関係者５２名を処分。

②　主な原因

○　秘密文書の取扱いの不徹底

秘密文書を不正に複写する等の不適切な行為が行われるなど、秘密文書の取扱い要領が不徹底

○　外部からの働き掛けに対する対応の不十分

防衛交流の活発化により、ちょう報工作の対象となる機会や職員の範囲も増大しているにもかかわらず、対応が不十分。また、我が国において過去にちょう報事件の摘発実績のある国等に対する職員の警戒心が低下

○　施設等機関等における保全機能の未整備

Ｈ３佐が勤務していた防衛研究所を始めとする陸・海・空自衛隊の部隊及び機関以外の組織（施設等機関等）について、各自衛隊が有している調査隊のような組織の健全性を保全する機能が未整備

○　職員の身上把握の不十分

個人的弱点を抱える職員はちょう報工作の対象として狙われやすいところ、上司による職員の身上把握が不十分

③　講じた処置

○　**秘密漏えい防止のための管理態勢等の整備**

関係職員の限定、秘密文書の的確な管理の徹底等

※平成１８年４月、私有パソコン等での業務用データ取扱い禁止、ファイル暗号化ソフトの導入等

○　**秘密保全に係る罰則の強化**

「防衛秘密」制度の新設（自衛隊法の改正）

○　**外部からの働き掛けへの対応要領の制度化**

各国駐在武官等との接触要領の策定（各国駐在武官と接触する際の事前了解等）

※平成１８年１２月、部外者（各国駐在武官等を除く。）からの不自然な働き掛けへの対応要領の策定

○　**情報保全に関連する部隊の充実・強化**

各自衛隊の情報保全隊を新設（中央と地方の部隊の指揮系統を一元化し、施設等機関等の保全業務の支援を任務化）

※平成２１年８月、陸海空情報保全隊を統合し、自衛隊情報保全隊を新編

○　**秘密を取り扱う職員の教育・身上把握の充実**

保全教育の拡充及び部隊等の長による十分な身上把握・カウンセリング等の充実（ちょう報工作の態様に関する保全教育の実施、ちょう報工作の対象として狙われやすい個人的弱点を抱える隊員の把握等）

※平成１８年４月、秘密保全に係る重い責任を自覚させるための「誓約書」の提出

※平成１９年５月、個別面談方式による全隊員に対する指導を実施（以後、年１回以上実施）

○　**全庁的な情報保全体制の整備**

委員会を設置し、情報保全に係る施策のフォローアップを実施（事務次官を長とする防衛庁情報保全委員会を設置）

※平成１９年４月、情報流出事案の再発防止を期すため、防衛大臣を長とする情報流出対策会議を設置

内閣情報調査室職員に対するロシア大使館職員による情報収集活動事案

事案の概要

○ 内閣情報調査室職員Aは、業務を通じ、在日ロシア大使館員と知り合った。

○ Aは、その後、歴代の同大使館員と接触を続ける中で、次第に金品の提供を受けるようになった。

○ やがて、Aは、部内情報を自ら取りまとめて提供するに至った。

○ 平成20年1月、Aは、収賄と国家公務員法違反（守秘義務違反）の疑いで書類送検された（不起訴処分（起訴猶予）、情報漏えい発覚直後に懲戒免職）。

主な反省教訓事項

○ 同種事案は、誰にでも起こり得るもの。

○ 服務指導や研修により、摘発への現実感を醸成して抑止力とすることも必要。

○ 職員に対するきめ細やかな教育や研修が不十分。

○ 情報保全一般に対する組織的な取組が不十分。

内閣情報調査室職員に対するロシア大使館職員による情報収集活動事案

主な具体的対応

○　情報保全に関する教育・研修の充実強化

－内容の質的向上、定期的受講の義務付け等

○　情報保全に関する組織・管理体制の強化

・　人的管理

－秘密取扱者適格性確認制度（セキュリティクリアランス制度）の的確な実施

・　物的管理

－特別管理秘密制度の的確な実施、電磁的記録媒体の管理強化

持ち込み規制物品の見直し

平成23年1月5日
海 上 保 安 庁

中国漁船衝突事件映像情報流出事案の概要について

1. 事案の概要

第五管区海上保安本部神戸海上保安部巡視艇乗組員（当時）が、平成22年11月4日、神戸市内において、動画サイト「YouTube」に中国漁船衝突事件映像情報（以下「衝突事件映像」という。）をアップロードし、故意にインターネット上に流出させたもの。

この衝突事件映像を流出させた職員が、衝突事件映像を入手した経路は以下のとおりであった。

（1） 平成22年9月17日、事件捜査のため、第十一管区海上保安本部職員は、行政情報システムの海上保安大学校のパブリックフォルダを用いて、衝突事件映像を海上保安大学校に伝送しようとしたが、この際、当該第十一管区海上保安本部職員と海上保安大学校職員の間で、衝突事件映像の削除についてきちんと確認しなかったため、同年9月17日から9月22日までの間、衝突事件映像が海上保安大学校のパブリックフォルダに掲載されたままとなり、不特定多数の海上保安庁職員が入手可能な状態となっていた。

（2） 同年9月19日、衝突事件映像を流出させた職員の同僚職員が、たまたま別の用件で、海上保安大学校のパブリックフォルダにアクセスしたところ、衝突事件映像を発見し、巡視艇の行政情報端末機に保存した。

（3） 同年10月31日、衝突事件映像を流出させた職員は、当該行政情報端末機から衝突事件映像を私有USBメモリに保存し、部外に持ち出したもの。

2. 懲戒処分等の内容

平成22年12月22日、衝突事件映像を流出させた職員については「停職12月」（同日付、辞職）、海上保安庁長官については「減給（1／10）1月」とするほか、衝突事件映像の不適正な取扱いを行った者及び管理監督者について「戒告」4名、「訓告」12名、「厳重注意(文書)」6名の合計24名に対する懲戒処分等を実施した。

平成23年１月５日
警　　察　　庁

国際テロ対策に係るデータのインターネット上への掲出事案に関する中間的見解等について（要旨）

はじめに

○　12月９日、本事案につき国家公安委員会から指示。

○　警察に対する国民の信頼を確保する上で重要と判断し、取りまとめ。

１　これまでの調査の概要

○　10月29日午後９時頃、通報により認知。警察庁・警視庁で調査開始。

○　ＡＰＥＣ首脳会議に向けた警察活動に支障が生じ、業務が妨害されたことなどから、警視庁は、データ掲出の発信元等について捜査中。

・　契約者情報、接続ログを印刷した書面等を差し押さえ

・　「ウィニー」、一般ウェブサイト等、複数の方法によりインターネット上に掲出されており、関係するＩＰアドレス等は多数

・　国外サーバに係るＩＰアドレスの解明のため関係国等に協力要請

○　また、警察庁国際テロリズム対策課・警視庁外事第三課において、警察が保有する情報の外部への持ち出しの可能性について捜査・調査中

・　外事第三課では、外部記録媒体の使用履歴の証跡管理その他の管理が不十分と思われるコンピュータが一部存在することが判明

・　現在、関係職員等に対する聞き取り、保存されている膨大なデータの検証等の捜査・調査を実施中

２　本件データの評価

○　警察が保有するデータの中には、本件データとファイル形式等が同一のものは存在しない。

○　他方、本件データに含まれる情報の内容、様式及び体裁の分析、関係職員からの聞き取り等を行ったところ、本件データには、警察職員が取り扱った蓋然性が高い情報が含まれていると認められた。

○　本件データには、次のような情報とみられるものが含まれており、警察が作成し、又は保管しているものであるか否かを個別に明らかにすることは差し控えたい。

・　個人又は団体に関する情報

・　関係国との個別のテロ対策に係る協力関係に関する情報

・　警察による情報収集活動等に関する情報

3　国家公安委員会から指示された事項に関する警察の取組状況及び今後の方針

(1) 捜査及び調査の徹底

○　警察では、引き続き、あらゆる可能性を視野に入れて必要な捜査及び調査を推進。東京地検が告訴を受理しているところ、検察当局とも連携。

(2) 個人情報が掲出された者に対する保護その他の措置

○　警察では、個人情報が掲出された方に個別に面会するなどして、必要な措置を確認するための取組みを推進中。

・　警察庁では、全国外事担当課長会議で指示

・　警視庁では、副総監通達を発出し、関係者からの相談、苦情等の申出に対し迅速かつ適切な措置を講ずることなどを指示

○　警視庁では、本事案発生直後から、プロバイダ等に対して、本件データのウェブページからの削除につき協力を要請。引き続き取組みを強化。

(3) 情報保全の徹底・強化

○　情報保全に関するプロジェクト・チームの設置、緊急実地調査の実施、今後の在り方の検討、監査の強化等の取組みを推進中。

おわりに

○　警察としては、警察職員が取り扱った蓋然性が高い情報が含まれているデータがインターネット上に掲出されたことにより、不安や迷惑を感じる方々が現にいるという事態に立ち至ったことは極めて遺憾。

○　警察では、組織の総力を挙げて取り組み、事実を究明していくこととしている。

※　留意事項

現在、捜査・調査中であり、法令上公にできない事項及び今後の捜査又は調査に支障を及ぼすおそれのある事項は記載していない。

（参考資料）

関係法令

○国家公務員法（昭和22年法律第120号）（抄）

（秘密を守る義務）

第百条　職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。

②～⑤　（略）

第百九条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

一～十一　（略）

十二　第百条第一項若しくは第二項又は第百六条の十二第一項の規定に違反して秘密を漏らした者

十三～十八　（略）

第百十一条　第百九条第二号より第四号まで及び第十二号又は前条第一項第一号、第三号から第七号まで、第九号から第十五号まで、第十八号及び第二十号に掲げる行為を企て、命じ、故意にこれを容認し、そそのかし又はそのほう助をした者は、それぞれ各本条の刑に処する。

○自衛隊法（昭和29年法律第165号）（抄）

（防衛秘密）

第九十六条の二　防衛大臣は、自衛隊についての別表第四に掲げる事項であつて、公になつていないもののうち、我が国の防衛上特に秘匿することが必要であるもの（日米相互防衛援助協定等に伴う秘密保護法（昭和二十九年法律第百六十六号）第一条第三項に規定する特別防衛秘密に該当するものを除く。）を防衛秘密として指定するものとする。

2　前項の規定による指定は、次の各号のいずれかに掲げる方法により行わなければならない。

一　政令で定めるところにより、前項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に標記を付すこと。

二　前項に規定する事項の性質上前号の規定によることが困難である場合において、政令で定めるところにより、当該事項が同項の規定の適用を受けることとなる旨を当該事項を取り扱う者に通知すること。

3　防衛大臣は、自衛隊の任務遂行上特段の必要がある場合に限り、国の行政機関の職員のうち防衛に関連する職務に従事する者又は防衛省との契約に基づき防衛秘密に係る物件の製造若しくは役務の提供を業とする者に、政令で定めるところにより、防衛秘密の取扱いの業務を行わせることができる。

4　防衛大臣は、第一項及び第二項に定めるもののほか、政令で定めるところにより、第一項に規定する事項の保護上必要な措置を講ずるものとする。

第百二十二条　防衛秘密を取り扱うことを業務とする者がその業務により知得した防衛秘密を漏らしたときは、五年以下の懲役に処する。防衛秘密を取り扱うことを業務としなくなつた後においても、同様とする。

2　前項の未遂罪は、罰する。

3　過失により、第一項の罪を犯した者は、一年以下の禁錮又は三万円以下の罰金に処する。

4　第一項に規定する行為の遂行を共謀し、教唆し、又は煽動した者は、三年以下の懲役に処する。

5　第二項の罪を犯した者又は前項の罪を犯した者のうち第一項に規定する行為の遂行を共謀したものが自首したときは、その刑を減軽し、又は免除する。

6　第一項から第四項までの罪は、刑法第三条の例に従う。

別表第四　（第九十六条の二関係）

一　自衛隊の運用又はこれに関する見積り若しくは計画若しくは研究

二　防衛に関し収集した電波情報、画像情報その他の重要な情報

三　前号に掲げる情報の収集整理又はその能力

四　防衛力の整備に関する見積り若しくは計画又は研究

五　武器、弾薬、航空機その他の防衛の用に供する物（船舶を含む。第八号及び第九号において同じ。）の種類又は数量

六　防衛の用に供する通信網の構成又は通信の方法

七　防衛の用に供する暗号

八　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの仕様、性能又は使用方法

九　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの製作、検査、修理又は試験の方法

十　防衛の用に供する施設の設計、性能又は内部の用途（第六号に掲げるものを除く。）

○自衛隊法施行令（昭和29年政令第179号）（抄）

（標記の方法）

第百十三条の二　法第九十六条の二第二項第一号の規定による標記は、別表第十一に掲げる様式に従い、同条第一項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件の見やすい箇所に、印刷、押印又は刻印その他これらに準ずる確実な方法により付さなければならない。この場合において、当該文書、図画又は物件のうち同項に規定する事項を記録し、又は化体する部分を容易に区分することができるときは、当該標記は、当該部分に付さなければならない。

（通知の方法）

第百十三条の三　法第九十六条の二第二項第二号の規定による通知は、同条第一項に規定する事項を特定して記載した書面により行わなければならない。

（他の行政機関における防衛秘密の取扱いの業務）

第百十三条の四　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する職務に従事する者に防衛秘密の取扱いの業務を行わせるときは、次に掲げる事項について、あらかじめ、当該行政機関の長と協議するものとする。

一　防衛秘密の取扱いの業務を管理する者の指名に関すること。

二　防衛秘密の取扱いの業務に従事する職員の範囲の指定に関すること。

三　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

四　防衛秘密の伝達（文書、図画又は物件の交付以外の方法によるものに限る。以下この節において同じ。）の手続に関すること。

五　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

六　当該行政機関以外の者への防衛秘密の提供の制限に関すること。

七　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

八　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（契約業者における防衛秘密の取扱いの業務）

第百十三条の五　防衛省との契約に基づき防衛秘密に係る物件の製造又は役務の提供を業とする者（次項及び第百十三条の十一において「契約業者」という。）は、次に掲げる基準に適合していなければならない。

一　防衛秘密の保護上必要な措置に関し役員及び職員が遵守すべき規則を定めているこ

と。

二　防衛秘密の取扱いの業務を管理する者を選任していること。

三　防衛秘密の取扱いの業務に従事する役員及び職員に防衛秘密の保護上必要な措置に関する教育を行つていること。

四　防衛秘密に係る文書、図画又は物件を保管するための施設設備その他防衛秘密の保護上必要な施設設備を設置していること。

2　契約業者との契約においては、次に掲げる事項を定めなければならない。

一　防衛秘密の取扱いの業務に従事する役員及び職員の範囲の指定に関すること。

二　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

三　防衛秘密の伝達の手続に関すること。

四　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

五　当該契約業者以外の者への防衛秘密の提供の制限に関すること。

六　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

七　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（防衛秘密管理者）

第百十三条の六　防衛大臣は、防衛省の職員のうちから、防衛秘密の取扱いの業務を管理する者（以下この節において「防衛秘密管理者」という。）を指名するものとする。

（防衛秘密の指定に伴う措置）

第百十三条の七　防衛大臣は、法第九十六条の二第一項に規定する事項を防衛秘密として指定したときは、指定に関する記録を作成するとともに、防衛秘密として指定した事項を当該事項に係る防衛秘密管理者に通報するものとする。

（防衛秘密の表示）

第百十三条の八　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定された場合において、第百十三条の二の規定により標記が付されたもの以外に当該防衛秘密として指定された事項を記録する文書、図画若しくは物件又は当該事項を化体する物件があるときは、当該文書、図画又は物件に、同条の規定の例により、防衛秘密の表示をする措置を講じなければならない。ただし、当該物件の性質上表示をすることが困難である場合は、この限りでない。

（防衛秘密の周知）

第百十三条の九　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定されたときは、当該事項の取扱いの業務に従事する防衛省の職員にその旨を周知させなければならない。

（職員の範囲の指定）

第百十三条の十　防衛秘密の取扱いの業務に従事する防衛省の職員の範囲は、防衛秘密管理者が定める。

（他の行政機関等における防衛秘密の取扱いの業務に伴う措置）

第百十三条の十一　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する

職務に従事する者又は契約業者に防衛秘密の取扱いの業務を行わせるときは、防衛秘密管理者に防衛秘密に係る文書、図画若しくは物件を交付させ、又は防衛秘密を伝達させるものとする。

2　前項の交付又は伝達は、防衛秘密として指定された事項を特定して行うものとする。

（防衛秘密が要件を欠くに至つた場合の措置）

第百十三条の十二　防衛大臣は、防衛秘密として指定した事項が法第九十六条の二第一項に規定する要件を欠くに至つたときは、速やかに、当該事項に係る防衛秘密管理者に当該事項が防衛秘密でなくなつた旨を通報するものとする。

2　前項の通報を受けた防衛秘密管理者は、直ちに、当該通報に係る事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に付された第百十三条の二の規定による標記及び第百十三条の八の規定による表示を抹消する措置を講ずるとともに、当該事項の取扱いの業務に従事する防衛省の職員及び前条第一項の規定により当該事項に係る文書、図画若しくは物件を交付し、又は当該事項を伝達した相手方に当該事項が防衛秘密でなくなつた旨を周知させなければならない。

（防衛秘密の取扱いの管理のための措置）

第百十三条の十三　防衛秘密管理者は、第百十三条の八から前条までに規定するもののほか、防衛大臣の定めるところにより、防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱い及び防衛秘密の伝達を適切に管理するための措置を講じなければならない。

（委任規定）

第百十三条の十四　この節に規定するもののほか、防衛秘密の保護上必要な措置に関する細目は、防衛大臣が定める。

○日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号）（抄）

（定義）

第一条　この法律において「日米相互防衛援助協定等」とは、日本国とアメリカ合衆国との間の相互防衛援助協定、日本国とアメリカ合衆国との間の船舶貸借協定及び日本国に対する合衆国艦艇の貸与に関する協定をいう。

2　この法律において「装備品等」とは、船舶、航空機、武器、弾薬その他の装備品及び資材をいう。

3　この法律において「特別防衛秘密」とは、左に掲げる事項及びこれらの事項に係る文書、図画又は物件で、公になつていないものをいう。

一　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された装備品等について左に掲げる事項

イ　構造又は性能

ロ　製作、保管又は修理に関する技術

ハ　使用の方法

ニ　品目及び数量

二　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された情報で、装備品等に関する前号イからハまでに掲げる事項に関するもの

（特別防衛秘密保護上の措置）

第二条　特別防衛秘密を取り扱う国の行政機関の長は、政令で定めるところにより、特別防衛秘密について、標記を附し、関係者に通知する等特別防衛秘密の保護上必要な措置を講ずるものとする。

（罰則）

第三条　左の各号の一に該当する者は、十年以下の懲役に処する。

一　わが国の安全を害すべき用途に供する目的をもつて、又は不当な方法で、特別防衛秘密を探知し、又は収集した者

二　わが国の安全を害する目的をもつて、特別防衛秘密を他人に漏らした者

三　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を他人に漏らしたもの

2　前項第二号又は第三号に該当する者を除き、特別防衛秘密を他人に漏らした者は、五年以下の懲役に処する。

3　前二項の未遂罪は、罰する。

第四条　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らしたものは、二年以下の禁こ又は五万円以下の罰金に処する。

2　前項に掲げる者を除き、業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らした者は、一年以下の禁こ又は三万円以下の罰金に処する。

第五条　第三条第一項の罪の陰謀をした者は、五年以下の懲役に処する。

2　第三条第二項の罪の陰謀をした者は、三年以下の懲役に処する。

3　第三条第一項の罪を犯すことを教唆し、又はせん動した者は、第一項と同様とし、同条第二項の罪を犯すことを教唆し、又はせん動した者は、前項と同様とする。

4　前項の規定は、教唆された者が教唆に係る犯罪を実行した場合において、刑法（明治四十年法律第四十五号）総則に定める教唆の規定の適用を排除するものではない。

（自首減免）

第六条　第三条第一項第一号若しくは第三項又は前条第一項若しくは第二項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

（この法律の解釈適用）

第七条　この法律の適用にあたつては、これを拡張して解釈して、国民の基本的人権を不当に侵害するようなことがあつてはならない。

○日米相互防衛援助協定等に伴う秘密保護法施行令（昭和29年政令第149号）（抄）

（秘密区分）

第一条　日米相互防衛援助協定等に伴う秘密保護法第一条第三項に規定する特別防衛秘密は、その秘密の保護の必要度に応じて、機密、極秘又は秘のいずれかに区分しなければならない。

2　前項の「機密」とは、秘密の保護が最高度に必要であつて、その漏えいが我が国の安全に対し、特に重大な損害を与えるおそれのあるものをいう。

3　第一項の「極秘」とは、秘密の保護が高度に必要であつて、その漏えいが我が国の安全に対し、重大な損害を与えるおそれのあるものをいう。

4　第一項の「秘」とは、秘密の保護が必要であつて、機密及び極秘に該当しないものをいう。

（秘密区分の指定、変更及び解除）

第二条　国の行政機関（内閣府並びに内閣府設置法（平成十一年法律第八十九号）第四十九条第一項及び第二項に規定する機関並びに国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関をいう。以下同じ。）の長（以下「各省庁の長」という。）で、アメリカ合衆国政府から特別防衛秘密に属する事項又は文書、図画若しくは物件の供与を受けたものは、その特別防衛秘密につき、前条に規定する秘密区分の指定を行わなければならない。

2　前項の国の行政機関の長は、同項の規定により指定した秘密区分を変更することができる。

3　第一項の国の行政機関の長は、特別防衛秘密として秘匿する必要がなくなつたとき、又は公になつたものがあるときは、その部分に限り、速やかに、秘密区分の指定を解除しなければならない。

4　第一項の国の行政機関の長は、特別防衛秘密について、前三項の規定により秘密区分を指定し、変更し、又は解除したときは、必要に応じ、その旨を関係行政機関に通知しなければならない。

（標記）

第三条　各省庁の長は、その取り扱う特別防衛秘密に属する文書、図画又は物件につき、これらが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨の標記をしなければならない。

2　各省庁の長は、前条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、速やかに、前項の標記を変更し、又は抹消しなければならない。

3　第一項の標記の様式は、別記様式のとおりとする。

（通知）

第四条　各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図画若しくは物件であつて、前条の規定による標記ができないもの若しくは標記をすることが適当でないものについては、関係者に対し、文書又は口頭により、これが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨の通知をしなければならない。

2　各省庁の長は、第二条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、必要に応じ、速やかに、その旨を関係者に対し、文書により、通知しなければならない。

（掲示）

第五条　各省庁の長は、その管理する施設内にある特別防衛秘密に属する物件について、必要があるときは、その物件に近接してはならない旨の掲示を行うものとする。

（委託中における特別防衛秘密保護上の措置）

第六条　各省庁の長は、その取り扱う特別防衛秘密を製作、修理、実験、調査研究、複製等のため政府機関以外の者に委託する場合は、委託中における秘密の漏えいの危険を防止するため、契約条項に秘密保持に関する規定を設ける等必要な措置を講じなければならない。

（特別防衛秘密保護上の措置の実施細目）

第七条　第二条から前条までに規定するもののほか、各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図面若しくは物件の複製、送達、伝達、接受、保管、破棄等その取扱いに関し、特別防衛秘密の保護上必要な措置を講じなければならない。

2　前項に規定する特別防衛秘密の保護上必要な措置の実施細目については、各省庁の長が定める。

○日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法（昭和27年法律第138号）（抄）

（定義）

第一条　この法律において「協定」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定をいう。

2　この法律において「合衆国軍隊」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約に基づき日本国にあるアメリカ合衆国の陸軍、空軍及び海軍をいう。

3　この法律において「合衆国軍隊の構成員」、「軍属」又は「家族」とは、協定第一条に規定する合衆国軍隊の構成員、軍属又は家族をいう。

（合衆国軍隊の機密を侵す罪）

第六条　合衆国軍隊の機密（合衆国軍隊についての別表に掲げる事項及びこれらの事項に係る文書、図画若しくは物件で、公になつていないものをいう。以下同じ。）を、合衆国軍隊の安全を害すべき用途に供する目的をもつて、又は不当な方法で、探知し、又は収集した者は、十年以下の懲役に処する。

2　合衆国軍隊の機密で、通常不当な方法によらなければ探知し、又は収集することができないようなものを他人に漏らした者も、前項と同様とする。

3　前二項の未遂罪は、罰する。

第七条　前条第一項又は第二項の罪の陰謀をした者は、五年以下の懲役に処する。

2　前条第一項又は第二項の罪を犯すことを教唆し、又はせん動した者も、前項と同様とする。

3　前項の規定は、教唆された者が、教唆に係る犯罪を実行した場合において、刑法総則に定める教唆の規定の適用を排除するものではない。

第八条　第六条第一項の罪、同項に係る同条第三項の罪又は同条第一項に係る前条第一項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

別表

一　防衛に関する事項

イ　防衛の方針若しくは計画の内容又はその実施の状況

ロ　部隊の隷属系統、部隊数、部隊の兵員数又は部隊の装備

ハ　部隊の任務、配備又は行動

ニ　部隊の使用する軍事施設の位置、構成、設備、性能又は強度

ホ　部隊の使用する艦船、航空機、兵器、弾薬その他の軍需品の種類又は数量

二　編制又は装備に関する事項

イ　編制若しくは装備に関する計画の内容又はその実施の状況

ロ　編制又は装備の現況

ハ　艦船、航空機、兵器、弾薬その他の軍需品の構造又は性能

三　運輸又は通信に関する事項

イ　軍事輸送の計画の内容又はその実施の状況
ロ　軍用通信の内容
ハ　軍用暗号

○不正競争防止法（平成５年法律第47号）（抄）

（定義）

第二条　この法律において「不正競争」とは、次に掲げるものをいう。

一～六　（略）

七　営業秘密を保有する事業者（以下「保有者」という。）からその営業秘密を示された場合において、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為

八～十五　（略）

２～５　（略）

６　この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

７～10　（略）

（罰則）

第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。

一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。以下この条において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第三条に規定する不正アクセス行為をいう。）その他の保有者の管理を害する行為をいう。以下この条において同じ。）により、営業秘密を取得した者

二　詐欺等行為又は管理侵害行為により取得した営業秘密を、不正の利益を得る目的で、又はその保有者に損害を加える目的で、使用し、又は開示した者

三　営業秘密を保有者から示された者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、次のいずれかに掲げる方法でその営業秘密を領得した者

イ　営業秘密記録媒体等（営業秘密が記載され、又は記録された文書、図画又は記録媒体をいう。以下この号において同じ。）又は営業秘密が化体された物件を横領すること。

ロ　営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その複製を作成すること。

ハ　営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装すること。

四　営業秘密を保有者から示された者であって、その営業秘密の管理に係る任務に背いて前号イからハまでに掲げる方法により領得した営業秘密を、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、使用し、又は開示した者

五　営業秘密を保有者から示されたその役員（理事、取締役、執行役、業務を執行する社員、監事若しくは監査役又はこれらに準ずる者をいう。次号において同じ。）又は従業者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、その営業秘密を使用し、又は開示した者（前号に掲げる者を除く。）

六　営業秘密を保有者から示されたその役員又は従業者であった者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その在職中に、その営業秘密の管理に係る任務に背いてその営業秘密の開示の申込みをし、又はその営業秘密の使用若しくは開示について請託を受けて、その営業秘密をその職を退いた後に使用し、又は開示した者（第四号に掲げる者を除く。）

七　不正の利益を得る目的で、又はその保有者に損害を加える目的で、第二号又は前三号の罪に当たる開示によって営業秘密を取得して、その営業秘密を使用し、又は開示した者

2・3　（略）

4　第一項第二号又は第四号から第七号までの罪は、詐欺等行為若しくは管理侵害行為があった時又は保有者から示された時に日本国内において管理されていた営業秘密について、日本国外においてこれらの罪を犯した者にも適用する。

5～7　（略）

第二十二条　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、前条第一項第一号、第二号若しくは第七号又は第二項に掲げる規定の違反行為をしたときは、行為者を罰するほか、その法人に対して三億円以下の罰金刑を、その人に対して本条の罰金刑を科する。

2　前項の場合において、当該行為者に対してした前条第一項第一号、第二号及び第七号並びに第二項第五号の罪に係る同条第三項の告訴は、その法人又は人に対しても効力を生じ、その法人又は人に対してした告訴は、当該行為者に対しても効力を生ずるものとする。

3　第一項の規定により前条第一項第一号、第二号若しくは第七号又は第二項の違反行為につき法人又は人に罰金刑を科する場合における時効の期間は、これらの規定の罪についての時効の期間による。

第2回秘密保全のための法制の在り方に関する有識者会議　座席表

平成23年2月18日（金）午後1時30分～午後3時30分　於：官邸4階大会議室

（出入口）

内閣情報調査室	内閣情報調査室	内閣情報官	内閣官房長官	縣委員（座長）	櫻井委員	防衛省
○	○	○	○	○	○	○

事務局　○　○　○　○

配付資料

資料１　「防衛秘密」制度の運用状況

資料２　秘密の範囲・秘密の管理①に関する考え方（事務局案）・論点

機密性2情報

対外非公表　取扱注意　配付資料2

秘密保全のための法制の在り方に関する有識者会議（第２回）

秘密の範囲・秘密の管理①に関する考え方（事務局案）・論点

平成２３年２月１８日

第1　秘密保全法制の目的

対外非公表　取扱注意

事　務　局　案

現 状

○ 外国情報機関等の情報収集活動により、情報が漏えいし、又はそのおそれが生じた事案が従来から発生

○ IT技術やネットワーク社会の進展に伴い、政府の保有する情報がネットワーク上に流出し、極めて短期間に世界規模で広がる事案が発生

⇒ 我が国の国益を守り、国民の安全を確保するためには、政府が保有する重要な情報の漏えいにより国益が損なわれるような事態を防止する制度を確立する必要あり

○ 政府の政策判断が適正に行われるためには、政府部内や外国との間での情報共有の促進が重要

⇒ 秘密保全に関する法制度を整備し、秘匿すべき情報が漏れないという相互信頼を確立することが不可欠

⇕

秘密保全に関する我が国の現行法令は、防衛秘密や特別防衛秘密に関する保全制度はあるが、秘密の漏えいを防止するための管理に関する規定や罰則の整備が不十分

本法制の目的

政府が保有する特に秘匿を要する情報の漏えいを防止

⇒ 国益や国民の安全を確保

⇒ 政府の秘密保全体制に対する国内外の信頼を確保

※ 秘密保全と情報公開との適切なバランスに留意が必要であり、守らなければならない秘密を守りつつ、情報の公開がいたずらに制限されないようにすべき。

論 点

○ 目的の当否

第2　秘密の範囲（秘密とすべき事項①）

対外非公表　取扱注意

事　務　局　案

※　本法制で保護の対象とする特に秘匿を要する秘密を便宜的に「特別秘密」と呼ぶこととする。

特別秘密※として保護すべき事項の範囲

ある事項を秘密として厳格な保全の対象とすることは、これにより得られる利益がある反面、国の説明責任への影響や行政コストの増大も考えられる

⇩

行政機関等が保有する秘密情報の中でも、国の存立にとって重要なもののみを特別秘密として厳格な保全の対象とすることが適当

⇒

①国の安全
②外交
③公共の安全及び秩序の維持

の３分野を対象とすることが適当

※　いわゆる捜査資料については、様々な資料が含まれる上、分量も膨大であることから、捜査資料であることを理由にそのすべてを一律に本法制の秘密として取り扱うことは適当でないが、個別の捜査資料の中に本法制の下で特別秘密として取り扱われるべきものが含まれる場合には、その秘密保持について特別の取扱いを検討する必要があると考えられる。

論　点

○事項の範囲の当否

第2 秘密の範囲 （秘密とすべき事項②）

事 務 局 案

事項の限定列挙・秘匿の必要性による絞り込み

○ 特別秘密として保護する情報は、特に秘匿の必要性が高いものに限定

⇨ 前記3分野の中から別表形式等で具体的事項を列挙

具体的事項の例：（一例であり、今後、法制化の際には更なる精査が必要）

○ 国の安全
「自衛隊の運用又はこれに関する見積り、計画若しくは研究」
「防衛に関し収集した電波情報、画像情報その他の重要な情報」
「武器、弾薬、航空機その他の防衛の用に供する物の種類又は数量」

○ 外交
「外交における重要な交渉、協力及び政務の処理の内容」
「外交において必要な外国等、国際機関等又は国際情勢に関する重要な情報」

○ 公共の安全及び秩序の維持
「テロに対処するための計画又はこれらの実施状況若しくはこれらに係る研究」
「テロを実行するおそれのある者又は組織の意図又は能力に係る内部情報等」

⇨ 高度の秘匿の必要性を要件化

要件の例：

○「我が国の防衛上、外交上又は公共の安全及び秩序の維持上特に秘匿することが必要である場合」

○「その漏えいにより国の重大な利益を害するおそれがある場合」

参考：自衛隊法第９６条の２第１項（抄）

防衛大臣は、自衛隊についての別表第四に掲げる事項であつて、公になつていないもののうち、我が国の防衛上特に秘匿することが必要であるもの…を防衛秘密として指定するものとする。

論 点

○絞り込みの方法・内容の当否

第2 秘密の範囲 （秘密の作成又は取得の主体に関する範囲）

対外非公表　取扱注意

事 務 局 案

秘密の作成又は取得の主体 （当該主体が作成・取得した情報を本法制の適用対象とすべきか）

行政機関等	国の行政機関	○ 本法制の目的…政府が保有する秘密の漏えい防止	適用対象
	独立行政法人等	○ 国の安全等に関する情報を作成・取得する例あり ○ 実質的には国の行政の一端を担う公的機関	適用対象に含めることが適当
	地方公共団体	○ 公共の安全・秩序の維持に関して特に秘匿を要する情報を作成・取得する例あり（警察事務） ○ 公的機関として国と密接な関係を有しつつ、地域における行政を実施	適用対象に含めることが適当 ただし、通常取り扱う特別秘密は警察事務等に限られると考えられるところ、地方公共団体の自主性も考慮すると、地方公共団体に対する適用範囲を限定すること等も選択肢
民間・大学		○ 国の安全等に関する情報を作成・取得する可能性あり ● 経済活動の自由・学問の自由の観点から、国家による過度の干渉にもつながりかねない ● 民間における情報漏えいに関しては、不正競争防止法において従業員等による営業秘密の開示等に対する処罰を規定	適用対象としないことが適当 ただし、行政機関等からの事業委託を受ける場合は、当該事業に関しては委託をした行政機関等と実質的に一体と考えられるから、このような場合は、民間や大学が作成・取得した情報も適用対象とすることが適当

論 点

○ 主体の範囲の是非

第3　秘密の管理①（秘密の指定）

対外非公表　取扱注意

事　務　局　案

1　指定行為

特別秘密は厳格な保全の対象 … 対象となる範囲を明確に特定することが適当

⇨ 標記（通知）による指定が適当　…　実質秘であり、かつ、要式行為たる指定行為により外縁を明確化されたものに限定

2　指定権者

○ 原則として、秘密の作成・取得主体である行政機関等が指定

○ 事業委託を受けた民間企業等が作成・取得した情報：
委託をした行政機関等が、情報の流出による当該事業への影響等を最も的確に判断できる　⇨ 原則として、委託元である行政機関等が指定

3　指定の効果

○ 特別秘密としての取扱いを受けることになる

⇨ 厳重な人的管理・物的管理に服する

⇨ 特別秘密の作成・取得の目的に照らし、他の行政機関等や民間企業等と共有すべき場合には、共有を認めることが適当（自衛隊法上の防衛秘密も、一定の要件の下で防衛省外の者への伝達が認められている）

ただし、特別秘密の漏えいを防ぐために、共有先の行政機関等又は民間企業等において、法令又は契約等により特別秘密の適切な管理が確保されることを前提とすることが適当

第3　秘密の管理①（秘密の指定）

対外非公表　取扱注意

事　務　局　案（続き）

4　他の行政目的のための秘密の伝達

許認可、会計検査、捜査等の他の行政機関等の事務の遂行のため、本来伝達を想定していない当該他の行政機関等に特別秘密を伝達する必要性が認められる場合があり得るが、本法制の趣旨にかんがみ望ましいものではない

⇨ 他の行政機関等における当該情報の必要性等を踏まえ、特別秘密の伝達の必要性を的確に判断すべき

⇨ 伝達先において法令に基づき特別秘密の管理が確保されていることを前提とするなど、伝達により当該秘密の保護が損なわれないようにすべき

5　指定の解除

指定の要件に該当しなくなった特別秘密について、指定を迅速に解除することは、本法制に対する国民の理解を得る上で重要

⇨ 要件に該当しなくなった場合、指定権者において速やかに指定を解除する義務を定める

⇨ さらに、一定期間ごとに指定の要否を再検討する機会を設ける更新制を採用すべきか

6　指定の調整等

特別秘密は、その性格上、統一的に指定され、解除されることが必要

⇨ 国の行政機関間…特別秘密の指定及び解除について判断が異なる場合の調整の仕組みを整理することが必要

⇨ 国の行政機関以外の行政機関等の指定・解除…国が一定の関与を行う枠組みを設けることが必要

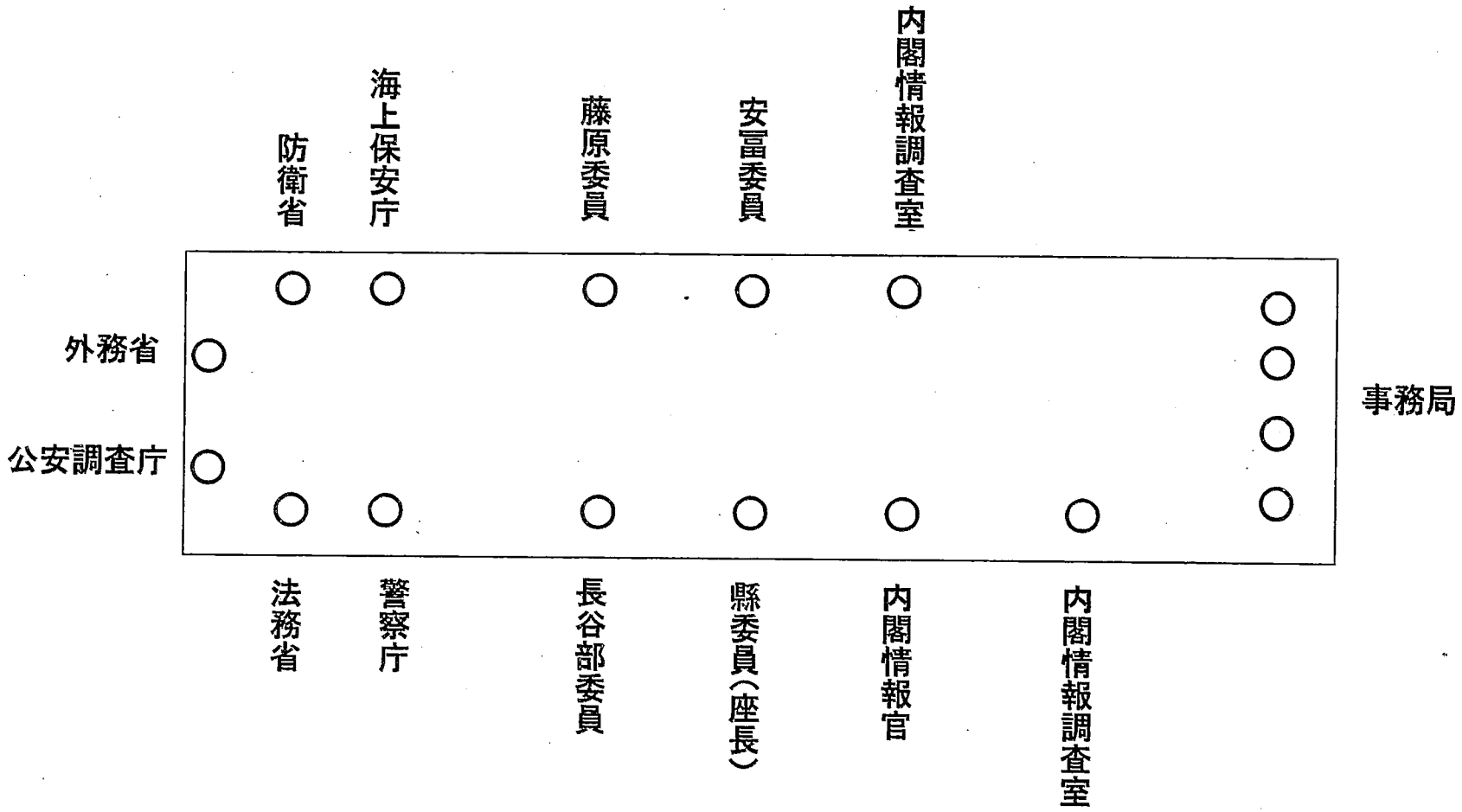
論　点

○指定行為・指定権者　－　独立行政法人、地方公共団体の扱い
○指定の効果・他の行政目的のための伝達　－　外部との共有の在り方・条件
○指定の解除　－　解除制度の在り方
○指定の調整等　－　仕組みの要否・当否

第3回秘密保全のための法制の在り方に関する有識者会議　座席表

平成23年4月8日（金）午後1時～午後3時　於：内閣府本府5階特別会議室

（出入口）



配付資料

資料１　現行の秘密取扱者適格性確認制度

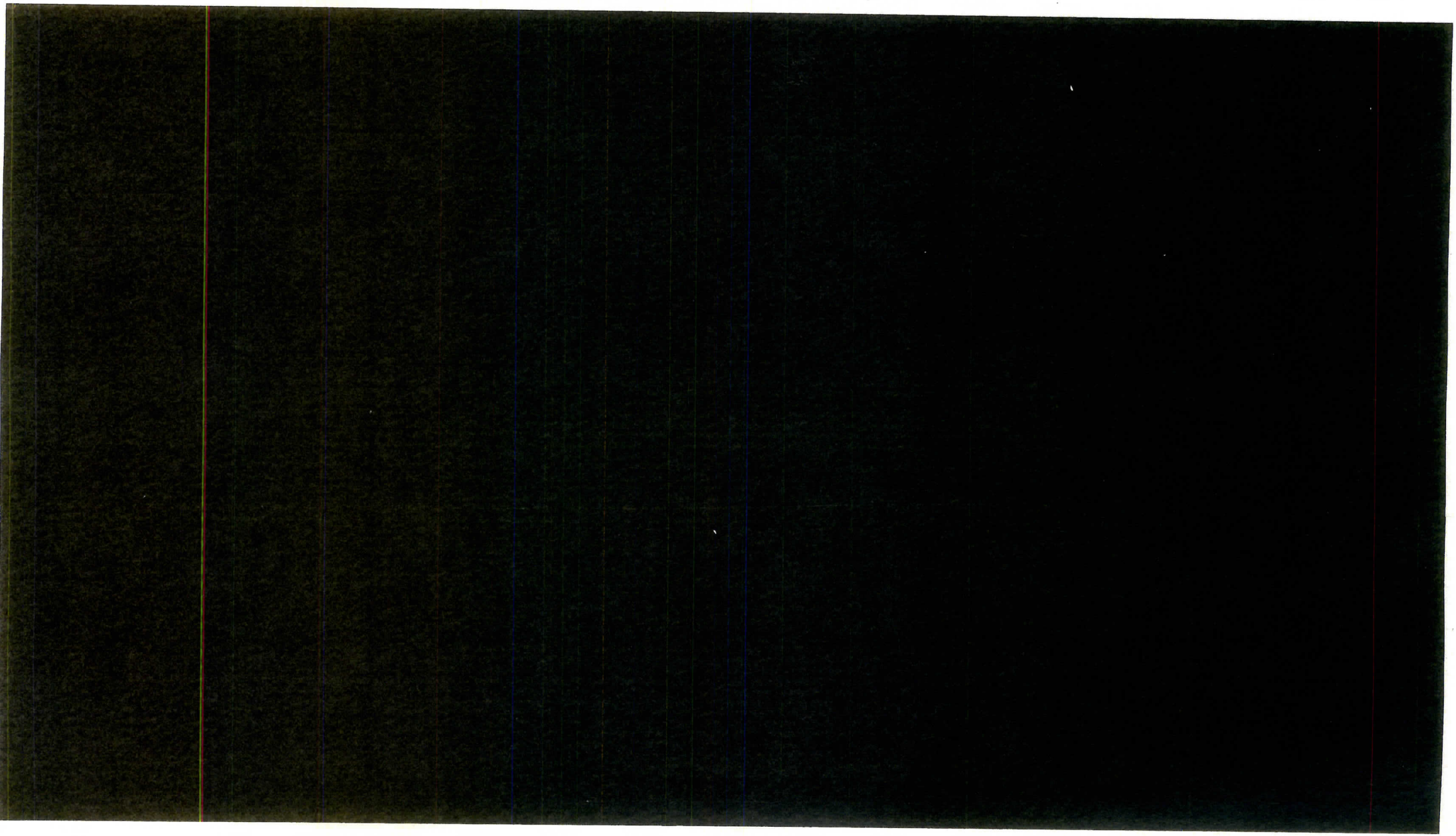
資料２　秘密の管理②に関する考え方（事務局案）・論点

資料３　諸外国における秘密取扱者適格性確認制度の概要

秘密取扱者適格性確認制度の概要

対外非公表

席上回収



対外非公表　取扱注意　配布資料2

秘密保全のための法制の在り方に関する有識者会議（第３回）

秘密の管理②に関する考え方（事務局案）・論点

平成２３年４月８日

第３　秘密の管理②（概要）

対外非公表　取扱注意

事　務　局　案

特　別　秘　密

行政機関等が保有する秘密情報の中でも、国の存立にとって重要なもの

厳　重　な　管　理　に　よ　る　保　全

１　秘密の指定

２　人的管理
（１）　取扱者の限定（適格性確認制度）
（２）　管理責任体制
（３）　研修

３　物的管理

○　ライフサイクル※の各段階における管理
※　特別秘密が作成・取得又は伝達されてから保管・利用等を経て廃棄又は移管まで

○　電子計算機の取扱い等の管理

○　検査

第３　秘密の管理②人的管理（適格性確認制度①）

対外非公表　取扱注意

事　務　局　案

１　特別秘密を取り扱わせる者の限定

○ 特別秘密を取り扱わせるに足る信用性・信頼性を有している者と確認された者が業務遂行のために知る必要のある場合にのみ特定の特別秘密を取り扱わせることを基本とすべき。

⇨ 適格性確認

①　我が国における適格性確認の現状と課題

≪現状≫

特別管理秘密※の取扱者に係る適格性確認制度を実施（平成21年４月～）

（「カウンターインテリジェンス機能の強化に関する基本方針」（平成19年８月カウンターインテリジェンス推進会議決定）による。）

≪課題≫

- 対象者が国の行政機関の職員のみであり（法的位置付けはない）、同様に特別秘密を取り扱わせる民間事業者等の職員が含まれていないこと。
- 適格性確認の実施権者が、確認の判断材料となる情報を公務所その他の公私の団体に照会する権限が明定されていないこと。　等

②　諸外国（米、英、独、仏）の例

○ 国にとって重大な秘密を保全する制度の必要不可欠な一部として適格性確認制度を導入・運用

≪共通点≫

- 制度の内容が法令等によって明らかにされていること。
- 国の行政機関から事業委託を受ける民間事業者等の職員も対象としていること。
- 情報収集・裏付けのため公務所その他の公私の団体に対して渡航履歴等の照会を行っていること。
- 結果を本人に通知していること。
- 収集された個人情報を厳格に保護することとしていること。　等

⇨ 秘密保全制度の整備に当たっては、適格性確認を法制度上明らかに位置付けることが以下の点から重要

- 特別秘密の保全の実効性を向上させること。
- 適格性確認を含む秘密保全制度への国民の理解を得ること。
- 我が国の秘密保全体制に対する国内外からの信用・信頼を維持・向上させること。

論　点

○ 秘密保全制度の整備に当たって適格性確認制度を法制度上明らかに位置付けることの当否

※ 各行政機関が保有する国の安全、外交上の秘密その他の国の重大な利益に関する事項であって、公になっていないもののうち、特に秘匿することが必要なものとして当該機関の長が指定したもの

第３　秘密の管理②人的管理（適格性確認制度②）

対外非公表　取扱注意

事　務　局　案

２　対象者

特別秘密の取扱いが当然に想定される行政機関等・民間事業者等※1

- ○　特別秘密を作成・取得する行政機関等で特別秘密を取り扱う者　＊
- ○　作成・取得の目的に照らし伝達される行政機関等又は民間事業者等で特別秘密を取り扱う者　＊

特別秘密の作成・取得の目的に照らし、特別秘密の取扱いが本来は想定されていない行政機関等

- ○　その事務の遂行のために必要性が認められて特別秘密の伝達を受け、取り扱う者　＊
  - 特別秘密を取り扱うことが事前に予測されておらず、かつ、緊急に当該秘密を取り扱わなければ事務の遂行に著しく支障を来す者※2

適格性確認を実施

＊　行政機関の長等は、適格性の確認を実施中である者に、速やかに特別秘密を取り扱わせなければならないと認められる十分な理由がある場合には、正規の方法に準じて暫定的に適格性を確認の上、一定期間に限り、例外的に特別秘密を取り扱わせることができることとする。
　なお、一定期間を超えた場合には、正規の適格性確認なしに当該者に特別秘密を取り扱わせることはできない。

≪特別秘密の保護が損なわれないために以下を実施≫

- ○　適格性確認以外の人的管理（P7参照）
- ○　特別秘密の保管・利用等における物的管理（同上）
- ○　適格性が疑われるようなことがない旨の誓約書を提出させる（例）

≪継続して特別秘密を取り扱わせる場合≫

- ○　一定期間内に適格性確認を実施（その必要性について要検討）

○　我が国の行政権が属する内閣を組織する内閣総理大臣及び国務大臣は適格性確認の対象外
（その他の特別な任命の要件・手続が採用されている職については、個別に判断）

論　点

- ○　対象者の範囲及び考え方の当否
- ○　正規の適格性確認の例外の場合における特別秘密の保全の在り方

※1　「民間事業者等」には、国の行政機関から委託を受けた者のほか、下請けの事業者も含まれる。
※2　該当し得る行政機関の事務については、個別に検討していく。

第３　秘密の管理②人的管理（適格性確認制度③）

対外非公表　取扱注意

事　務　局　案

３　実施権者

考え方

国の存立にとって重要な秘密として国が特別秘密に指定したものについて、これを厳重な管理に服せしめるのは国の責務　⇒　国の厳重な管理の一環として、取り扱わせようとする者を限定し、秘密漏えいのリスクを低減させる措置は、国が自ら実施することが最も適当

≪特別秘密の取扱機関≫	≪ 実 施 権 者 ≫	≪ 備 考 ≫
国の行政機関	各行政機関の長	○ それぞれ任務・所掌事務に基づき事務を処理・執行 ○ 各行政機関の長の判断に一貫性が確保されるよう調査の事項、方法等について共通化が必要
独立行政法人等	主務大臣	○ 主務大臣の関与の下で事務・事業を実施 （○ 国と密接な関係を有し、実質的に国の行政の一端を担っていることを考慮し、独立行政法人等が自ら適格性確認を行うこともあり得る）
都道府県警察	警視総監又は警察本部長※	○ 都道府県警察は、国家的性格を有する警察事務を所掌
民間事業者等	委託した国の行政機関の長	○ 委託した国の行政機関側の必要性に基づいた秘密の取扱い

※ 警察以外の地方公共団体を本法制の対象とする場合における実施権者については別途検討

論　点

○ 考え方の当否

○ 各実施権者の当否
（特に独立行政法人等、都道府県警察、民間事業者等）

第3　秘密の管理②人的管理（適格性確認制度④）

対外非公表　取扱注意

事　務　局　案

4　評価の観点及び調査事項

評価の観点

- 我が国の不利益となる行動をしないこと
- 諜報活動に取り込まれる弱点がないこと
- 自己管理能力があること又は自己を統制できない状態に陥らないこと
- ルールを遵守する意思及び能力があること
- 情報を保全する意思及び能力があること

調査事項（例）

- 対日有害活動その他これに類する活動への関与
- 外国への渡航履歴
- 本人・配偶者等の人物特定事項
- 懲戒処分歴等
- 犯罪歴
- 金銭問題
- アルコール依存
- 薬物の濫用等
- 精神状態
- 情報の不適切な取扱い
- 特異な言動

評価基準

秘密保全上のリスクを評価

適格性を確認

又は

適格性を否定

○　必要な調査事項の明示　⇦　制度の透明性を高め、国民の理解を得るため

○　評価の基準は明示せず　⇦　秘密保全上のリスクを回避するため
（対抗措置を取られる機会を与えるおそれ）

論　点

○　評価の観点の当否
○　調査事項の検討の方向性
○　評価の観点・調査事項を明示し、評価基準を明示しないことの当否

第３　秘密の管理②人的管理（適格性確認制度⑤）

対外非公表　取扱注意

事　務　局　案

５　方法・手続

対象職員の同意

対象職員 ⇔ 実施権者

≪説明≫

≪書面による同意≫

適格性確認の実施（公私の団体への照会等を含む。）

実施権者による調査

対象職員 ⇔ 実施権者

≪調査票の提出≫※

≪面接≫

更に必要がある場合

≪公私の団体への照会≫
① 対象職員自らが資料を取り寄せて提出
② 実施権者が照会権限に基づき照会

≪対象職員をよく知る者への質問≫
対象者の同意を得て実施権者が実施

※　国の行政機関の長が、独立行政法人等、地方公共団体又は民間事業者等の職員の適格性確認を実施する場合、当該職員は、調査票を密封の上、所属機関を経由して提出

的確な実施

判断に重要な影響を与える事項がある場合には、本人からより詳細な説明を聞くなど、慎重かつ細心の注意を払うことが必要

通知

適格性を確認

必要に応じ、有効期限を超える前に再確認を実施

又は

適格性を否定

直接国民の権利・義務を形成し、又はその範囲を確定しないため、行政処分に該当せず

○　適格性確認の実施に当たっては、様々な個人情報等を取り扱う必要があるところ、必要な範囲を超えて個人情報を収集しないこと、収集した個人情報を適格性確認以外の目的で利用・提供しないこと等、個人情報の保護に係る法令に基づき、実施権者は対象職員のプライバシーの保護が確実に図られるよう必要かつ適切な措置を講ずることが必要

論　点

○　適格性確認の調査の方法・手続についての当否

第３　秘密の管理②人的管理（その他）及び物的管理

対外非公表　取扱注意

事　務　局　案

その他の人的管理

≪管理責任体制≫

○　特別秘密を取り扱う機関ごとに、組織内における役割・責任の適切な分担体制を構築

⇨　情報保全のための措置を確実・効率的に実施

（分担体制の例）
- 特別秘密の取扱業務の全般を管理する責任者
- 組織の基礎的な単位で管理責任を補佐する者
- 日常的な取扱いの場面において、個別具体的な保全措置に係る事務を行う担当者

≪研　修≫

○　特別秘密を取り扱わせることとする時点及び定期的な研修の実施

⇨　保全に必要な具体的知識の徹底

⇨　保全の意識の高揚

物　的　管　理

○　特別秘密が作成・取得あるいは伝達されてから移管又は廃棄されるまでの各段階等において、日常的に保全措置を講ずることが必要。

（個別具体的な保全措置の例）
- 特別秘密に係る文書・図画・物件の作成・取得の手続
- 特別秘密に係る文書・図画・物件の運搬・交付及び特別秘密の伝達の方法
- 特別秘密に係る文書・図画の保管・利用等のアクセスの手続・方法
- 特別秘密に係る文書・図画・物件の廃棄又は移管の手続・方法

- 特別秘密に係る電子計算機情報の取扱い方法
- 携帯型情報通信・記録機器の持込みの制限

- 特別秘密の保護の状況についての検査の実施

○　特別秘密を取り扱うことが当然に想定されている行政機関等や民間事業者等　⇨　保全措置を実施

○　特別秘密を取り扱うことが想定されていないが、事務遂行のため特別秘密を伝達された行政機関等　⇨　上記の行政機関等や民間事業者等に準じた保全措置を実施

⇨　技術的な細目であることを考慮して法制上に適切に位置付けていく。

論　点

○　上記の考え方の当否

対外非公表　取扱注意　配布資料3

秘密保全のための法制の在り方に関する有識者会議（第３回）

諸外国におけるセキュリティクリアランス制度の概要

平成２３年４月８日

アメリカにおけるセキュリティクリアランス制度

対外非公表　取扱注意

根拠		①合衆国法典第50編第15章第6節第435条～第438条（秘密情報へのアクセス手続、クリアランス、照会権限、例外等）、②行政命令12968号（クリアランス）、③秘密情報へのアクセスに関する背景調査基準、④秘密情報へのアクセスの適格性決定のための判定ガイドライン、⑤行政命令13526号（秘密指定）　等
クリアランスの区分		取り扱う秘密の区分（「機密」、「極秘」、「秘」）に応じた3段階のクリアランス
適格性確認の対象者		・大統領・副大統領を除く連邦行政府職員、契約事業者等（行政命令12968号） ・大統領・副大統領・連邦議会議員・連邦最高裁判所裁判官及び大統領による任命を受けた連邦裁判所裁判官は対象外（法第437条）
	※　例外措置	・人命又は国土防衛上の差し迫った脅威への対応が必要な緊急の場合→関係行政機関の長又はその指名した職員は、適格性を確認されていない者に対する秘密情報の開示を許可できる。ただし、開示は最小限に限定される。 ・適格性確認の終了前に業務遂行が必須である例外的な場合→提出された調査票に対する好意的な評価に加え、機密レベルでは連邦捜査局への犯罪歴等照会及び国防省への照会を経て、暫定的に適格性が確認される。
実施権者		連邦行政府機関が適格性を判定（契約事業者等については、秘密を提供する連邦政府機関がスポンサーとなって判定）
	※　調査の委託	連邦人事局に委託可能（連邦捜査局等は自ら実施） ※　連邦人事局では、民間事業者を含む約9,000人のスタッフにより、年間約200万件の調査を実施。
評価の観点		米国への絶対的忠誠、人格の強靭性、信用性、正直さ、信頼性、思慮分別さ、確かな判断力、利益相反及び威圧の潜在的可能性からの自由、秘密の取扱いに係る規則を守る意思及び能力
調査事項		①合衆国に対する忠誠、②外国の影響、③外国への傾倒、④性的行動、⑤個人的行動、⑥経済状態、⑦アルコール消費、⑧薬物への関与、⑨精神状況、⑩犯罪行為、⑪セキュリティ規則違反、⑫職務外の活動、⑬情報技術システムの利用状況
調査票の項目		①テロ・政府転覆活動等団体への参加・関与等の経験、②海外渡航歴、海外活動歴、過去7年間の訪問国、③氏名、生年月日、出生地、国籍、過去7年間の住所及び就労状況、現在・過去の配偶者、親族・知人、④職歴、軍歴、⑤逮捕歴、⑥財務記録、債務不履行、⑦アルコールの摂取を原因とする治療・カウンセリングの経験、⑧非合法な薬物使用等の経験、⑨精神衛生状態についての専門家等のカウンセリング・入院経験、⑩民事訴訟に関する公記録　等
方法・手続	対象職員の同意・調査票の提出	本人が調査票に必要事項を記載し、個人情報提供同意書・自己の精神状態について医療関係者への照会同意書とともに提出
	対象職員との面接	基本的に機密レベルの秘密を取り扱う場合に面接を実施
	第三者に対する照会	・国の機関（連邦捜査局・連邦人事局・国防総省等）の記録のチェック、地方の（法執行）機関・金融機関等への照会（法第435条等） ・〔機密レベル〕配偶者又は同棲者に対する国の機関の記録のチェック、職歴の確認（過去7年間の雇用者等への照会を含む。）、訴訟記録の確認、知人（米国居住者4名。過去7年間の知り合い）への照会、近隣の人々・過去の配偶者からの聴取　等
	通知	判定結果を本人に通知（否定・取消しの場合は、国家安全保障上の利益・他の法令が許す範囲で、包括的で詳細な理由を書面で通知）
有効期限		機密レベル：5年（極秘レベル：10年、秘レベル：15年）

（注）　機密レベルのクリアランスでは、他に、（行政機関によっては）ポリグラフの実施が追加して行われる。

イギリスにおけるセキュリティクリアランス制度

対外非公表　取扱注意

根拠		①人的セキュリティと国家安全クリアランスの方針に関する政府声明（2010年7月改訂） ②セキュリティポリシーの枠組み（注：内閣府の定める政府統一基準で各省に義務的履行を求めるもの） ③英国政府の人的セキュリティ管理：クリアランスを受ける者への助言及びガイダンス　等
クリアランスの区分		取り扱う秘密の性質に応じた3段階のクリアランス（機密、極秘及び対テロリスト調査）
適格性確認の対象者		機密性の高い職務に従事する公務員、情報機関のメンバー、軍人、警察官、契約事業者及び一部のNGO関係者 ※　大臣、国会議員、裁判官・陪審員は対象外。
	※　例外措置	危機において、生命に急迫した危険が迫っている場合は事前の確認がなされずに情報が伝達されることがありうる。
実施権者		各行政機関及び警察が適格性を判定
	※　調査の委託	国防調査庁・外務省調査ユニットに委託可能（警察は独自に調査を実施）
評価の観点		信用性、誠実、信頼性
調査事項		雇用記録、犯罪歴情報、情報機関の記録、財産上の不正常、周囲の環境、人となり、ライフスタイル等
調査票の項目		・対象職員の人定事項、過去3年間の雇用歴、国籍、犯罪歴、過去5年間の住所、過去1年間以上の海外居住歴、既婚歴、配偶者（前配偶者を含む。）・両親の人定事項、英国軍隊・政府における雇用歴、スパイ・テロ・議会制民主主義の転覆活動等への関与経験 ・〔機密レベル以上〕上記についての詳細事項、兄弟・義父母・養父母等（配偶者に係るものを含む。）、同居人、過去10年間の雇用主、過去10年間の本人をよく知る者（3人以上）、学歴、信用・財務情報（本人及び配偶者のもの。）、健康状態に関する自己申告、かかりつけの医師
方法・手続	対象職員の同意・調査票の提出	・調査票に本人が記入、署名して提出。右提出により同意したとみなされる。 ・機密レベルのクリアランスでは、別途、補充調査票及び財産に関する調査票の提出が求められる。
	対象職員との面接	機密レベルの場合は必ず実施。その他の場合は必要に応じ実施。
	第三者に対する照会	・関係行政機関、警察、MI5への照会（クリアランスのレベルにより、配偶者（前配偶者を含む。）両親、同居人のものを含む。） ・〔極秘レベル以上〕信用情報機関への照会 ・〔機密レベル〕医療機関、本人をよく知る者等への照会
	通知	判定結果を本人に通知（否定の場合は、可能なら理由を提示）
有効期限		機密の場合は7年（初回のみ5年）で、その他の場合は10年（ただし、契約事業者の一部は3～5年）

ドイツにおけるセキュリティクリアランス制度

対外非公表　取扱注意

根拠		セキュリティ審査法
クリアランスの区分		取り扱う秘密の区分（機密、極秘、秘）に応じた3段階のクリアランス
適格性確認の対象者		セキュリティ上影響を及ぼす業務に任ぜられる予定の者（非公的機関を含む。） ※　連邦の憲法機関（大統領、議会、憲法裁判所）の構成員、裁判官等は対象外
	※　例外措置	特別な場合には、以下の①又は②の審査の結果、セキュリティ上のリスクの根拠が見出されなければ、セキュリティ審査の終了前にセキュリティ上影響を及ぼす活動の委託を許可 ①秘レベルの審査：適格性を判定する各行政機関が保有する独自の情報を考慮して調査票の記載事項について判断 ②極秘及び機密レベルのセキュリティ審査：それぞれ一段階低いレベルの審査の措置を終了していること
実施権者		各行政機関が適格性を判定（非公的機関については、右に対し機密等を交付しようとする連邦の各行政機関）
	※　調査の委託	連邦憲法擁護庁、軍防諜局に委託（連邦情報庁、連邦憲法擁護庁、軍防諜局は独自で実施）
評価の観点		①当事者の信用への疑念、②外国の情報機関からの特に恐喝される危険、③自由と民主的な基本秩序への支持に疑念がある場合、保安リスクが存在
調査票（保安宣誓書）の項目		①外国・旧東独の情報機関との関係、反憲法組織との関係、②18歳以降の外国における住所歴、パスポート番号、内務省がセキュリティ上懸念する国家における滞在歴・旅行歴・近親者等、③氏名、生年月日・出生地、国籍、過去5年間の国内における住所歴、身分証明書番号、④家族構成、家族の人定事項、⑤職歴、雇用主、学歴・軍歴等、係属中の懲戒手続、⑥係属中の刑事手続、⑦過去5年間の強制執行措置・現在の経済状態、⑧対象職員の身元確認のための情報提供者2人（極秘レベル以上）、対象職員に関する質問のための照会者3人（機密レベル）⑨過去のセキュリティ審査に関する情報〔法第13条に列挙されている〕
方法・手続	対象職員の同意・調査票の提出	・書面による同意 ・セキュリティ宣言書を本人から実施機関に送付 ・機密及び極秘レベルでは、配偶者又はパートナーに対しても、対象者本人の同意の下セキュリティ審査が実施される。
	対象職員との面接	（面接の実施については明記されていない）
	第三者に対する照会	・連邦中央登録局からの情報の入手、連邦刑事庁・連邦警察庁・連邦の情報機関への照会 ・所在地の警察機関への照会、配偶者又はパートナーへのセキュリティ審査（極秘レベル以上） ・調査票に記載した参考人あるいはそれ以外の情報提供者への質問（機密レベル）〔法第12条〕
	通知	判定結果を本人に通知（理由が付されるかどうかについては法には言及なし）
有効期限		機密レベルの場合は、10年ごとに再検査を行う

フランスにおけるセキュリティクリアランス制度

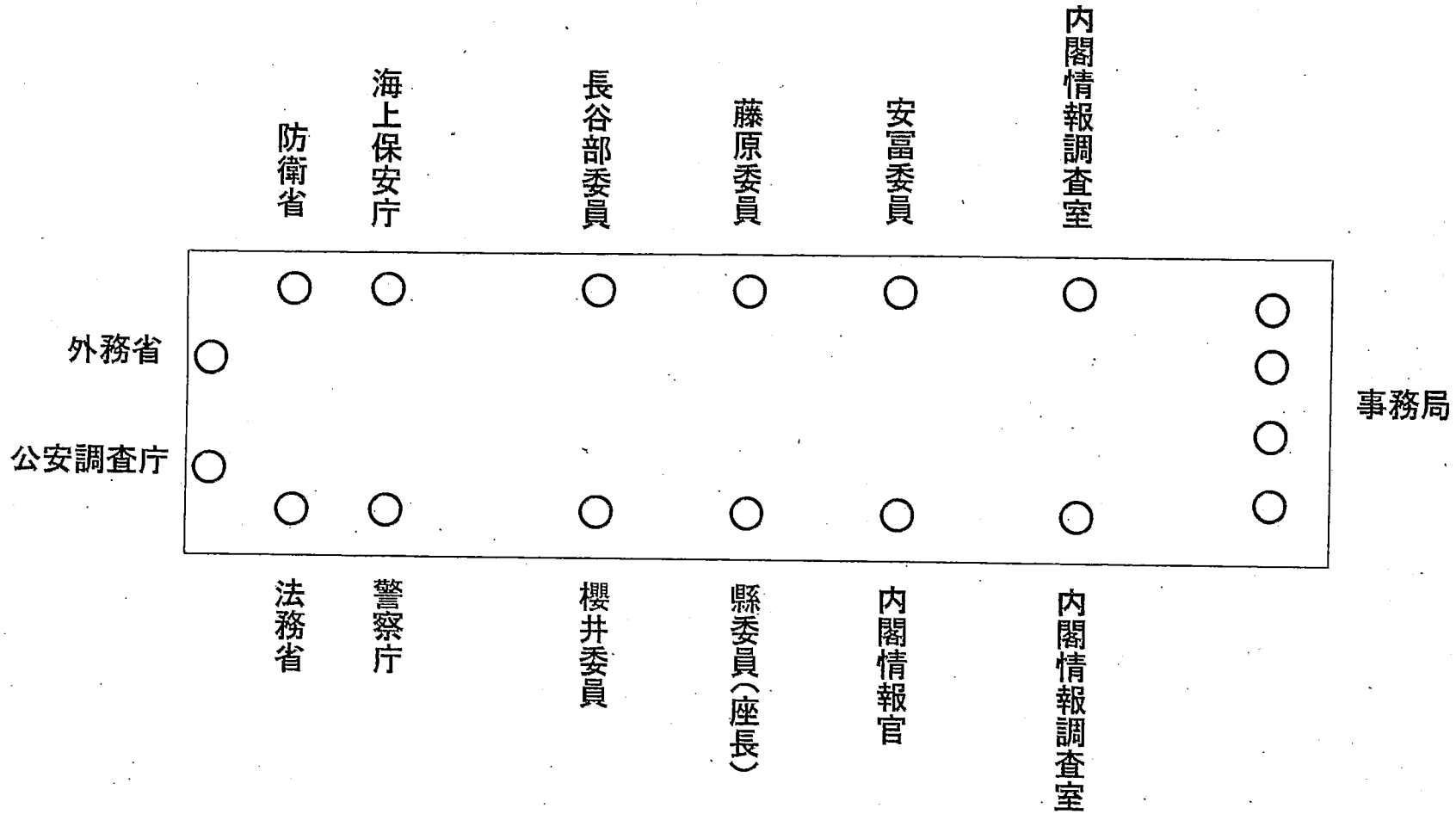
対外非公表　取扱注意

根拠		国防法典、国防秘密保全に関する政府間通達等
クリアランスの区分		取り扱う秘密の区分（機密、極秘、秘）に応じた3段階のクリアランス
適格性確認の対象者		秘密区分指定された情報・媒体を知る必要のある者（国の行政機関のほか、重要インフラ事業者である地方公共団体その他公共セクター、契約事業者等を含む。） ※　大統領、首相、大臣、議会の情報委員会を構成する議員は対象外（注：裁判官については不明）
	※　例外措置	・緊急の場合には15日以内に可否が決定される仮の適格性確認で6か月以内の取扱いが可能。対象者は、①政府高官・外交官・将官、②予期しない任務のため派遣された者、③通常の期間の遵守では不可能な条件で配属された高位の責任者が対象で、対象人数は著しく限定される。 ・秘レベルについて、公務員、民間の契約社員等は内務省・国防省への調査の委託なしに所属当局により適格性確認を得ることができる。
実施権者		機密レベルは首相府国防事務総長（首相名）、極秘・秘レベルは当該秘密を主管する行政機関の主管高等防衛官（大臣名）が適格性を判定
	※　調査の委託	文民（警察勤務者を含む。）等については内務省中央国内情報局へ委託、国防省に勤務する文民・軍人、国家憲兵隊員、国防省のために業務を行う組織・企業に係る調査は国防安全防護局が実施。
評価の観点		・本人自身が秘密漏えいに対する危険性を有していないか。 ・国益を危険にされるような脅し又は圧力（例えば、外国情報機関、テロリストグループ、反体制的活動に従事する個人又は組織からのもの）にさらされていないか。
調査票の項目		①過去5年の海外滞在歴、パスポート番号、②氏名、生年月日・出生地、国籍、過去6年間の住所歴、一時的な居所・セカンドハウスの住所、家族構成、身分証明書番号、家族の人定事項
方法・手続	対象職員の同意・調査票の提出	調査票の項目に本人が記入して提出。右調査票の提出をもって、調査開始への同意となる。
	対象職員との面接	（面接の実施については明記されていない）
	第三者に対する照会	[redacted]
	通知	判定結果を本人に面前で通知（否定する場合に秘区分に付される情報に関するものである場合、理由は不要）
有効期限		在任期間に限り有効であるが、機密レベルの場合は最長3年、極秘レベルの場合は最長5年、秘レベルの場合は最長10年

第4回秘密保全のための法制の在り方に関する有識者会議　座席表

平成23年4月22日（金）午前10時～正午　於：内閣府本府5階特別会議室

（出入口）



配付資料

資料１　罰則等に関する考え方（事務局案）・論点

資料２　我が国の秘密保全に関する現行法制の罰則

資料３　諸外国の秘密保全に関する法制における罰則

機密性2情報

対外非公表　取扱注意　配付資料１

秘密保全のための法制の在り方に関する有識者会議（第４回）

罰則等に関する
考え方（事務局案）・論点

平成２３年４月２２日

第4　罰則等

事　務　局　案

罰則に関する基本的な考え方

刑罰の必要性

特別秘密の漏えいを防止するためには、厳格な人的管理及び物的管理を行うのみならず、漏えい行為など本来特別秘密を知る立場にない者が特別秘密を知ることにつながる行為については刑罰をもって臨むことが必要

処罰対象の範囲

- ◆ 特別秘密の漏えいを防ぐには、その保全状態を保護することが効果的
- ◆ 処罰の範囲を必要最小限に抑えることが、本法制に対する国民の理解を得る上で重要

⇒ 特別秘密を現に保全している者、すなわち業務によりこれを取り扱う者による漏えいを処罰し、**特別秘密の漏えいを根元から抑止**することを基本的な考え方とする

法定刑

本来特別秘密を知る立場にない者が特別秘密を知ることにつながる行為を抑止するとともに、特別秘密の漏えい等という重い罪責に応じた処罰を可能にするような刑を定める

論　点

○　罰則に関する基本的な考え方の当否

第4　罰則等　（禁止行為）

事　務　局　案

故意の漏えい行為

業務により特別秘密を取り扱う者

自己の業務上の権限や地位に基づき特別秘密を知る者で、その業務性に応じた高度の保全義務を負う

→ 処罰

- **取扱業務者**（秘密の作成・取得の趣旨に従い秘密を取り扱うことを業務とする者）
- **業務知得者**（秘密の作成・取得の趣旨に照らし、その取扱いが本来は想定されていない行政機関等において、その事務の遂行上の必要性から秘密の伝達を受けこれを知得する者）

※ MDA秘密保護法では、取扱業務者による漏えい行為を業務知得者による漏えい行為よりも重く処罰
※ 自衛隊法では、取扱業務者による漏えい行為のみを処罰し、業務知得者による漏えい行為は処罰対象とせず

→ 処罰の程度につき要検討

※ 記者が取扱業務者に取材をして特別秘密の伝達を受けた場合、記者は自己の業務として取材をしているが、秘密の伝達は記者の業務上の権限や地位に基づくものではないから、業務知得者には該当しない

業務外知得者

（取扱業務者又は業務知得者以外の者）

- 特別秘密をより広範囲に拡散
- 業務として特別秘密を取り扱う者ではないため、業務外知得者への伝達の時点で特別秘密は既に保全状態から流出しており、処罰しても漏えいの根元からの抑止にはつながらない
- 例えば特別秘密文書をたまたま拾った一般人まで処罰対象になり得るなど処罰対象が広がる
- 正当な報道活動も構成要件に該当し得るため報道活動への影響も懸念される

→ 処罰しない

前段階にある、業務により特別秘密を取り扱う者による漏えい行為等の処罰を徹底

※ 業務外知得者が、我が国の安全を害する目的等の不当な目的をもって特別秘密を漏えいした場合等を処罰すべきか
→ 上記と同様、処罰しても根元からの抑止につながらず、一般人が処罰対象となり処罰範囲が広範。加えて、不当な目的での漏えい行為の場合、同目的の有無は必ずしも客観的に明らかではないため、報道機関への影響も懸念される

論　点

○ 故意の漏えい行為の処罰対象者の範囲の是非

第4　罰則等　（禁止行為）

事　務　局　案

過失による漏えい

特別秘密の性格に照らせば、過失による漏えいであっても国益や国民の安全の確保に大きな影響を及ぼすことには変わりがない

業務により特別秘密を取り扱う者

その業務に応じ、特別秘密を厳格に保全し漏えいを防ぐ責任を有している
→ 漏えいを防ぐ注意義務

⇒ 処罰

業務知得者

※ MDA秘密保護法では、取扱業務者の過失による漏えい行為を業務知得者の過失による漏えい行為よりも重く処罰

※ 自衛隊法では、取扱業務者の過失による漏えい行為のみを処罰し、業務知得者の過失による漏えい行為は処罰対象とせず

- 高度の注意義務を認めるべき基礎が十分ではない
- 過失犯を厳格に処罰すれば、業務の遂行それ自体よりも特別秘密の管理に業務の重点が移行し、その結果当該業務の遂行に支障を来たすおそれもあり得る

⇒ 処罰の程度につき要検討

論　点

○ 過失犯の処罰範囲の是非

第4　罰則等　（禁止行為）

事　務　局　案

特別秘密を取得（探知）する行為

※ 下記①②に該当する行為を便宜的に「特定取得行為」という

特別秘密の保全状態からの流出には、
漏えい行為の処罰では抑止できない、
取得行為を原因とする場合がある

① 窃盗、不正アクセス又は特別秘密の管理場所への侵入など、管理権を侵害する行為を手段として特別秘密を直接取得する場合

▼

取扱業務者等による漏えい行為が介在しないため、漏えい行為の処罰ではこれを抑止できない

② 欺罔により適法な伝達と誤信させ、あるいは暴行・脅迫によりその反抗を抑圧して、取扱業務者等から特別秘密を取得する場合

▼

取扱業務者等に漏えいの故意がないなど、漏えい行為の処罰が困難

特定取得行為を処罰することについては慎重な検討が必要

▼

特定取得行為は、犯罪行為や、犯罪に至らないまでも社会通念上是認できない行為を手段とするもので、適法な行為との区別は明確

▼

特定取得行為を処罰対象に加えても、正当な取材活動など本来許容されるべき行為が捜査や処罰の対象とされるおそれはない

特定取得行為は、特別秘密を保全状態から流出させる点で取扱業務者等による漏えい行為と同様の悪質性、危険性

▼

その行為が取扱業務者等によるものではないということのみをもって処罰対象から外されるとすれば、特別秘密の保全を目的とする本法制の趣旨を損ねる

▼

処罰範囲を必要最小限に抑えるという基本的な考え方の下でも、特定取得行為を処罰対象とすることはやむを得ない

※ 特定取得行為の中には、他の犯罪が成立する行為もあるが、同行為は取扱業務者等による漏えい行為と同様の悪質性、危険性があるから、特定取得行為として正面から処罰対象とすべき

論　点

○ 特定取得行為を処罰対象とすること及びその範囲の是非

第4　罰則等　（禁止行為）

対外非公表　取扱注意

事　務　局　案

未遂行為

故意の漏えい行為
特別秘密の漏えいの危険を現実化させる悪質性の高い行為

特定取得行為
漏えい行為と同様に秘密を漏えいさせる高い危険性

共謀行為

故意の漏えい行為
- 漏えい行為について共謀者間で具体性、特定性、現実性を持った合意
- 共謀者の一人の意思の変化では犯罪行為の遂行を容易に変更できない

→ 単独犯における犯行の決意に比べて犯罪実現の危険性が飛躍的に高まる

特定取得行為
漏えい行為と同様に秘密を漏えいさせる高い危険性

立法例を考慮
自衛隊法は、防衛秘密の漏えいの共謀を処罰

独立教唆行為及び煽動行為

取扱業務者等に対し、特別秘密を漏えいするよう働きかける行為
特別秘密の漏えいの危険を著しく高める行為であって悪質性が高い

特定取得行為
漏えい行為と同様に秘密を漏えいさせる高い危険性

立法例を考慮
自衛隊法は、防衛秘密の漏えいの独立教唆及び煽動を処罰

→ 処罰

自首減免規定

自首した者に対する必要的な刑の減軽又は免除を規定

- 現実の漏えいに至る前に自首することを促す
- ひいては実害の発生を未然に防ぐことを期待できる

立法例を考慮： 自衛隊法は、防衛秘密の漏えいの未遂及び共謀について、自首による刑の必要的減免を規定

漏えい行為及び特定取得行為の未遂及び共謀について、自首による刑の必要的減免

国外犯処罰規定

- 日本国外において日本国民のみならず日本国民以外の者によっても敢行され得る
- 漏えい行為等は我が国の重大な利益を害する

行為者の国籍を問わず我が国において処罰（刑法2条の例により、日本国外において罪を犯した全ての者を処罰）

論　点

○　これらの規定を設けることの是非

第4 罰則等 （法定刑）

事 務 局 案

法定刑

- ◆ 漏えい行為等に対する十分な抑止力
- ◆ 漏えい行為等を敢行した者に対してその罪責に応じた十分な刑罰を科す

⇒ 法定刑の上限を相当程度高くする必要

最も重い刑をもって臨むべき、業務により特別秘密を取り扱う者による故意の漏えい行為及び特定取得行為の法定刑を検討

自由刑

- ➢ これまでの検討内容に照らすと、防衛秘密に相当する事項は特別秘密に該当
- ➢ 防衛秘密の漏えい行為に対する最高刑は懲役5年

⇒ 本法制の最高刑も懲役5年が適当

- ➢ 立法例 （最高刑が懲役10年）
  - 刑事特別法、MDA秘密保護法
  - 不正競争防止法の営業秘密の開示行為等
- ➢ 特定取得行為においては窃盗罪（最高刑は懲役10年）なども手段となり得る

⇒ 最高刑を懲役10年とすることも考えられる

特に現行の防衛秘密制度との整合性が問題となることから、その必要性や相当性について更なる検討が必要

罰金刑

- ➢ 漏えい行為等の刑事責任は重く、罰金刑のみを科すことは適当でない
- ➢ これまでに敢行された秘密漏えい事案においては、金銭的対価を伴うものが少なくない

⇒ 抑止効果の観点

相当程度の罰金刑の併科

- ➢ 金銭的対価を伴わない事案や少額に過ぎない事案もある
- ➢ 漏えい等に対する報酬であれば没収・追徴も可能

自由刑と罰金刑は任意的併科

論 点

○ 法定刑の是非

第4　罰則等　（司法手続）

事　務　局　案

司法手続

漏えい等の事件において、対象となる秘密が実質秘であることが公判廷において争われた場合に、当該秘密を証拠提出してこれを公開したのでは秘密保全の趣旨に反することから、このような事態を回避しつつ必要な立証を行う必要

外形立証

秘密漏えい事件の裁判における実務

確立された立証方法として、いわゆる外形立証により、秘密そのものを公判に提出せずにその実質秘性を立証しており、秘密を守りつつ公判での立証を支障なく行うことができている

本法制については、保護すべき秘密の要件として、具体的かつ明確に列挙された事項のいずれかに該当するものであること、明示的な指定行為を要すること等を定めることを前提

外形立証は十分有効に行い得る

外形立証による実質秘性の立証

秘密漏えい事件において、争点となっている秘密が実質秘であることを立証するに当たり、
① 秘密の指定基準（指定権者、指定される秘密の範囲、指定及び解除の手続）が定められていること、
② 当該秘密が国家機関内部の適正な運用基準に則って指定されていること、
③ 当該秘密の種類、性質、秘扱いをする由縁等を立証することにより、当該秘密が実質秘であることを推認するもの

公判廷において特別秘密に該当する事項を秘匿し、別の呼称に言い換えるなどの特別の措置を採用することについて

特別秘密の漏えい等事件の公判については、外形立証による裁判遂行が可能であるとすれば、新たな手続を設ける必要性は低い

論　点

○　上記結論の是非

諸外国の秘密保全に関する法制における罰則

諸外国の秘密保全に関する法制における罰則（米国）

米国に損害を与える意図を有する者による国防情報の取得等	
秘密の内容	○　艦船、航空機、防衛施設、海軍工廠、海軍基地、潜水艦基地、燃料補給所、要塞、砲台、魚雷施設、船渠、運河、鉄道、兵器庫、野営地、工場、鉱業場、電信局、電話局、無線局、信号所、建築物、事務所、研究所、調査基地又はその他の国防に関連する場所であって、米国政府が所有し、建設し、若しくは建設中であるもの、米国、その職員、部局若しくは政府機関の管理下に置かれるもの、又は米国の排他的管轄権が及ぶものに関する情報 ○　米国、その部局、政府機関又は米国を代表する者等との契約又は合意の下で、艦船、航空機、兵器、軍需品又は戦時において用いられる物資若しくは機器が、製造、準備、修理、保管若しくは研究開発される場所に関する情報 ○　陸海空軍の用に供するものを準備、建造又は保管している場所で、戦時又は緊急時における大統領の宣言によって指定される禁止区域に関する情報（当該情報が国防に悪影響を及ぼし得る場合）
漏えい	
取得（探知）	国防に関する情報の取得を目的とし、かつ、上記の情報が利用されることで米国に損害を与え、若しくは外国を利する意図を有し、又はそうであろうと信じるに足る理由を有する者による、上記場所への接近、立入り若しくは上空の飛行、又はその他の方法による上記の情報の取得 【10年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第793条(a)

米国に損害を与える意図を有する者による国防情報の取得等	
秘密の内容	国防に関するあらゆるもののスケッチ、写真、ネガ、青写真、図面、地図、模型、装置、機器、文書、書面又は記録
漏えい	
取得（探知）	国防に関する情報の取得を目的とし、かつ、上記の情報が利用されることで米国に損害を与え、若しくは外国を利する意図を有し、又はそうであろうと信じるに足る理由を有する者による、複写、作成、製作若しくは取得又はそれらの未遂 【10年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第793条（b）

諸外国の秘密保全に関する法制における罰則（米国）

違法に取得された国防情報の受領・取得等	
秘密の内容	国防に関するあらゆるものの文書、書面、コードブック、暗号表、スケッチ、写真、ネガ、青写真、図面、地図、模型、装置、機器又は記録
漏えい	
取得（探知）	国防に関する情報の取得を目的とし、かつ、受領若しくは取得、又はこれらの合意若しくは開始の時点で、上記の情報が合衆国法典第18編第37章の条項に反する形で、取得、作成、製作若しくは取り扱われ、又はそれらがなされることとなることを認識し、又はそうであろうと信じるに足る理由を有する者による、あらゆる相手からの受領若しくは取得又はこれらの合意若しくは未遂 【10年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第793条（c）

国防情報の漏えい等	
秘密の内容	① 国防に関する、あらゆる文書、書面、コードブック、暗号表、スケッチ、写真、ネガ、青写真、図面、地図、模型、装置、機器又は記録 ② 国防に関する情報であって、米国に損害を与え、又は外国を利するように使用され得るものであると所持者が考えるに足る理由があるもの
漏えい	a) 適法に所持し、アクセスし、管理し、又は委託された者による、無権限者への故意の伝達、引渡し若しくは伝送若しくはこれらの行為がなされるようにすること又はこれらの未遂 b) 権限なく所持・アクセス・管理している者による、無権限者への故意の伝達、引渡し若しくは伝送若しくはこれらの行為がなされるようにすること又はこれらの未遂 【10年以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
その他	a) 適法に所持し、アクセスし、管理し、又は委託された者による、故意に所持し続け、権限ある公務員又は被用者の求めにもかかわらず、引き渡さないこと b) 権限なく所持・アクセス・管理している者による、故意に所持し続け、権限ある公務員又は被用者へ引き渡さないこと 【10年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第793条（d）（e）

諸外国の秘密保全に関する法制における罰則（米国）

重過失による国防情報の漏えい等	
秘密の内容	国防に関するあらゆる文書、書面、コードブック、暗号表、スケッチ、写真、ネガ、青写真、図面、地図、模型、装置、機器、記録又は情報
漏えい	
過失犯	委託され、又は適法に所持し、若しくは管理している者が、 重過失によって、 委託に反する適切な保管場所からの移動若しくは引渡し 又は紛失、窃取、取出し若しくは破棄 を可能にした場合 【10年以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
その他	委託され、又は適法に所持し、若しくは管理している者が、 委託に反する適切な保管場所からの移動若しくは引渡し、又は紛失、窃取、取出し若しくは破棄が、不法になされたことを認識しながら、これらの事実の上司への早急な報告を怠った場合 【10年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第793条（ｆ）

国防情報の取得・漏えい等の共謀	
秘密の内容	
漏えい	
取得（探知）	
その他	二以上の者が、第793条(a)～(f)に規定する違反行為を共謀し、かつ、一以上の者が、その目的を達成するために何らかの行為を行った場合 【共謀の目的である犯罪に対応する刑】
根拠	合衆国法典第18編第37章第793条(g)

諸外国の秘密保全に関する法制における罰則（米国）

外国政府への国防情報の漏えい等	
秘密の内容	国防に関するあらゆる文書、書面、コードブック、暗号表、スケッチ、写真、ネガ、青写真、図面、地図、模型、記録、装置、機器又は情報
漏えい	上記の情報が利用されることで米国に損害を与え、若しくは外国を利する意図を有し、又はそうであろうと信じるに足る理由を有する者による、外国政府、米国による承認の有無にかかわらず外国に存する党派、政党、陸・海軍、又はそれらの代表者、公務員、代理人、被雇用者、国民若しくは市民に対しての、直接又は間接の伝達、引渡し、伝送又はこれらの未遂 【死刑、無期刑又は有期刑（上限なし）】 陪審又は陪審が設置されていない場合は裁判所が、次のいずれかに該当すると認めない場合には、死刑は科されない。 ① 当該犯罪行為の結果、外国勢力により米国の諜報員として活動している個人が特定され、そのため当該個人の命が奪われた場合、又は ② 当該犯罪行為が、核兵器、軍用宇宙船・衛星、早期警戒システム等の大規模攻撃に対する防衛若しくは報復手段、戦争計画、通信傍受による情報収集、暗号情報又はその他の主要兵器システム若しくは防衛戦略の主要要素に直接関わる場合
取得（探知）	
根拠	合衆国法典第18編第37章第794条（a）

戦時における、敵への伝達を意図した国防情報の漏えい等	
秘密の内容	① 米国の軍隊、艦船、航空機又は軍需物資の移動、数量、種類、状態又は配置に関する情報 ② 陸海軍の作戦に係る計画又は対処方針に関する情報 ③ ある場所の要塞化若しくは防御のためになされ、若しくはそれらに関連してなされ、若しくはそれらを意図してなされた、あらゆる工事又は措置、又は国民の防御に関するその他の情報 であって、敵側の役に立ち得る情報
漏えい	戦時における、敵に伝達されることを意図しての、公表若しくは伝達又は顕在化の試み 【死刑、無期刑又は有期刑（上限なし）】
取得（探知）	戦時における、敵に伝達されることを意図しての、収集又は記録 【死刑又は無期刑又は有期刑（上限なし）】
根拠	合衆国法典第18編第37章第794条（b）

諸外国の秘密保全に関する法制における罰則（米国）

外国政府への国防情報の漏えい等の共謀	
秘密の内容	
漏えい	
取得（探知）	
その他	二以上の者が、第794条の規定の違反行為を共謀し、かつ、一以上の者が、その目的を達成するために何らかの行為を行った場合 【共謀の目的である犯罪に対応する刑】
根拠	合衆国法典第18編第37章第794条(c)

国防上の重要施設の写真等の作成	
秘密の内容	国防上の利益のため、大統領が、関連する情報が一般的に公開されることのないように保護を要すると指定した、極めて重要な軍事施設又は設備
漏えい	
取得（探知）	司令官等の許可を得ず、かつそれらの者による検閲又は必要なその他の措置をとらずに行った、写真、スケッチ、画像、描画、地図又は図形による説明の作成 【１年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第795条

国防上の重要施設の写真等の作成目的での航空機使用等	
秘密の内容	国防上の利益のため、大統領が、関連する情報が一般的に公開されることのないように保護を要すると指定した、極めて重要な軍事施設又は設備
漏えい	
取得（探知）	第７９５条に違反する形で、写真、スケッチ、画像、描画、地図又は図表による説明を作成する目的での、航空機又は飛行装置の使用又は使用許可 【１年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第796条

諸外国の秘密保全に関する法制における罰則（米国）

国防上の重要施設の写真等の漏えい等	
秘密の内容	国防上の利益のため、大統領が、関連する情報が一般的に公開されることのないように保護を要すると指定した、極めて重要な軍事施設又は設備
漏えい	大統領による上記指定を受けてから30日経過以後における、司令官等の許可を得ない、上記事項に係る、写真、スケッチ、画像、描画、地図又は図形による説明の公表、販売、又は譲渡。ただし、適切な軍当局の検閲済表示がなされているものについてはこの限りではない。 【１年以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
その他	大統領による上記指定を受けてから30日後以降における、司令官等の許可を得ない、上記事項に係る、写真、スケッチ、画像、図面、地図又は図形による説明の複製。ただし、適切な軍当局の検閲済表示がなされているものについてはこの限りではない。 【１年以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第37章第797条

米国・外国政府の暗号の漏えい等	
秘密の内容	（１）　米国又は外国政府のコード、暗号又は暗号システムに関する、性質、作成又は利用に関する秘密 （２）　米国又は外国政府によって利用され、作成され、又は利用が予定されている暗号目的又は通信傍受目的の装置、器具又は機器の設計、構造、利用、保守又は修理に関する秘密 （３）　米国又は外国政府による通信傍受活動に関する秘密 （４）　外国政府の通信の中から通信傍受により得られた秘密であって、当該秘密が通信傍受によって得られたものであることを認識しているもの （「秘密」とは、違反行為の時点で、米国政府機関が、国家安全保障を理由に、その公開・配布を制限又は禁止するよう特に指定した情報をいう。）
漏えい	無権限者への伝達、供給、伝送若しくはこれら以外のあらゆる方法を用いての提供、若しくは公表、又は米国の安全と利益を損い、若しくは米国に害をもたらし外国政府を利する目的でのあらゆる態様での利用 【10年以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	合衆国法典第18編第37章第798条(a), (b)

諸外国の秘密保全に関する法制における罰則（米国）

不正アクセスにより国防・外交上の重要情報を取得した者による漏えい等	
秘密の内容	①　国防上又は外交関係上の理由から無許可による開示から保護すべきものとして大統領命令又は制定法に従い米国政府によって指定された情報 ②　1954年原子力エネルギー法第11条第ｙ項に規定する「制限データ」 （②の「制限データ」とは、核兵器の設計・製造・使用、特別な核物質の生産又はエネルギー生産における特別な核物質の利用に関するあらゆるデータのうち、原子力委員会によって秘密指定が解除されていないものをいう。）
漏えい	上記の情報が利用されることで米国に損害を与え、若しくは外国を利することがあり得ると信じるに足る理由を有し、かつ、無権限又は権限を逸脱していることを認識しながらコンピューターにアクセスして上記情報を取得した者による、受理する権限のない者に対する、意図的な伝達、引渡し若しくは伝送、これらがされるようにすること又はこれらの未遂 【10年（再犯の場合は20年）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
その他	上記の情報が利用されることで米国に損害を与え、若しくは外国を利することがあり得ると信じるに足る理由を有し、かつ、無権限又は権限を逸脱していることを認識しながらコンピューターにアクセスして上記情報を取得した者が、意図的にそれを保持しそれを受領する権限のある政府職員に対して引き渡さないこと 【10年（再犯の場合は20年）以下の自由刑若しくは罰金又はこれらの併科】
根拠	合衆国法典第18編第４７章第1030条(a)(1)

秘密情報の無許可での持ち出し	
秘密の内容	○職務、地位又は契約により所持するに至った米国の秘密情報を含む文書又は資料 （「米国の秘密情報」とは、政府によって作成され、所有され、又は保持されている防衛又は外交に関する情報であって、国家安全保障上の観点から、無許可での開示から保護すべきものとして、法律又は大統領命令に基づき指定されたものをいう。）
漏えい	職務、地位又は契約により、上記文書又は資料を所持する者による、許可されない場所に保管する目的での、故意の無許可での持ち出し（議会への提供のために行うものを除く） 【１年以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	合衆国法典第18編第93章第1924条（a）～（ｃ）

諸外国の秘密保全に関する法制における罰則（米国）

原子力委員会により秘密指定されたデータの米国に損害を与える目的での漏えい等	
秘密の内容	制限データに関し、又はそれを含む文書、書面、スケッチ、写真、図面、模型、装置、機器、記録又は情報 （「制限データ」とは、核兵器の設計・製造・使用、特別な核物質の生産又はエネルギー生産における特別な核物質の利用に関するあらゆるデータのうち、原子力委員会によって秘密指定が解除されていないものをいう。）
漏えい	・合法又は違法に、所持、アクセス、管理又は受託する者による、米国に損害を与え、又は外国を利する目的での、伝達、伝送若しくは開示又はこれらの未遂若しくは共謀 【無期刑、有期刑（上限なし）若しくは罰金又はこれらの併科】 ・合法又は違法に、所持、アクセス、管理又は受託する者による、当該制限データが米国に損害を与え、又は外国を利するために使用されると信じるに足る理由を有しての、伝送、伝達若しくは開示又はこれらの未遂若しくは共謀 【10年以下の自由刑もしくは罰金又はこれらの併科】
取得（探知）	
根拠	合衆国法典第42編第23章第2274条(a)(b)

秘密エージェントを特定する情報の漏えい	
秘密の内容	・　秘密エージェントを特定する秘密情報にアクセスする権限があり、又はあった者による、上記情報が秘密エージェントを特定すること及び当該秘密エージェントと米国とのインテリジェンスに係る関係を秘匿するために米国が積極的措置を講じていることを知った上での、無権限者への上記情報の故意の開示 【10年以下の自由刑もしくは罰金又はこれらの併科】 ・　秘密情報にアクセスする権限がある結果として秘密エージェントの身元を把握した者による、上記情報が秘密エージェントを特定すること及び当該秘密エージェントと米国とのインテリジェンスに係る関係を秘匿するために米国が積極的措置を講じていることを知った上での、無権限者への上記情報の故意の開示 【５年以下の自由刑もしくは罰金又はこれらの併科】 ・　秘密エージェントを特定し暴露しようとする一連の活動が行われている過程における、当該活動が米国の対外情報活動を害し、妨げると信じる理由がある者による、当該情報がある個人を特定すること及び当該個人と米国とのインテリジェンスに係る秘密の関係を秘匿するために米国が積極的措置を講じていることを知った上での、無権限者への上記情報の故意の開示 【３年以下の自由刑もしくは罰金又はこれらの併科】
漏えい	
取得（探知）	
根拠	合衆国法典第50編第15章第421条(a)～(c)

諸外国の秘密保全に関する法制における罰則（米国）

安全保障に関する秘密情報の外国政府への漏えい・外国政府による取得等	
秘密の内容	米国の安全保障に影響を与えるものとして、大統領又は大統領の承認を得た行政機関若しくは企業の長によって秘密指定された情報
漏えい	政府若しくは行政機関の職員若しくは被雇用者、又は政府若しくは行政機関がすべて若しくは過半数の株式を所有している企業の職員若しくは被雇用者による、外国政府の代理人又は代表者であることを当該職員又は被雇用者が知り、又はそう信ずべき理由のある者に対する、上記情報が秘密指定されていることを知り、又は知るべき理由がある場合での、何らかの手段又は方法による伝達。ただし、当該情報を開示するにつき、大統領又は当該職員若しくは被用者を雇用している行政機関若しくは企業の長が、特別に授権している場合を除く。 【10年以下の自由刑若しくは罰金又はこれらの併科及び合衆国憲法又は法律に基づく名誉、報酬又は信任を伴う官職又は地位に就く資格の剥奪】
取得（探知）	外国政府の代理人又は代表者による、政府若しくは行政機関の職員若しくは被用者、又は政府若しくは行政機関がすべて若しくは過半数の株式を所有している企業の職員若しくは被用者からの、直接又は間接の、上記情報の取得若しくは受領又はこれらの試み。ただし、上記情報を保管し、又は管理する行政機関又は企業の長が、事前に、当該伝達を特別に認めている場合を除く。 【10年以下の自由刑若しくは罰金又はこれらの併科及び合衆国憲法又は法律に基づく名誉、報酬又は信任を伴う官職又は地位に就く資格の剥奪】
根拠	合衆国法典第50編第23章第783条(a)～(c)

公式外交コードの漏えい等	
秘密の内容	①公式外交コード又は当該コードを用いて用意され、若しくは用意されたものとされる事項 ②外国政府とその駐米公館の間の通信の過程で得られた事項
漏えい	政府の被雇用者の立場に基づき、公式外交コード又は当該コードを用いて用意され、若しくは用意されたものとされる事項を、取得し、又は保管若しくはアクセスでき、若しくはできた者による、故意の公表又は他者への提供 【10年以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	合衆国法典第18編第45章第952条

諸外国の秘密保全に関する法制における罰則（英国）

国の治安・利益を損なう目的による、禁止区域への接近等	
秘密の内容	禁止区域 ① 国が所有し、占有し、又は国のために占有する、防衛施設、兵器庫、海軍若しくは空軍の基地若しくは施設、工場、船渠、鉱業場、地雷敷設地、野営地、艦船若しくは航空機、又は、電信局、電話局、無線局、信号所若しくは事務所、及び、国が所有し、占有し、又は国のために占有する場所であって、軍需品若しくはそれに関連するスケッチ、図面、模型若しくは文書の製作、修理若しくは保管のためのもの、又は戦時に使用する金属、石油若しくは鉱物を採取するためのもの ② 国が所有しないが、軍需品又はこれらに関連するスケッチ、模型、図面若しくは文書が、国若しくは国のために行為する者との契約に基づき又は国の利益のために、製作、修理、取得、又は保管されている場所 ③ 国が所有し又は国のために使用される場所であって、当該場所に関する情報又は当該場所への損害が敵を利するとして、国務大臣の命令により当面禁止区域とするとして公表された場所 ④ 線路、道路、水路その他の水陸の移動手段（これらの一部又はこれらと接続されている建造物若しくは構造物を含む）、ガス、水道、電力施設その他の公共施設のために使用される場所、又は軍需品若しくはこれに関連するスケッチ、模型、図面若しくは文書が国のためではなく製作、修理若しくは保管されている場所であって、その情報が重要なものであり、又は当該場所等を破壊、妨害若しくは干渉された場合には敵を利するとして、国務大臣の命令により当面禁止区域とするとして公表された場所
漏えい	
取得（探知）	国の治安又は利益を損なう目的による、接近、視察、立ち寄り、侵入又は付近での滞在 【３年以上14年以下の自由刑】
根拠	１９１１年公務秘密法第１条、３条 １９２０年公務秘密法第８条

国の治安・利益を損なう目的による、敵に有用なスケッチ等の作成	
秘密の内容	直接又は間接に敵に有用となり、有用となり得、又は有用となることを意図したスケッチ、図面、模型又は記録
漏えい	
取得（探知）	国の治安又は利益を損なう目的による、上記スケッチ等の作成 【３年以上14年以下の自由刑】
根拠	１９１１年公務秘密法第１条 １９２０年公務秘密法第８条

諸外国の秘密保全に関する法制における罰則（英国）

国の治安・利益を損なう目的による、敵に有用な情報の漏えい・取得等	
秘密の内容	直接又は間接に敵に有用となり、有用となり得、又は有用となることを意図した、機密信号、暗号、スケッチ、図面、模型、記事、記録又はその他の文書若しくは情報
漏えい	国の治安又は利益を損なう目的による、上記情報等の第三者への伝達又は公表 【３年以上14年以下の自由刑】
取得（探知）	国の治安又は利益を損なう目的による、上記情報等の取得、収集又は記録 【３年以上14年以下の自由刑】
根拠	１９１１年公務秘密法第１条 １９２０年公務秘密法第８条

防諜・諜報職員による防諜・諜報情報の漏えい	
秘密の内容	防諜又は諜報に関する情報、文書その他の物
漏えい	①　防諜機関若しくは諜報機関の職員又は職員であった者が、当該機関の職員としての地位に基づき保有し、又は保有していた、防諜又は諜報に関する情報、文書その他の物の、正当な権限のない開示 ②　この規定の対象となることについて通知を受ける者又は受けていた者が、通知が有効な間に職務を通じて保有し、又は保有していた、防諜又は諜報に関する情報、文書その他の物の、正当な権限のない開示 （「通知」は、対象者の業務が防諜又は諜報に関するものあって、国家安全保障の利害の観点から本規定の対象とすべきと大臣が判断する場合に、大臣の書面により行われる。） 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第１条（１）、（６） １９８９年公務秘密法第10条（１）

諸外国の秘密保全に関する法制における罰則（英国）

その他の職員等による防諜・諜報情報の漏えい	
秘密の内容	（防諜機関若しくは諜報機関の職員又は職員であった者及びこの規定の対象となることについて通知を受ける者又は受けていた者を除き、公務員、政府と契約関係にある者又はこれらであった者が、その職位・立場に基づき保有し、又は保有していた）防諜又は諜報に関する情報、文書その他の物
漏えい	公務員、政府と契約関係にある者又はこれらであった者による正当な権限なく行われる害を及ぼす開示 （「害を及ぼす開示とは、 ①　防諜若しくは諜報の業務又はこれらの一部の遂行に支障をきたすもの ②　権限なく開示がなされた場合には①の害が生じるおそれがある情報、文書その他の物、又は①の被害と同様の事態が生じるおそれがある種別又は内容に該当する情報、文書その他の物が開示の対象となるもの をいう。） 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第１条（３）、（４） １９８９年公務秘密法第10条（１）

諸外国の秘密保全に関する法制における罰則（英国）

公務員等による防衛情報の漏えい	
秘密の内容	（公務員又は政府と契約関係にある者としての地位に基づき保有しており、又は保有していた）防衛に関する情報、文書その他の物 （「防衛」とは、 ①　国軍の規模、形態、組織、ロジスティクス、部隊編成、戦略的配置、作戦、及び準備・訓練の状況 ②　国軍の武器、備品その他の装備、これらの装備の発明、開発、生産及び操作並びにこれらの装備に関する調査研究 ③　防衛に関する政策及び戦略並びに軍事に関する計画及び諜報 ④　戦時に必要な必需品の支給及び供給を維持するための計画及び方策をいう。）
漏えい	公務員、政府と契約関係にある者又はこれらであった者による正当な権限なくなされる、害を及ぼす開示 （「害を及ぼす開示」とは、 ①　軍の任務を遂行するための軍事力若しくはその一部に害を及ぼし、軍の構成員の生命を失わせ、若しくはその身体に危険を及ぼし、又は軍の施設若しくは設備に重大な損害を及ぼすもの ②　①のほか、海外における英国の国益を損ね、かかる国益の増大若しくは保護にとって重大な障害となり、又は海外における英国国民の安全に害を及ぼすもの ③　権限のない開示がなされた場合には①又は②のような影響が生じるおそれがある情報、文書その他の物 が開示の対象となるものをいう。） 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第２条 １９８９年公務秘密法第10条（１）

諸外国の秘密保全に関する法制における罰則（英国）

公務員等による国際関係情報の漏えい	
秘密の内容	（公務員又は政府と契約関係にある者としての地位に基づき保有しており、又は保有していた）国際関係に関する情報、文書その他の物又は英国以外の国若しくは国際機関から取得した秘密の情報、文書その他の物
漏えい	公務員、政府と契約関係にある者又はこれらであった者による正当な権限なくなされる害を及ぼす開示 （「害を及ぼす開示」とは、 ① 海外における英国の国益を損ね、かかる国益の増大若しくは保護にとって重大な障害となり、又は海外における英国国民の安全に害を及ぼすもの ② 権限のない開示がなされた場合には①の影響が生じるおそれがある情報、文書その他の物が開示の対象となるもの をいう。） 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第３条（１）（２） １９８９年公務秘密法第10条（１）

公務員等による犯罪を惹起する情報等の漏えい	
秘密の内容	（公務員又は政府と契約関係にある者としての地位に基づき保有しており、又は保有していた） ① 開示により、犯罪を生ぜしめる情報、文書その他の物 ② 開示により、被拘禁者の逃亡又は被拘禁者の保護を害するその他の行為を容易にする情報、文書その他の物 ③ 開示により、犯罪の予防若しくは探知又は容疑者の逮捕若しくは訴追の妨げとなる情報、文書その他の物 ④ 権限なき開示により、①～③に記述される影響が生ずるおそれがある情報、文書その他の物
漏えい	公務員、政府と契約関係にある者又はこれらであった者による正当な権限なき開示 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第４条（１）（２）

諸外国の秘密保全に関する法制における罰則（英国）

公務員等による通信傍受に関する情報等の漏えい	
秘密の内容	（公務員又は政府と契約関係にある者としての地位に基づき保有しており、又は保有していた） ①　１９８５年通信傍受法第２条に基づく令状により、若しくは２０００年捜査権限規制法第５条に基づく通信傍受令状により行われる通信傍受により得られる情報、これらの通信傍受による情報の取得に関する情報、又はかかる通信傍受に使用され、使用のために保管され、若しくは通信傍受により得られた文書その他の物 ②　１９８９年防諜機関法第３条若しくは１９９４年諜報機関法第５条に基づく令状によって授権された行為により、若しくは同法第７条の授権により得られる情報、かかる行為による情報の入手に関する情報、又はかかる行為に使用され、使用のために保管され、若しくはかかる行為によって得られた文書その他の物
漏えい	公務員、政府と契約関係にある者又はこれらであった者による正当な権限なき開示 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第４条（３）

公務秘密法違反の開示等により秘密情報を取得した者による漏えい	
秘密の内容	○１９８９年公務秘密法第４条までの規定により保護対象となっている情報、文書その他の物
漏えい	１９８９年公務秘密法第４条までの規定による保護対象であること及び次のいずれかに該当することにより保有するに至ったものであることを知り又はそう信ずるに足る合理的理由がある場合における、次のいずれかにより保有するに至った者による正当な権限なき開示 ①　公務員又は政府と契約関係にある者による正当な権限なき開示 ②　公務員又は政府と契約関係にある者が、秘匿性の確保を条件とし、又は秘匿性の確保を合理的に期待して行った委託 ③　②の委託を受けた者による正当な権限なき開示 ・ただし、防諜、諜報、防衛、若しくは国際関係に関する情報、文書その他の物又は外国若しくは国際機関から入手した秘密の情報、文書その他の物については、次のいずれかの場合を除く ・害を及ぼす開示でない場合 ・害を及ぼす開示であることを知らず、又は害を及ぼすと信ずるに足る合理的理由がなかった場合 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第５条（１）～（５）

諸外国の秘密保全に関する法制における罰則（英国）

公務秘密法違反の開示等により秘密情報を取得した者による漏えい	
秘密の内容	１９１１年公務秘密法第１条違反により保有するに至った情報、文書その他の物
漏えい	１９１１年公務秘密法第１条違反により保有するに至ったことを知り、又はそう信ずるに足る合理的理由がある場合における適法な権限のない開示 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第５条（６）

英国から外国等に伝達された防衛情報等を不当に取得した者による漏えい	
秘密の内容	防諜、諜報、防衛又は国際関係に関するものであって、英国により又は英国のために、秘匿性を確保して外国又は国際機関に伝達された情報、文書その他の物
漏えい	・　伝達された当該国又は国際機関若しくはその加盟国の授権に基づかない開示により保有するに至った者による害を及ぼす開示 ・　ただし、当該情報、文書その他の物の内容及びその保有の経緯がこの規定に定めるものに該当し、その開示が害を及ぼすものであることを知り、又はそう信ずるに足る合理的理由がある場合に限り処罰する ・　次のいずれかに該当する場合は罰しない ・保有するに至った者が、適法な権限により開示する場合 ・当該伝達された国又は国際機関若しくはその加盟国の権限に基づき、すでに公開された場合 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第６条

諸外国の秘密保全に関する法制における罰則（英国）

公務員等による秘密文書等に関する注意懈怠等	
秘密の内容	１９８９年公務秘密法第７条までの規定により、無権限でなされる開示が違法となる文書その他の物（であって、公務員又は政府と契約関係にある者としての地位に基づき保有され、又は管理されていたもの）
漏えい	
過失犯	公務員（第１条第１項の通知を受けた者を含む）又は政府の受託業者が、その職位・立場に応じ十分に期待できる注意を怠った場合 【３月以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
その他	・　公務員（第１条第１項の通知を受けた者を含む）によるその職務上の義務に反した文書又は物件の保持 ・　政府と契約関係にある者による文書又は物件の返却又は処分に係る当局の指示の不遵守 【３月以下の自由刑若しくは罰金又はこれらの併科】
根拠	１９８９年公務秘密法第８条（１）～（３） １９８９年公務秘密法第10条（２）

秘匿の確保を条件として開示された文書等に関する注意懈怠	
秘密の内容	１９８９年公務秘密法第５条の規定によりその権限のない開示が違法となる文書その他の物（であって、保有され、又は管理されているもの）
漏えい	
過失犯	当該文書等について秘匿の確保を条件とした上で、又は公務員若しくは政府の受託業者が秘匿の確保を合理的に期待し得る状況において、これらの者から取得した者が、当該個人の職位・立場に照らして合理的に期待される、権限なくなされる開示を防止するための注意を怠った場合 【３月以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
その他	文書又は物件の返却又は処分に係る当局の指示の不遵守 【３月以下の自由刑若しくは罰金又はこれらの併科】
根拠	１９８９年公務秘密法第８条（４） １９８９年公務秘密法第10条（２）

諸外国の秘密保全に関する法制における罰則（英国）

秘密文書等の返却・処分に係る指示の不遵守	
秘密の内容	１９８９年公務秘密法第６条の規定によりその権限のない開示が違法となる文書その他の物（であって、保有され、又は管理されているもの）
漏えい	
取得（探知）	
その他	文書又は物件の返却又は処分に係る当局の指示の不遵守 【３月以下の自由刑若しくは罰金又はこれらの併科】
根拠	１９８９年公務秘密法第８条（５） １９８９年公務秘密法第10条（２）

特定の公的な情報の開示	
秘密の内容	前条項までの規定（特に第5条5項）によって公開されないように保護されている情報、文書その他の物へのアクセスを得る目的で利用できる公的な情報、文書その他の物
漏えい	上記秘密として挙げられる公的な情報、文書その他の物を、権限なく上述の目的で用いられることが合理的に予想される状況下における開示 開示した情報、文書その他の物が公的なものとされるのは、以下の場合。 ⅰ）開示者が公務員又は政府の受託業者という職位・立場によりこれを保有又は入手していた場合 ⅱ）開示者が、公務員又は政府の受託業者という職位・立場により、開示の対象となったものを保有若しくは入手していたことを知り、又はそれと信ずるに足る合理的根拠がある場合 【２年（略式手続の場合は６月）以下の自由刑若しくは罰金又はこれらの併科】
取得（探知）	
根拠	１９８９年公務秘密法第８条（６）～（８） １９８９年公務秘密法第10条（１）

諸外国の秘密保全に関する法制における罰則（独国）

国家機密の外国勢力への漏えい・漏えい目的の取得等	
秘密の内容	国家機密 （「国家機密」とは、限定された範囲の者のみに入手可能で、ドイツ連邦共和国の対外的安全に対して重大な不利益を及ぼす危険を回避するため、外国の勢力に対して秘密にしておかなければならない事実、物又は知識をいう。自由で民主主義的な基本秩序に反する事実、又は、国家間で合意した軍備の制限に、ドイツ連邦共和国の条約相手国に対して秘密にしながら違反する事実は、国家機密ではない。）
漏えい	①　外国の勢力若しくはその仲介者への教示、又は ②　ドイツ連邦共和国に不利益を与え、若しくは外国の勢力に利益を与えるために、無権限の者に取得させ、若しくは公表すること により、ドイツ連邦共和国の対外的安全に対して、重大な不利益を及ぼす危険を生じさせること（第94条） 【１年以上の自由刑】 【犯情の特に重い事案では、無期又は５年以上の自由刑】 （「犯情の特に重い事案」とは、原則として、行為者が、 ①国家機密の保持をその者に特別に義務づける責任ある地位を濫用したとき、又は ②その行為により、ドイツ連邦共和国の対外的安全に対して、特に重大な不利益を及ぼす危険を生じさせたとき をいう。）
取得（探知）	漏えいするための国家機密の取得（第96条（１）） 【１年以上10年以下の自由刑】
その他	（第94条又は第96条１項では、処罰の対象となっていない場合において） ①　外国の勢力のための、国家機密の獲得若しくは通報に向けられた活動、又は ②　外国の勢力若しくはその仲介者に対する、上記活動の用意がある旨の表明（第98条） 【５年以下の自由刑又は罰金】 【犯情の特に重い事案では、１年以上10年以下の自由刑】 （「犯情の特に重い事案」とは、原則として、行為者が、国家機密の保持をその者に特別に義務づける責任ある地位を濫用したときをいう。）
根拠	刑法第93条、第94条、第96条（１）、第98条

諸外国の秘密保全に関する法制における罰則（独国）

国家機密の漏えい・過失漏えい・漏えい目的の取得	
秘密の内容	政府の行政機関により、又はその指示により秘密にされている国家機密
漏えい	無権限の者に取得させ、又は公表することにより、ドイツ連邦共和国の対外的安全に対して、重大な不利益を及ぼす危険を生じさせること又はその未遂 （第94条が適用される場合を除く）（第95条） 【６月以上５年以下の自由刑】 【犯情の特に重い事案では、１年以上10年以下の自由刑】 （「犯情の特に重い事案」とは、原則として、行為者が、 ① 国家機密の保持をその者に特別に義務づける責任ある地位を濫用したとき、又は ② その行為により、ドイツ連邦共和国の対外的安全に対して、特に重大な不利益を及ぼす危険を生じさせたとき をいう。）
過失犯	・ 過失により無権限の者に取得させ、又は公表することにより、ドイツ連邦共和国の対外的安全に対して、重大な不利益を及ぼす危険を生じさせること（第97条（１）） 【５年以下の自由刑又は罰金】 ・ 軽率に、公務、職務上の地位又は官庁の委託により入手可能であった上記国家機密を、無権限の者に取得させることにより、ドイツ連邦共和国の対外的安全に対して、重大な不利益を及ぼす危険を過失により生じさせること（第97条（２）） 【３年以下の自由刑又は罰金】
取得（探知）	上記漏えいをするための取得又はその未遂（第96条（２）） 【６月以上５年以下の自由刑】
根拠	刑法第95条、第96条（２）、第97条

国家機密とはならない秘密の外国勢力への漏えい等	
秘密の内容	自由で民主主義的な基本秩序に反する事実、又は国家間で合意した軍備の制限に、ドイツ連邦共和国の条約相手国に対して秘密にしながら違反する事実であるために、国家機密とはならない秘密
漏えい	外国の勢力又はその仲介者への教示により、ドイツ連邦共和国の対外的安全に対して、重大な不利益を及ぼす危険を生じさせること（第97条ａ） 【１年以上の自由刑】 【犯情の特に重い事案では、無期又は５年以上の自由刑】 （「犯情の特に重い事案」とは、原則として、行為者が、 ① 国家機密の保持をその者に特別に義務づける責任ある地位を濫用したとき、又は ② その行為によりドイツ連邦共和国の対外的安全対して、特に重大な不利益を及ぼす危険を生じさせたとき をいう。）
取得（探知）	外国の勢力又はその仲介者への教示のための取得（第96条（１）準用） 【１年以上10年以下の自由刑】
根拠	刑法第97条ａ

諸外国の秘密保全に関する法制における罰則（独国）

国家機密を国家機密でないと誤信した上での漏えい等	
秘密の内容	（行政機関により、又はその指示により秘密にされている）国家機密
漏えい	
	当該国家機密が、第97条ａに掲げる種類の秘密であると誤信し、第94条から第97条までに規定する行為を行った場合であって、 ①　当該誤信が、行為者の責めに帰するとき ②　当該行為が、誤信された当該違反に対して抵抗する目的から出たものでないとき、又は ③　当該行為が、当該事情の下で目的のために適切な手段でないとき（「適切な手段」とは、原則として、行為者が連邦議会の構成員に事前に援助を求めることを指す）（第97条ｂ（１）） 【各条に規定する罰則】
取得（探知）	
根拠	刑法第97条ｂ（１）

外国の諜報機関のための諜報活動等	
秘密の内容	
漏えい	
取得（探知）	
その他	（第94条若しくは第96条第１項、又は、これらに併せて適用されるときの第97条ａ若しくは第97条ｂでは処罰対象とならない場合において） ①　外国の勢力の諜報機関のための、事実、物又は知識の通報又は提供に向けての、ドイツ連邦共和国に対する諜報活動、又は ②　外国の勢力の諜報機関若しくはその仲介者に対する、上記活動の用意がある旨の表明 【５年以下の自由刑又は罰金】 【犯情の特に重い事案では、1年以上10年以下の自由刑】 （「犯情の特に重い事案」とは、原則として、行為者が、官庁により、若しくはその指示により秘密にされている事実、物又は知識を通報し、又は交付したとき、及び、 ①　このような秘密の保持を特別に義務づける責任ある地位を濫用したとき、又は ②　その行為により、ドイツ連邦共和国の対外的安全対して、重大な不利益を及ぼす危険を生じさせたとき をいう。）
根拠	刑法第99条

諸外国の秘密保全に関する法制における罰則（独国）

公務員による秘密の漏えい・過失漏えい	
秘密の内容	①　公務担当者として、 ②　公務のために特に義務付けられた者として、又は ③　人事代表法による任務と権限を行使する者として、 ゆだねられ、又は知ることとなった秘密
漏えい	権限なしに漏えいし、かつ、それによって重要な公共利益を危うくしたこと又はその未遂 【５年以下の自由刑又は罰金】
過失犯	過失によって重要な公共利益を危うくしたとき 【１年以下の自由刑又は罰金】
取得（探知）	
根拠	刑法第353条ｂ(1)

守秘義務を負う物件・情報の漏えい	
秘密の内容	○　連邦若しくは州の立法機関又はそれらの委員会の決議に基づき、守秘義務を負う物件又は情報 ○　その他の行政機関から秘密侵害の場合の可罰性を示され、公式に守秘義務を負う物件又は情報
漏えい	（刑法第353条ｂ(1)の場合を除き） 権限なしに他人に得させ、又は公表し、かつ、それによって重要な公共利益を危うくしたこと又はその未遂 【３年以下の自由刑又は罰金】
取得（探知）	
根拠	刑法第353条ｂ(2)

諸外国の秘密保全に関する法制における罰則（仏国）

国民の基本的利益に関する情報の外国勢力への漏えい・漏えい目的での収集等	
秘密の内容	○　その利用、開示又は収集が、国民の基本的利益を損なう情報、技法、物、文書、情報処理データ又はファイル （「国民の基本的利益」とは、国の独立性、領土の一体性、国の安全性、共和政体、国防及び外交能力、国内外における国民の保護、自然環境とその周囲の状況の調和並びに国の科学・経済力及び文化的遺産の重要な要素をいう。） ○　仏国と、外国又は国際機関との間で締結され正式に承認かつ公示された秘区分情報の保護に関する安全保障協定にしたがって交換される情報 ○　仏国と、欧州連合の機関又は組織との間で交換され、欧州連合官報への公示対象となった、安全保障規則にしたがって交換される情報
漏えい	・　外国の勢力、外国の企業・組織、外国の管理下にある企業・組織又はその代理人への、提供又はそれらによるアクセスを可能にすること 【15年以下の拘禁刑及び罰金】 ・　外国の勢力、外国の企業・組織、外国の管理下にある企業・組織又はその代理人のための、それらの提供を目的とする行為（対象となる秘密の内容は、上記の「情報、技法、物品、文書、情報処理データ又はファイル」に加え、「装置」も含む） 【10年以下の拘禁刑及び罰金】
取得（探知）	・　外国の勢力、外国の企業・組織、外国の管理下にある企業・組織又はその代理人に引き渡す目的での収集 【10年以下の拘禁刑及び罰金】 ・　外国の勢力、外国の企業・組織、外国の管理下にある企業・組織又はその代理人のための、それらの取得を目的とする行為（対象となる秘密の内容は、上記の「情報、技法、物品、文書、情報処理データ又はファイル」に加え、「装置」も含む） 【10年以下の拘禁刑及び罰金】
その他	※北大西洋条約署名国又は北大西洋条約機構の利益に反して行われる上記行為にも、上記罰則が適用される。
根拠	刑法第411-6条～第411-8条、第414-8条、第414-9条

国防に関する立入禁止区域への無許可立入り	
秘密の内容	国防に関わる官民の機関、法人又は企業において、自由な通行が禁止され、かつ、施設若しくは設備の保護又は研究・調査・製造上の秘密の確保のために境界を定められている、囲われた場所又は土地の内部
漏えい	
取得（探知）	許可のない立入り及びその未遂 【６月以下の拘禁刑及び罰金】
根拠	刑法第413-7条、第413-8条

諸外国の秘密保全に関する法制における罰則（仏国）

公務員等による国防上の秘密の漏えい・過失漏えい等	
秘密の内容	○　国防上の秘密の性質を有する技法、物、文書、情報、情報ネットワーク、情報処理データ又はファイル （「国防上の秘密の性質を有するもの」とは、その伝播又はそれへのアクセスを制限するための秘密指定措置の対象となっている、国防に関する技法、物、文書、情報、情報ネットワーク、情報処理データ又はファイルをいう。） ○　仏国と、外国又は国際機関との間で締結され正式に承認かつ公示された秘区分情報の保護に関する安全保障協定にしたがって交換される情報 ○　仏国と、欧州連合の機関又は組織の間で交換され、欧州連合官報での公示対象となった、安全保障規則にしたがって交換される情報
漏えい	・　身分若しくは職業によって、又は職務若しくは一時的若しくは恒常的な任務に基づいて、上記秘密を所持する者が、 ①　資格のない者にアクセスさせ、公表し、若しくは資格のない者に伝達する行為又はこれらの未遂、 ②　他人にアクセスさせ、破棄させ、横領させ、窃取させ、複製させ、又は暴露させる行為 【７年以下の拘禁刑及び罰金】 ・　上記（身分若しくは職業によって、又は職務若しくは一時的若しくは恒常的な任務に基づいて，上記秘密を所持する者）以外の者による、上記秘密の内容の公表若しくは資格のない者に知らせる行為又はこれらの未遂 【５年以下の拘禁刑及び罰金】
過失犯	身分若しくは職業によって，又は職務若しくは一時的若しくは恒常的な任務に基づいて，上記秘密を所持する者が、過失又は怠慢により、上記秘密を伝達し、公表し若しくは資格のない者にアクセスさせ、又は破棄させ、横領させ、窃取させ、複製させ、若しくは暴露させる行為 【３年以下の拘禁刑及び罰金】
取得（探知）	・　身分若しくは職業によって，又は職務若しくは一時的若しくは恒常的な任務に基づいて、上記秘密を所持する者による、横領、窃取若しくは複製又はその未遂 【７年以下の拘禁刑及び罰金】 ・　上記（身分若しくは職業によって，又は職務若しくは一時的若しくは恒常的な任務に基づいて，上記秘密を所持する者）以外の者による、上記秘密の取得、アクセス、知得、窃取、複製又はこれらの未遂 【５年以下の拘禁刑及び罰金】
その他	・　身分若しくは職業によって，又は職務若しくは一時的若しくは恒常的な任務に基づいて、上記秘密を所持する者による、破棄又はその未遂 【７年以下の拘禁刑及び罰金】 ・　上記（身分若しくは職業によって，又は職務若しくは一時的若しくは恒常的な任務に基づいて，上記秘密を所持する者）以外の者による、方法を問わず、上記秘密の破棄又はその未遂 【５年以下の拘禁刑及び罰金】 ※北大西洋条約署名国又は北大西洋条約機構の利益に反して行われる上記行為にも、上記罰則が適用される。
根拠	刑法第413-10条、第413-11条、第413-12条、第414-8条、第414-9条

国防秘密として秘密指定された区域に無権限者を立ち入らせる行為等	
秘密の内容	○　国防秘密として秘密指定された区域 （※立ち入ること自体により，そこに所在する設備又はそこで行われている活動によって国防秘密を知られてしまう区域についてのみ、国防秘密として秘密指定の対象とすることができる） ○　仏国と、外国又は国際機関との間で締結され正式に承認かつ公示された秘区分情報の保護に関する安全保障協定にしたがって交換される情報 ○　仏国と、欧州連合の機関又は組織の間で交換され、欧州連合官報での公示対象となった、安全保障規則にしたがって交換される情報
漏えい	・　身分若しくは職業，又は職務若しくは一時的若しくは恒常的な任務に基づく責任者が，資格のない者を当該区域に立ち入らせる行為 ・　資格のある者が，当該区域に所在する設備又は当該区域内で行われている活動の性質に関する要素を公表し又は資格のない者に知らせる行為 【７年以下の拘禁刑及び罰金】 ・　資格のない者が、当該区域に所在する設備又は当該区域内で行われている活動の性質に関する要素を公表し又は資格のない者に知らせる行為 【５年以下の拘禁刑及び罰金】
過失犯	国防秘密として秘密指定された区域についての、身分若しくは職業，又は職務若しくは一時的若しくは恒常的な任務に基づく責任者が、不注意又は怠慢によって、資格のない者を当該区域に立ち入らせ、又は、当該区域内に所在する設備又は当該区域内で行われている活動の性質に関する要素を公表し若しくは資格のない者に知らせる行為 【３年以下の拘禁刑及び罰金】
取得（探知）	資格のない者による、当該区域への立入り 【５年以下の拘禁刑及び罰金】
その他	※北大西洋条約署名国又は北大西洋条約機構の利益に反して行われる上記行為にも、上記罰則が適用される。
根拠	刑法第413-9-1条、第413-10-1条、第413-11-1条、第414-8条、第414-9条

（参考資料）

関係法令

○国家公務員法（昭和22年法律第120号）（抄）

（秘密を守る義務）

第百条　職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。

②～⑤　（略）

第百九条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

一～十一　（略）

十二　第百条第一項若しくは第二項又は第百六条の十二第一項の規定に違反して秘密を漏らした者

十三～十八　（略）

第百十一条　第百九条第二号より第四号まで及び第十二号又は前条第一項第一号、第三号から第七号まで、第九号から第十五号まで、第十八号及び第二十号に掲げる行為を企て、命じ、故意にこれを容認し、そそのかし又はそのほう助をした者は、それぞれ各本条の刑に処する。

○自衛隊法（昭和29年法律第165号）（抄）

（防衛秘密）

第九十六条の二　防衛大臣は、自衛隊についての別表第四に掲げる事項であつて、公になつていないもののうち、我が国の防衛上特に秘匿することが必要であるもの（日米相互防衛援助協定等に伴う秘密保護法（昭和二十九年法律第百六十六号）第一条第三項に規定する特別防衛秘密に該当するものを除く。）を防衛秘密として指定するものとする。

2　前項の規定による指定は、次の各号のいずれかに掲げる方法により行わなければならない。

一　政令で定めるところにより、前項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に標記を付すこと。

二　前項に規定する事項の性質上前号の規定によることが困難である場合において、政令で定めるところにより、当該事項が同項の規定の適用を受けることとなる旨を当該事項を取り扱う者に通知すること。

3　防衛大臣は、自衛隊の任務遂行上特段の必要がある場合に限り、国の行政機関の職員のうち防衛に関連する職務に従事する者又は防衛省との契約に基づき防衛秘密に係る物件の製造若しくは役務の提供を業とする者に、政令で定めるところにより、防衛秘密の取扱いの業務を行わせることができる。

4　防衛大臣は、第一項及び第二項に定めるもののほか、政令で定めるところにより、第一項に規定する事項の保護上必要な措置を講ずるものとする。

第百二十二条　防衛秘密を取り扱うことを業務とする者がその業務により知得した防衛秘密を漏らしたときは、五年以下の懲役に処する。防衛秘密を取り扱うことを業務としなくなつた後においても、同様とする。

2　前項の未遂罪は、罰する。

3　過失により、第一項の罪を犯した者は、一年以下の禁錮又は三万円以下の罰金に処する。

4　第一項に規定する行為の遂行を共謀し、教唆し、又は煽動した者は、三年以下の懲役に処する。

5　第二項の罪を犯した者又は前項の罪を犯した者のうち第一項に規定する行為の遂行を共謀したものが自首したときは、その刑を減軽し、又は免除する。

6　第一項から第四項までの罪は、刑法第三条の例に従う。

別表第四　（第九十六条の二関係）

一　自衛隊の運用又はこれに関する見積り若しくは計画若しくは研究

二　防衛に関し収集した電波情報、画像情報その他の重要な情報

三　前号に掲げる情報の収集整理又はその能力

四　防衛力の整備に関する見積り若しくは計画又は研究

五　武器、弾薬、航空機その他の防衛の用に供する物（船舶を含む。第八号及び第九号において同じ。）の種類又は数量

六　防衛の用に供する通信網の構成又は通信の方法

七　防衛の用に供する暗号

八　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの仕様、性能又は使用方法

九　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの製作、検査、修理又は試験の方法

十　防衛の用に供する施設の設計、性能又は内部の用途（第六号に掲げるものを除く。）

○自衛隊法施行令（昭和29年政令第179号）（抄）

（標記の方法）

第百十三条の二　法第九十六条の二第二項第一号の規定による標記は、別表第十一に掲げる様式に従い、同条第一項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件の見やすい箇所に、印刷、押印又は刻印その他これらに準ずる確実な方法により付さなければならない。この場合において、当該文書、図画又は物件のうち同項に規定する事項を記録し、又は化体する部分を容易に区分することができるときは、当該標記は、当該部分に付さなければならない。

（通知の方法）

第百十三条の三　法第九十六条の二第二項第二号の規定による通知は、同条第一項に規定する事項を特定して記載した書面により行わなければならない。

（他の行政機関における防衛秘密の取扱いの業務）

第百十三条の四　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する職務に従事する者に防衛秘密の取扱いの業務を行わせるときは、次に掲げる事項について、あらかじめ、当該行政機関の長と協議するものとする。

一　防衛秘密の取扱いの業務を管理する者の指名に関すること。

二　防衛秘密の取扱いの業務に従事する職員の範囲の指定に関すること。

三　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

四　防衛秘密の伝達（文書、図画又は物件の交付以外の方法によるものに限る。以下この節において同じ。）の手続に関すること。

五　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

六　当該行政機関以外の者への防衛秘密の提供の制限に関すること。

七　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

八　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（契約業者における防衛秘密の取扱いの業務）

第百十三条の五　防衛省との契約に基づき防衛秘密に係る物件の製造又は役務の提供を業とする者（次項及び第百十三条の十一において「契約業者」という。）は、次に掲げる基準に適合していなければならない。

一　防衛秘密の保護上必要な措置に関し役員及び職員が遵守すべき規則を定めているこ

と。

二　防衛秘密の取扱いの業務を管理する者を選任していること。

三　防衛秘密の取扱いの業務に従事する役員及び職員に防衛秘密の保護上必要な措置に関する教育を行つていること。

四　防衛秘密に係る文書、図画又は物件を保管するための施設設備その他防衛秘密の保護上必要な施設設備を設置していること。

2　契約業者との契約においては、次に掲げる事項を定めなければならない。

一　防衛秘密の取扱いの業務に従事する役員及び職員の範囲の指定に関すること。

二　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

三　防衛秘密の伝達の手続に関すること。

四　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

五　当該契約業者以外の者への防衛秘密の提供の制限に関すること。

六　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

七　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（防衛秘密管理者）

第百十三条の六　防衛大臣は、防衛省の職員のうちから、防衛秘密の取扱いの業務を管理する者（以下この節において「防衛秘密管理者」という。）を指名するものとする。

（防衛秘密の指定に伴う措置）

第百十三条の七　防衛大臣は、法第九十六条の二第一項に規定する事項を防衛秘密として指定したときは、指定に関する記録を作成するとともに、防衛秘密として指定した事項を当該事項に係る防衛秘密管理者に通報するものとする。

（防衛秘密の表示）

第百十三条の八　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定された場合において、第百十三条の二の規定により標記が付されたもの以外に当該防衛秘密として指定された事項を記録する文書、図画若しくは物件又は当該事項を化体する物件があるときは、当該文書、図画又は物件に、同条の規定の例により、防衛秘密の表示をする措置を講じなければならない。ただし、当該物件の性質上表示をすることが困難である場合は、この限りでない。

（防衛秘密の周知）

第百十三条の九　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定されたときは、当該事項の取扱いの業務に従事する防衛省の職員にその旨を周知させなければならない。

（職員の範囲の指定）

第百十三条の十　防衛秘密の取扱いの業務に従事する防衛省の職員の範囲は、防衛秘密管理者が定める。

（他の行政機関等における防衛秘密の取扱いの業務に伴う措置）

第百十三条の十一　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する

職務に従事する者又は契約業者に防衛秘密の取扱いの業務を行わせるときは、防衛秘密管理者に防衛秘密に係る文書、図画若しくは物件を交付させ、又は防衛秘密を伝達させるものとする。

2　前項の交付又は伝達は、防衛秘密として指定された事項を特定して行うものとする。

（防衛秘密が要件を欠くに至つた場合の措置）

第百十三条の十二　防衛大臣は、防衛秘密として指定した事項が法第九十六条の二第一項に規定する要件を欠くに至つたときは、速やかに、当該事項に係る防衛秘密管理者に当該事項が防衛秘密でなくなつた旨を通報するものとする。

2　前項の通報を受けた防衛秘密管理者は、直ちに、当該通報に係る事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に付された第百十三条の二の規定による標記及び第百十三条の八の規定による表示を抹消する措置を講ずるとともに、当該事項の取扱いの業務に従事する防衛省の職員及び前条第一項の規定により当該事項に係る文書、図画若しくは物件を交付し、又は当該事項を伝達した相手方に当該事項が防衛秘密でなくなつた旨を周知させなければならない。

（防衛秘密の取扱いの管理のための措置）

第百十三条の十三　防衛秘密管理者は、第百十三条の八から前条までに規定するもののほか、防衛大臣の定めるところにより、防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱い及び防衛秘密の伝達を適切に管理するための措置を講じなければならない。

（委任規定）

第百十三条の十四　この節に規定するもののほか、防衛秘密の保護上必要な措置に関する細目は、防衛大臣が定める。

○日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号）（抄）

（定義）

第一条　この法律において「日米相互防衛援助協定等」とは、日本国とアメリカ合衆国との間の相互防衛援助協定、日本国とアメリカ合衆国との間の船舶貸借協定及び日本国に対する合衆国艦艇の貸与に関する協定をいう。

2　この法律において「装備品等」とは、船舶、航空機、武器、弾薬その他の装備品及び資材をいう。

3　この法律において「特別防衛秘密」とは、左に掲げる事項及びこれらの事項に係る文書、図画又は物件で、公になつていないものをいう。

一　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された装備品等について左に掲げる事項

イ　構造又は性能

ロ　製作、保管又は修理に関する技術

ハ　使用の方法

ニ　品目及び数量

二　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された情報で、装備品等に関する前号イからハまでに掲げる事項に関するもの

（特別防衛秘密保護上の措置）

第二条　特別防衛秘密を取り扱う国の行政機関の長は、政令で定めるところにより、特別防衛秘密について、標記を附し、関係者に通知する等特別防衛秘密の保護上必要な措置を講ずるものとする。

（罰則）

第三条　左の各号の一に該当する者は、十年以下の懲役に処する。

一　わが国の安全を害すべき用途に供する目的をもつて、又は不当な方法で、特別防衛秘密を探知し、又は収集した者

二　わが国の安全を害する目的をもつて、特別防衛秘密を他人に漏らした者

三　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を他人に漏らしたもの

2　前項第二号又は第三号に該当する者を除き、特別防衛秘密を他人に漏らした者は、五年以下の懲役に処する。

3　前二項の未遂罪は、罰する。

第四条　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らしたものは、二年以下の禁こ又は五万円以下の罰金に処する。

2　前項に掲げる者を除き、業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らした者は、一年以下の禁こ又は三万円以下の罰金に処する。

第五条　第三条第一項の罪の陰謀をした者は、五年以下の懲役に処する。

2　第三条第二項の罪の陰謀をした者は、三年以下の懲役に処する。

3　第三条第一項の罪を犯すことを教唆し、又はせん動した者は、第一項と同様とし、同条第二項の罪を犯すことを教唆し、又はせん動した者は、前項と同様とする。

4　前項の規定は、教唆された者が教唆に係る犯罪を実行した場合において、刑法（明治四十年法律第四十五号）総則に定める教唆の規定の適用を排除するものではない。

（自首減免）

第六条　第三条第一項第一号若しくは第三項又は前条第一項若しくは第二項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

（この法律の解釈適用）

第七条　この法律の適用にあたつては、これを拡張して解釈して、国民の基本的人権を不当に侵害するようなことがあつてはならない。

○日米相互防衛援助協定等に伴う秘密保護法施行令（昭和29年政令第149号）（抄）

（秘密区分）

第一条　日米相互防衛援助協定等に伴う秘密保護法第一条第三項に規定する特別防衛秘密は、その秘密の保護の必要度に応じて、機密、極秘又は秘のいずれかに区分しなければならない。

2　前項の「機密」とは、秘密の保護が最高度に必要であつて、その漏えいが我が国の安全に対し、特に重大な損害を与えるおそれのあるものをいう。

3　第一項の「極秘」とは、秘密の保護が高度に必要であつて、その漏えいが我が国の安全に対し、重大な損害を与えるおそれのあるものをいう。

4　第一項の「秘」とは、秘密の保護が必要であつて、機密及び極秘に該当しないものをいう。

（秘密区分の指定、変更及び解除）

第二条　国の行政機関（内閣府並びに内閣府設置法（平成十一年法律第八十九号）第四十九条第一項及び第二項に規定する機関並びに国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関をいう。以下同じ。）の長（以下「各省庁の長」という。）で、アメリカ合衆国政府から特別防衛秘密に属する事項又は文書、図画若しくは物件の供与を受けたものは、その特別防衛秘密につき、前条に規定する秘密区分の指定を行わなければならない。

2　前項の国の行政機関の長は、同項の規定により指定した秘密区分を変更することができる。

3　第一項の国の行政機関の長は、特別防衛秘密として秘匿する必要がなくなつたとき、又は公になつたものがあるときは、その部分に限り、速やかに、秘密区分の指定を解除しなければならない。

4　第一項の国の行政機関の長は、特別防衛秘密について、前三項の規定により秘密区分を指定し、変更し、又は解除したときは、必要に応じ、その旨を関係行政機関に通知しなければならない。

（標記）

第三条　各省庁の長は、その取り扱う特別防衛秘密に属する文書、図画又は物件につき、これらが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨の標記をしなければならない。

2　各省庁の長は、前条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、速やかに、前項の標記を変更し、又は抹消しなければならない。

3　第一項の標記の様式は、別記様式のとおりとする。

（通知）

第四条　各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図画若しくは物件であつて、前条の規定による標記ができないもの若しくは標記をすることが適当でないものについては、関係者に対し、文書又は口頭により、これが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨の通知をしなければならない。

2　各省庁の長は、第二条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、必要に応じ、速やかに、その旨を関係者に対し、文書により、通知しなければならない。

（掲示）

第五条　各省庁の長は、その管理する施設内にある特別防衛秘密に属する物件について、必要があるときは、その物件に近接してはならない旨の掲示を行うものとする。

（委託中における特別防衛秘密保護上の措置）

第六条　各省庁の長は、その取り扱う特別防衛秘密を製作、修理、実験、調査研究、複製等のため政府機関以外の者に委託する場合は、委託中における秘密の漏えいの危険を防止するため、契約条項に秘密保持に関する規定を設ける等必要な措置を講じなければならない。

（特別防衛秘密保護上の措置の実施細目）

第七条　第二条から前条までに規定するもののほか、各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図面若しくは物件の複製、送達、伝達、接受、保管、破棄等その取扱いに関し、特別防衛秘密の保護上必要な措置を講じなければならない。

2　前項に規定する特別防衛秘密の保護上必要な措置の実施細目については、各省庁の長が定める。

○日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法（昭和27年法律第138号）（抄）

（定義）

第一条　この法律において「協定」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定をいう。

2　この法律において「合衆国軍隊」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約に基づき日本国にあるアメリカ合衆国の陸軍、空軍及び海軍をいう。

3　この法律において「合衆国軍隊の構成員」、「軍属」又は「家族」とは、協定第一条に規定する合衆国軍隊の構成員、軍属又は家族をいう。

（合衆国軍隊の機密を侵す罪）

第六条　合衆国軍隊の機密（合衆国軍隊についての別表に掲げる事項及びこれらの事項に係る文書、図画若しくは物件で、公になつていないものをいう。以下同じ。）を、合衆国軍隊の安全を害すべき用途に供する目的をもつて、又は不当な方法で、探知し、又は収集した者は、十年以下の懲役に処する。

2　合衆国軍隊の機密で、通常不当な方法によらなければ探知し、又は収集することができないようなものを他人に漏らした者も、前項と同様とする。

3　前二項の未遂罪は、罰する。

第七条　前条第一項又は第二項の罪の陰謀をした者は、五年以下の懲役に処する。

2　前条第一項又は第二項の罪を犯すことを教唆し、又はせん動した者も、前項と同様とする。

3　前項の規定は、教唆された者が、教唆に係る犯罪を実行した場合において、刑法総則に定める教唆の規定の適用を排除するものではない。

第八条　第六条第一項の罪、同項に係る同条第三項の罪又は同条第一項に係る前条第一項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

別表

一　防衛に関する事項

イ　防衛の方針若しくは計画の内容又はその実施の状況

ロ　部隊の隷属系統、部隊数、部隊の兵員数又は部隊の装備

ハ　部隊の任務、配備又は行動

ニ　部隊の使用する軍事施設の位置、構成、設備、性能又は強度

ホ　部隊の使用する艦船、航空機、兵器、弾薬その他の軍需品の種類又は数量

二　編制又は装備に関する事項

イ　編制若しくは装備に関する計画の内容又はその実施の状況

ロ　編制又は装備の現況

ハ　艦船、航空機、兵器、弾薬その他の軍需品の構造又は性能

三　運輸又は通信に関する事項

イ　軍事輸送の計画の内容又はその実施の状況
ロ　軍用通信の内容
ハ　軍用暗号

○不正競争防止法（平成５年法律第47号）（抄）

（定義）

第二条　この法律において「不正競争」とは、次に掲げるものをいう。

一～六　（略）

七　営業秘密を保有する事業者（以下「保有者」という。）からその営業秘密を示された場合において、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為

八～十五　（略）

２～５　（略）

６　この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

７～10　（略）

（罰則）

第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。

一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。以下この条において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第三条に規定する不正アクセス行為をいう。）その他の保有者の管理を害する行為をいう。以下この条において同じ。）により、営業秘密を取得した者

二　詐欺等行為又は管理侵害行為により取得した営業秘密を、不正の利益を得る目的で、又はその保有者に損害を加える目的で、使用し、又は開示した者

三　営業秘密を保有者から示された者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、次のいずれかに掲げる方法でその営業秘密を領得した者

イ　営業秘密記録媒体等（営業秘密が記載され、又は記録された文書、図画又は記録媒体をいう。以下この号において同じ。）又は営業秘密が化体された物件を横領すること。

ロ　営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その複製を作成すること。

ハ　営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装すること。

四　営業秘密を保有者から示された者であって、その営業秘密の管理に係る任務に背いて前号イからハまでに掲げる方法により領得した営業秘密を、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、使用し、又は開示した者

五　営業秘密を保有者から示されたその役員（理事、取締役、執行役、業務を執行する社員、監事若しくは監査役又はこれらに準ずる者をいう。次号において同じ。）又は従業者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、その営業秘密を使用し、又は開示した者（前号に掲げる者を除く。）

六　営業秘密を保有者から示されたその役員又は従業者であった者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その在職中に、その営業秘密の管理に係る任務に背いてその営業秘密の開示の申込みをし、又はその営業秘密の使用若しくは開示について請託を受けて、その営業秘密をその職を退いた後に使用し、又は開示した者（第四号に掲げる者を除く。）

七　不正の利益を得る目的で、又はその保有者に損害を加える目的で、第二号又は前三号の罪に当たる開示によって営業秘密を取得して、その営業秘密を使用し、又は開示した者

2・3　（略）

4　第一項第二号又は第四号から第七号までの罪は、詐欺等行為若しくは管理侵害行為があった時又は保有者から示された時に日本国内において管理されていた営業秘密について、日本国外においてこれらの罪を犯した者にも適用する。

5～7　（略）

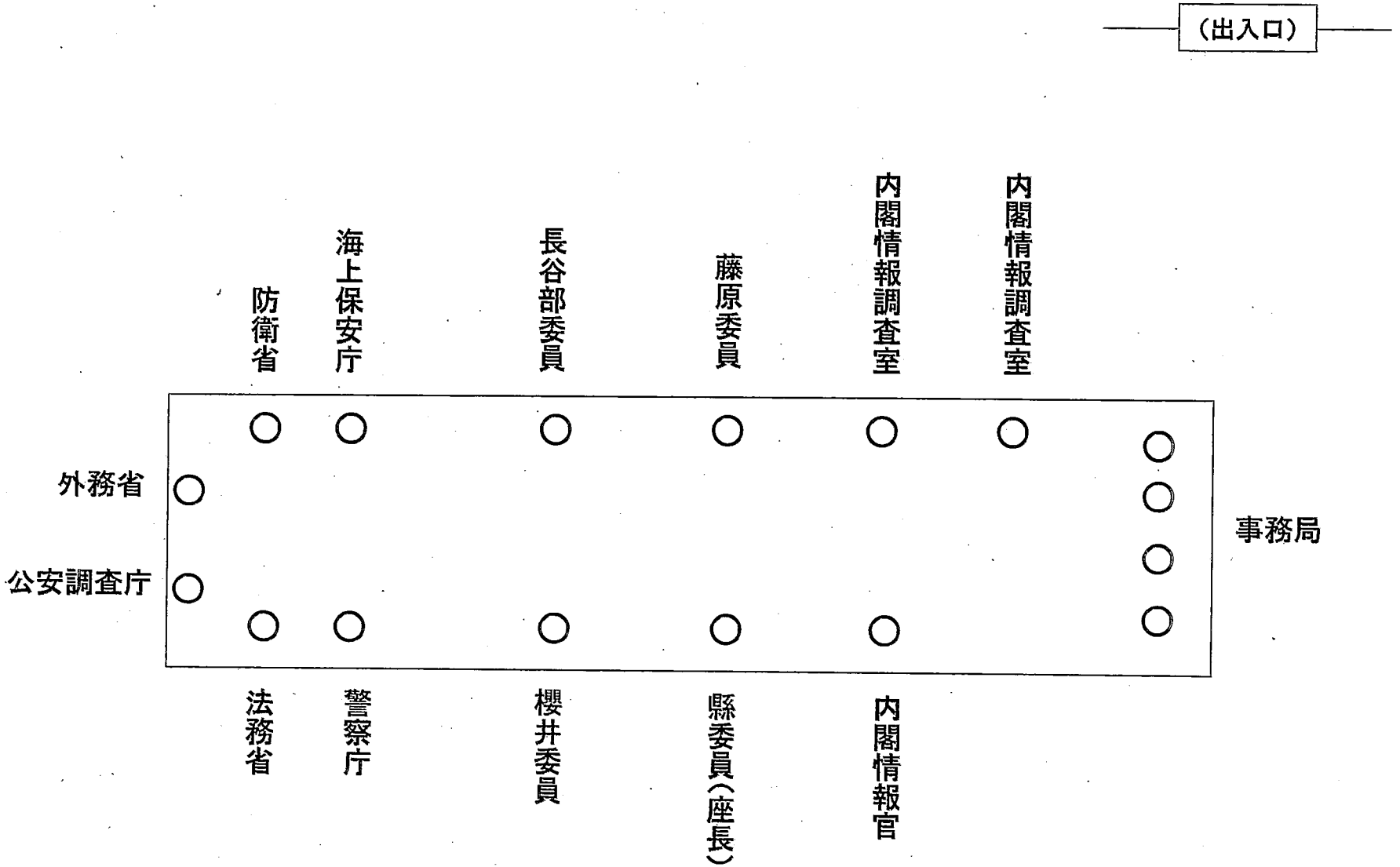
第二十二条　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、前条第一項第一号、第二号若しくは第七号又は第二項に掲げる規定の違反行為をしたときは、行為者を罰するほか、その法人に対して三億円以下の罰金刑を、その人に対して本条の罰金刑を科する。

2　前項の場合において、当該行為者に対してした前条第一項第一号、第二号及び第七号並びに第二項第五号の罪に係る同条第三項の告訴は、その法人又は人に対しても効力を生じ、その法人又は人に対してした告訴は、当該行為者に対しても効力を生ずるものとする。

3　第一項の規定により前条第一項第一号、第二号若しくは第七号又は第二項の違反行為につき法人又は人に罰金刑を科する場合における時効の期間は、これらの規定の罪についての時効の期間による。

第5回秘密保全のための法制の在り方に関する有識者会議　座席表

平成23年5月13日(金)午前10時～正午　於:内閣府本府5階特別会議室



機密性2情報

対外非公表　取扱注意　配布資料

秘密保全のための法制の在り方に関する有識者会議（第５回）

法形式、国民の知る権利等との関係、立法府及び司法府に関する考え方（事務局案）・論点

平成２３年５月１３日

第5　法形式

事　務　局　案

本法制の形式について

○　本法制は、特別秘密の厳格な保全により国益や国民の安全を確保すること等を目的とするものであり、主に服務規律の維持を目的として守秘義務を課す公務員法等とは趣旨が異なる
⇒　**公務員法等の改正により本法制を実現することは適当ではない**

○　特別秘密のうち、外交、公共の安全及び秩序の維持の分野については、国の安全の分野についての自衛隊法のような**受け皿となり得る既存の法令は見いだし難い**

⇒　**新規立法によることが必要**

※　運用の統一性や制度の一覧性を確保するという観点から、**単一の法制によること**が適当

本法制における特別秘密と防衛秘密及び特別防衛秘密との関係

防衛秘密

本法制の対象とする秘密との間で秘密として保護する理由に異なるところはない

⇒　**本法制に取り込み、統一的に運用すること**が適当

特別防衛秘密

本法制の対象とする秘密との間で秘密として保護する理由に異なるところはない

⇒　MDA秘密保護法は、日米相互防衛援助協定等に伴うものという特別な性格を有している

⇒　**引き続きMDA秘密保護法によること**が適当

※　合衆国軍隊の機密（日米地位協定の実施に伴う刑事特別法）
刑事特別法が米国のために在日米軍の秘密情報を保護するものであり、我が国の存立にとって重要な秘密情報を保護する本法制とは保護法益が異なる
⇒　**引き続き同法によるべき**ものと考えられる

論　点

○　上記の考え方の当否

第6　国民の知る権利等との関係

対外非公表　取扱注意

事　務　局　案

1　国民の知る権利

本法制における特別秘密として保護される情報は、政府の保有する秘密情報の中でも国の存立にとって重要なもので、我が国の安全、外交、公共の安全及び秩序の維持という観点から、特に秘匿することが必要なもの

⇒ 本法制の特別秘密が国民に知らされないことをもって、国民の知る権利との関係で問題を生ずるものではない

2　取材の自由

○　漏えいの教唆について、最高裁判例によれば、正当な取材活動は処罰対象とならず、取材の手段・方法が刑罰法令に触れる場合や社会観念上是認できない態様のものである場合に刑罰の対象となる

○　特定取得罪も、取材の自由の下で保護されるべき取材活動を刑罰の対象とするものではない

⇒ 本法制は、取材の自由を不当に制限するものではない

本法制は適切に運用されれば、国民の知る権利との関係で問題を生ずる又は取材の自由を不当に制限するものではないが、念のため、例えば、国民の権利が不当に制限されることがないように留意すべき旨を定めることも選択肢として考えられる

論　点

○　上記の考え方の妥当性

第7　立法府及び司法府

対外非公表　取扱注意

事　務　局　案

○ 特別秘密の作成・取得の目的に従い伝達を受けることは想定されない
○ 立法府及び司法府が業務上の必要性から特別秘密の伝達を受けることがあり得る ⇒ <u>立法府及び司法府に本法制を適用すべきか</u>

立法府

国会議員

法律上、守秘義務を課せられていない

▽

本法制の適用の是非の検討に当たっては、国会議員の活動の在り方も踏まえつつ、立法府における秘密会の在り方や秘密保全の在り方全般と特別秘密の管理の在り方との関係を整理する必要

▽

立法府の在り方の根幹に関わることから、
<u>一義的には立法府における議論に委ねることが適当</u>

国会議員であっても、行政機関の長又は幹部として特別秘密を取り扱う場合には、行政府の職員として本法制の対象とすべき※

（ただし、本法制の適格性確認については、内閣総理大臣及び国務大臣は対象外、その他の特別な任命の要件・手続が採用されている職は個別に判断）

国会職員

国会議員とともに立法府における議論に委ねることが適当

司法府

裁判官

罰則を伴う守秘義務が設けられていない

▽

本法制の適用の是非の検討に当たっては、裁判官の職業倫理の在り方も踏まえつつ、裁判官による秘密保全の在り方全般と特別秘密の管理の在り方との関係を整理する必要

▽

<u>司法制度全体への影響を踏まえて別途検討されることが適当</u>

裁判所職員

裁判官とともに司法制度全体への影響を踏まえて別途検討されることが適当

弁護士

○ 司法府に属する者ではない
○ 司法府についての検討を直ちに実施すべき状況にない

▽

弁護士に関する検討を先行させることは不適当

論　点

○ 上記の考え方の当否

※　自衛隊法においては、防衛大臣、副大臣及び大臣政務官は、防衛秘密の取扱業務者として同法の適用対象とされている。

（参考資料）

関係法令

○国家公務員法（昭和22年法律第120号）（抄）

（秘密を守る義務）

第百条　職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。

②～⑤　（略）

第百九条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

一～十一　（略）

十二　第百条第一項若しくは第二項又は第百六条の十二第一項の規定に違反して秘密を漏らした者

十三～十八　（略）

第百十一条　第百九条第二号より第四号まで及び第十二号又は前条第一項第一号、第三号から第七号まで、第九号から第十五号まで、第十八号及び第二十号に掲げる行為を企て、命じ、故意にこれを容認し、そそのかし又はそのほう助をした者は、それぞれ各本条の刑に処する。

○自衛隊法（昭和29年法律第165号）（抄）

（防衛秘密）

第九十六条の二　防衛大臣は、自衛隊についての別表第四に掲げる事項であつて、公になつていないもののうち、我が国の防衛上特に秘匿することが必要であるもの（日米相互防衛援助協定等に伴う秘密保護法（昭和二十九年法律第百六十六号）第一条第三項に規定する特別防衛秘密に該当するものを除く。）を防衛秘密として指定するものとする。

2　前項の規定による指定は、次の各号のいずれかに掲げる方法により行わなければならない。

一　政令で定めるところにより、前項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に標記を付すこと。

二　前項に規定する事項の性質上前号の規定によることが困難である場合において、政令で定めるところにより、当該事項が同項の規定の適用を受けることとなる旨を当該事項を取り扱う者に通知すること。

3　防衛大臣は、自衛隊の任務遂行上特段の必要がある場合に限り、国の行政機関の職員のうち防衛に関連する職務に従事する者又は防衛省との契約に基づき防衛秘密に係る物件の製造若しくは役務の提供を業とする者に、政令で定めるところにより、防衛秘密の取扱いの業務を行わせることができる。

4　防衛大臣は、第一項及び第二項に定めるもののほか、政令で定めるところにより、第一項に規定する事項の保護上必要な措置を講ずるものとする。

第百二十二条　防衛秘密を取り扱うことを業務とする者がその業務により知得した防衛秘密を漏らしたときは、五年以下の懲役に処する。防衛秘密を取り扱うことを業務としなくなつた後においても、同様とする。

2　前項の未遂罪は、罰する。

3　過失により、第一項の罪を犯した者は、一年以下の禁錮又は三万円以下の罰金に処する。

4　第一項に規定する行為の遂行を共謀し、教唆し、又は煽動した者は、三年以下の懲役に処する。

5　第二項の罪を犯した者又は前項の罪を犯した者のうち第一項に規定する行為の遂行を共謀したものが自首したときは、その刑を減軽し、又は免除する。

6　第一項から第四項までの罪は、刑法第三条の例に従う。

別表第四　（第九十六条の二関係）

一　自衛隊の運用又はこれに関する見積り若しくは計画若しくは研究

二　防衛に関し収集した電波情報、画像情報その他の重要な情報

三　前号に掲げる情報の収集整理又はその能力

四　防衛力の整備に関する見積り若しくは計画又は研究

五　武器、弾薬、航空機その他の防衛の用に供する物（船舶を含む。第八号及び第九号において同じ。）の種類又は数量

六　防衛の用に供する通信網の構成又は通信の方法

七　防衛の用に供する暗号

八　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの仕様、性能又は使用方法

九　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの製作、検査、修理又は試験の方法

十　防衛の用に供する施設の設計、性能又は内部の用途（第六号に掲げるものを除く。）

○自衛隊法施行令（昭和29年政令第179号）（抄）

（標記の方法）

第百十三条の二　法第九十六条の二第二項第一号の規定による標記は、別表第十一に掲げる様式に従い、同条第一項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件の見やすい箇所に、印刷、押印又は刻印その他これらに準ずる確実な方法により付さなければならない。この場合において、当該文書、図画又は物件のうち同項に規定する事項を記録し、又は化体する部分を容易に区分することができるときは、当該標記は、当該部分に付さなければならない。

（通知の方法）

第百十三条の三　法第九十六条の二第二項第二号の規定による通知は、同条第一項に規定する事項を特定して記載した書面により行わなければならない。

（他の行政機関における防衛秘密の取扱いの業務）

第百十三条の四　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する職務に従事する者に防衛秘密の取扱いの業務を行わせるときは、次に掲げる事項について、あらかじめ、当該行政機関の長と協議するものとする。

一　防衛秘密の取扱いの業務を管理する者の指名に関すること。

二　防衛秘密の取扱いの業務に従事する職員の範囲の指定に関すること。

三　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

四　防衛秘密の伝達（文書、図画又は物件の交付以外の方法によるものに限る。以下この節において同じ。）の手続に関すること。

五　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

六　当該行政機関以外の者への防衛秘密の提供の制限に関すること。

七　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

八　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（契約業者における防衛秘密の取扱いの業務）

第百十三条の五　防衛省との契約に基づき防衛秘密に係る物件の製造又は役務の提供を業とする者（次項及び第百十三条の十一において「契約業者」という。）は、次に掲げる基準に適合していなければならない。

一　防衛秘密の保護上必要な措置に関し役員及び職員が遵守すべき規則を定めていること。

二　防衛秘密の取扱いの業務を管理する者を選任していること。

三　防衛秘密の取扱いの業務に従事する役員及び職員に防衛秘密の保護上必要な措置に

関する教育を行つていること。

四　防衛秘密に係る文書、図画又は物件を保管するための施設設備その他防衛秘密の保護上必要な施設設備を設置していること。

2　契約業者との契約においては、次に掲げる事項を定めなければならない。

一　防衛秘密の取扱いの業務に従事する役員及び職員の範囲の指定に関すること。

二　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

三　防衛秘密の伝達の手続に関すること。

四　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

五　当該契約業者以外の者への防衛秘密の提供の制限に関すること。

六　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

七　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（防衛秘密管理者）

第百十三条の六　防衛大臣は、防衛省の職員のうちから、防衛秘密の取扱いの業務を管理する者（以下この節において「防衛秘密管理者」という。）を指名するものとする。

（防衛秘密の指定に伴う措置）

第百十三条の七　防衛大臣は、法第九十六条の二第一項に規定する事項を防衛秘密として指定したときは、指定に関する記録を作成するとともに、防衛秘密として指定した事項を当該事項に係る防衛秘密管理者に通報するものとする。

（防衛秘密の表示）

第百十三条の八　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定された場合において、第百十三条の二の規定により標記が付されたもの以外に当該防衛秘密として指定された事項を記録する文書、図画若しくは物件又は当該事項を化体する物件があるときは、当該文書、図画又は物件に、同条の規定の例により、防衛秘密の表示をする措置を講じなければならない。ただし、当該物件の性質上表示をすることが困難である場合は、この限りでない。

（防衛秘密の周知）

第百十三条の九　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定されたときは、当該事項の取扱いの業務に従事する防衛省の職員にその旨を周知させなければならない。

（職員の範囲の指定）

第百十三条の十　防衛秘密の取扱いの業務に従事する防衛省の職員の範囲は、防衛秘密管理者が定める。

（他の行政機関等における防衛秘密の取扱いの業務に伴う措置）

第百十三条の十一　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する職務に従事する者又は契約業者に防衛秘密の取扱いの業務を行わせるときは、防衛秘密管理者に防衛秘密に係る文書、図画若しくは物件を交付させ、又は防衛秘密を伝達させるものとする。

2　前項の交付又は伝達は、防衛秘密として指定された事項を特定して行うものとする。

（防衛秘密が要件を欠くに至つた場合の措置）

第百十三条の十二　防衛大臣は、防衛秘密として指定した事項が法第九十六条の二第一項に規定する要件を欠くに至つたときは、速やかに、当該事項に係る防衛秘密管理者に当該事項が防衛秘密でなくなつた旨を通報するものとする。

2　前項の通報を受けた防衛秘密管理者は、直ちに、当該通報に係る事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に付された第百十三条の二の規定による標記及び第百十三条の八の規定による表示を抹消する措置を講ずるとともに、当該事項の取扱いの業務に従事する防衛省の職員及び前条第一項の規定により当該事項に係る文書、図画若しくは物件を交付し、又は当該事項を伝達した相手方に当該事項が防衛秘密でなくなつた旨を周知させなければならない。

（防衛秘密の取扱いの管理のための措置）

第百十三条の十三　防衛秘密管理者は、第百十三条の八から前条までに規定するもののほか、防衛大臣の定めるところにより、防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱い及び防衛秘密の伝達を適切に管理するための措置を講じなければならない。

（委任規定）

第百十三条の十四　この節に規定するもののほか、防衛秘密の保護上必要な措置に関する細目は、防衛大臣が定める。

○日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号）（抄）

（定義）

第一条　この法律において「日米相互防衛援助協定等」とは、日本国とアメリカ合衆国との間の相互防衛援助協定、日本国とアメリカ合衆国との間の船舶貸借協定及び日本国に対する合衆国艦艇の貸与に関する協定をいう。

2　この法律において「装備品等」とは、船舶、航空機、武器、弾薬その他の装備品及び資材をいう。

3　この法律において「特別防衛秘密」とは、左に掲げる事項及びこれらの事項に係る文書、図画又は物件で、公になつていないものをいう。

一　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された装備品等について左に掲げる事項

イ　構造又は性能

ロ　製作、保管又は修理に関する技術

ハ　使用の方法

ニ　品目及び数量

二　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された情報で、装備品等に関する前号イからハまでに掲げる事項に関するもの

（特別防衛秘密保護上の措置）

第二条　特別防衛秘密を取り扱う国の行政機関の長は、政令で定めるところにより、特別防衛秘密について、標記を附し、関係者に通知する等特別防衛秘密の保護上必要な措置を講ずるものとする。

（罰則）

第三条　左の各号の一に該当する者は、十年以下の懲役に処する。

一　わが国の安全を害すべき用途に供する目的をもつて、又は不当な方法で、特別防衛秘密を探知し、又は収集した者

二　わが国の安全を害する目的をもつて、特別防衛秘密を他人に漏らした者

三　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を他人に漏らしたもの

2　前項第二号又は第三号に該当する者を除き、特別防衛秘密を他人に漏らした者は、五年以下の懲役に処する。

3　前二項の未遂罪は、罰する。

第四条　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らしたものは、二年以下の禁こ又は五万円以下の罰金に処する。

2　前項に掲げる者を除き、業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らした者は、一年以下の禁こ又は三万円以下の罰金に処する。

第五条　第三条第一項の罪の陰謀をした者は、五年以下の懲役に処する。

2　第三条第二項の罪の陰謀をした者は、三年以下の懲役に処する。

3　第三条第一項の罪を犯すことを教唆し、又はせん動した者は、第一項と同様とし、同

条第二項の罪を犯すことを教唆し、又はせん動した者は、前項と同様とする。

4　前項の規定は、教唆された者が教唆に係る犯罪を実行した場合において、刑法（明治四十年法律第四十五号）総則に定める教唆の規定の適用を排除するものではない。

（自首減免）

第六条　第三条第一項第一号若しくは第三項又は前条第一項若しくは第二項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

（この法律の解釈適用）

第七条　この法律の適用にあたつては、これを拡張して解釈して、国民の基本的人権を不当に侵害するようなことがあつてはならない。

○日米相互防衛援助協定等に伴う秘密保護法施行令（昭和29年政令第149号）（抄）

（秘密区分）

第一条　日米相互防衛援助協定等に伴う秘密保護法第一条第三項に規定する特別防衛秘密は、その秘密の保護の必要度に応じて、機密、極秘又は秘のいずれかに区分しなければならない。

2　前項の「機密」とは、秘密の保護が最高度に必要であつて、その漏えいが我が国の安全に対し、特に重大な損害を与えるおそれのあるものをいう。

3　第一項の「極秘」とは、秘密の保護が高度に必要であつて、その漏えいが我が国の安全に対し、重大な損害を与えるおそれのあるものをいう。

4　第一項の「秘」とは、秘密の保護が必要であつて、機密及び極秘に該当しないものをいう。

（秘密区分の指定、変更及び解除）

第二条　国の行政機関（内閣府並びに内閣府設置法（平成十一年法律第八十九号）第四十九条第一項及び第二項に規定する機関並びに国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関をいう。以下同じ。）の長（以下「各省庁の長」という。）で、アメリカ合衆国政府から特別防衛秘密に属する事項又は文書、図画若しくは物件の供与を受けたものは、その特別防衛秘密につき、前条に規定する秘密区分の指定を行わなければならない。

2　前項の国の行政機関の長は、同項の規定により指定した秘密区分を変更することができる。

3　第一項の国の行政機関の長は、特別防衛秘密として秘匿する必要がなくなつたとき、又は公になつたものがあるときは、その部分に限り、速やかに、秘密区分の指定を解除しなければならない。

4　第一項の国の行政機関の長は、特別防衛秘密について、前三項の規定により秘密区分を指定し、変更し、又は解除したときは、必要に応じ、その旨を関係行政機関に通知しなければならない。

（標記）

第三条　各省庁の長は、その取り扱う特別防衛秘密に属する文書、図画又は物件につき、これらが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨

の標記をしなければならない。

2　各省庁の長は、前条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、速やかに、前項の標記を変更し、又は抹消しなければならない。

3　第一項の標記の様式は、別記様式のとおりとする。

（通知）

第四条　各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図画若しくは物件であつて、前条の規定による標記ができないもの若しくは標記をすることが適当でないものについては、関係者に対し、文書又は口頭により、これが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨の通知をしなければならない。

2　各省庁の長は、第二条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、必要に応じ、速やかに、その旨を関係者に対し、文書により、通知しなければならない。

（掲示）

第五条　各省庁の長は、その管理する施設内にある特別防衛秘密に属する物件について、必要があるときは、その物件に近接してはならない旨の掲示を行うものとする。

（委託中における特別防衛秘密保護上の措置）

第六条　各省庁の長は、その取り扱う特別防衛秘密を製作、修理、実験、調査研究、複製等のため政府機関以外の者に委託する場合は、委託中における秘密の漏えいの危険を防止するため、契約条項に秘密保持に関する規定を設ける等必要な措置を講じなければならない。

（特別防衛秘密保護上の措置の実施細目）

第七条　第二条から前条までに規定するもののほか、各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図面若しくは物件の複製、送達、伝達、接受、保管、破棄等その取扱いに関し、特別防衛秘密の保護上必要な措置を講じなければならない。

1　前項に規定する特別防衛秘密の保護上必要な措置の実施細目については、各省庁の長が定める。

（注）日本国とアメリカ合衆国との間の相互防衛援助協定（抄）

第三条

1　各政府は、この協定に従つて他方の政府が供与する秘密の物件、役務又は情報についてその秘密の漏せつ又はその危険を防止するため、両政府の間で合意する秘密保持の措置を執るものとする。

2　（略）

○日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法（昭和27年法律第138号）（抄）

（定義）

第一条　この法律において「協定」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定をいう。

2　この法律において「合衆国軍隊」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約に基づき日本国にあるアメリカ合衆国の陸軍、空軍及び海軍をいう。

3　この法律において「合衆国軍隊の構成員」、「軍属」又は「家族」とは、協定第一条に規定する合衆国軍隊の構成員、軍属又は家族をいう。

（合衆国軍隊の機密を侵す罪）

第六条　合衆国軍隊の機密（合衆国軍隊についての別表に掲げる事項及びこれらの事項に係る文書、図画若しくは物件で、公になつていないものをいう。以下同じ。）を、合衆国軍隊の安全を害すべき用途に供する目的をもつて、又は不当な方法で、探知し、又は収集した者は、十年以下の懲役に処する。

2　合衆国軍隊の機密で、通常不当な方法によらなければ探知し、又は収集することができないようなものを他人に漏らした者も、前項と同様とする。

3　前二項の未遂罪は、罰する。

第七条　前条第一項又は第二項の罪の陰謀をした者は、五年以下の懲役に処する。

2　前条第一項又は第二項の罪を犯すことを教唆し、又はせん動した者も、前項と同様とする。

3　前項の規定は、教唆された者が、教唆に係る犯罪を実行した場合において、刑法総則に定める教唆の規定の適用を排除するものではない。

第八条　第六条第一項の罪、同項に係る同条第三項の罪又は同条第一項に係る前条第一項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

別表

一　防衛に関する事項

イ　防衛の方針若しくは計画の内容又はその実施の状況

ロ　部隊の隷属系統、部隊数、部隊の兵員数又は部隊の装備

ハ　部隊の任務、配備又は行動

ニ　部隊の使用する軍事施設の位置、構成、設備、性能又は強度

ホ　部隊の使用する艦船、航空機、兵器、弾薬その他の軍需品の種類又は数量

二　編制又は装備に関する事項

イ　編制若しくは装備に関する計画の内容又はその実施の状況

ロ　編制又は装備の現況

ハ　艦船、航空機、兵器、弾薬その他の軍需品の構造又は性能

三　運輸又は通信に関する事項

イ　軍事輸送の計画の内容又はその実施の状況

ロ　軍用通信の内容

ハ　軍用暗号

（注）日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定【日米地位協定】（抄）

第二十三条

（前略）　日本国政府は、その領域において合衆国政府の設備、備品、財産、記録及び公務上の情報の十分な安全及び保護を確保するため、並びに適用されるべき日本国の法令に基づいて犯人を罰するため、必要な立法を求め、及び必要なその他の措置を執ることに同意する。

○不正競争防止法（平成５年法律第47号）（抄）

（定義）

第二条　この法律において「不正競争」とは、次に掲げるものをいう。

一～六　（略）

七　営業秘密を保有する事業者（以下「保有者」という。）からその営業秘密を示された場合において、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密を使用し、又は開示する行為

八～十五　（略）

２～５　（略）

６　この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

７～10　（略）

（罰則）

第二十一条　次の各号のいずれかに該当する者は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。

一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。以下この条において同じ。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第三条に規定する不正アクセス行為をいう。）その他の保有者の管理を害する行為をいう。以下この条において同じ。）により、営業秘密を取得した者

二　詐欺等行為又は管理侵害行為により取得した営業秘密を、不正の利益を得る目的で、又はその保有者に損害を加える目的で、使用し、又は開示した者

三　営業秘密を保有者から示された者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、次のいずれかに掲げる方法でその営業秘密を領得した者

イ　営業秘密記録媒体等（営業秘密が記載され、又は記録された文書、図画又は記録媒体をいう。以下この号において同じ。）又は営業秘密が化体された物件を横領すること。

ロ　営業秘密記録媒体等の記載若しくは記録について、又は営業秘密が化体された物件について、その複製を作成すること。

ハ　営業秘密記録媒体等の記載又は記録であって、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装すること。

四　営業秘密を保有者から示された者であって、その営業秘密の管理に係る任務に背いて前号イからハまでに掲げる方法により領得した営業秘密を、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、使用し、又は開示した者

五　営業秘密を保有者から示されたその役員（理事、取締役、執行役、業務を執行する

社員、監事若しくは監査役又はこれらに準ずる者をいう。次号において同じ。）又は従業者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その営業秘密の管理に係る任務に背き、その営業秘密を使用し、又は開示した者（前号に掲げる者を除く。）

六　営業秘密を保有者から示されたその役員又は従業者であった者であって、不正の利益を得る目的で、又はその保有者に損害を加える目的で、その在職中に、その営業秘密の管理に係る任務に背いてその営業秘密の開示の申込みをし、又はその営業秘密の使用若しくは開示について請託を受けて、その営業秘密をその職を退いた後に使用し、又は開示した者（第四号に掲げる者を除く。）

七　不正の利益を得る目的で、又はその保有者に損害を加える目的で、第二号又は前三号の罪に当たる開示によって営業秘密を取得して、その営業秘密を使用し、又は開示した者

2・3　（略）

4　第一項第二号又は第四号から第七号までの罪は、詐欺等行為若しくは管理侵害行為があった時又は保有者から示された時に日本国内において管理されていた営業秘密について、日本国外においてこれらの罪を犯した者にも適用する。

5～7　（略）

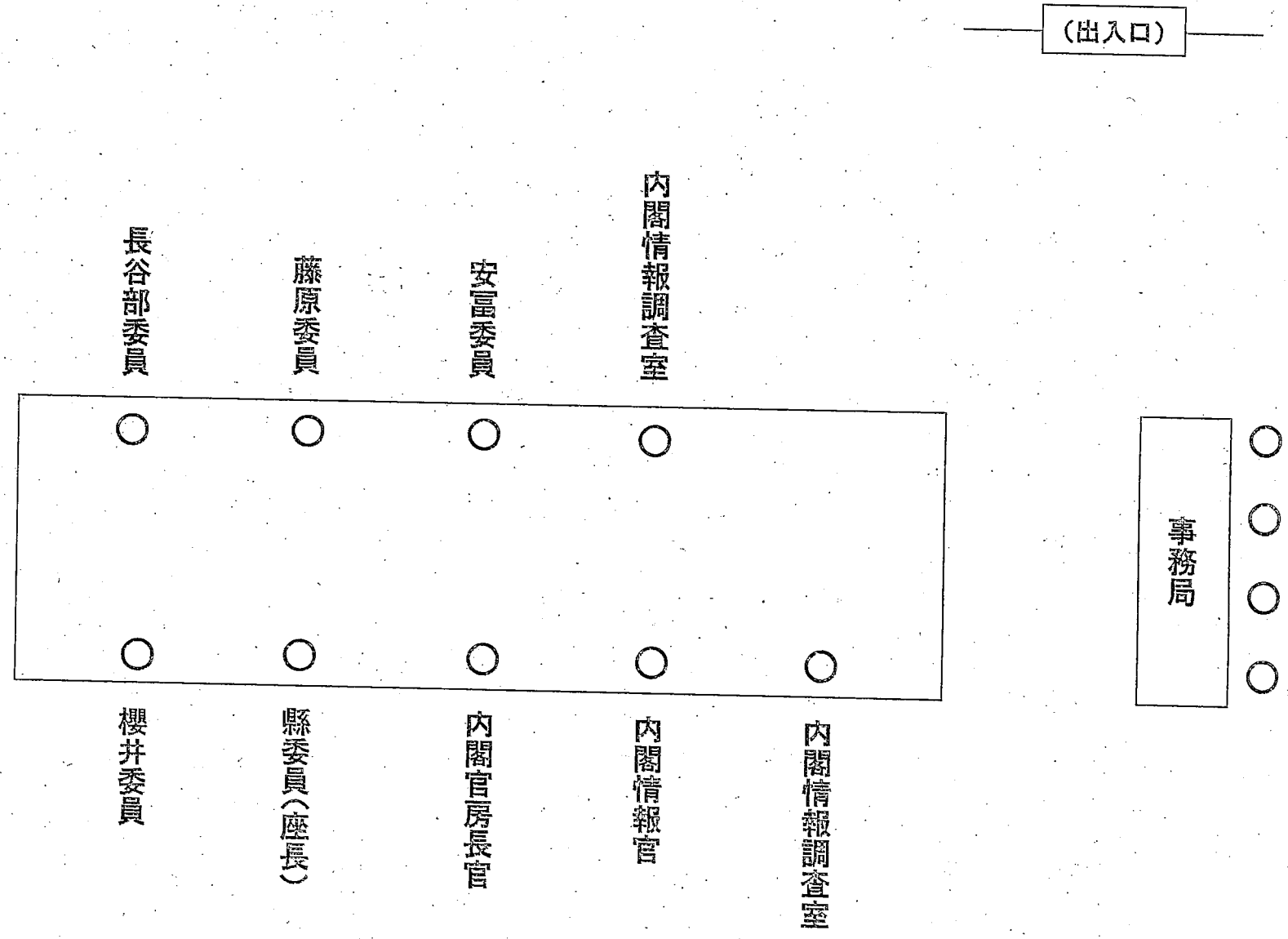
第二十二条　法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、前条第一項第一号、第二号若しくは第七号又は第二項に掲げる規定の違反行為をしたときは、行為者を罰するほか、その法人に対して三億円以下の罰金刑を、その人に対して本条の罰金刑を科する。

2　前項の場合において、当該行為者に対してした前条第一項第一号、第二号及び第七号並びに第二項第五号の罪に係る同条第三項の告訴は、その法人又は人に対しても効力を生じ、その法人又は人に対してした告訴は、当該行為者に対しても効力を生ずるものとする。

3　第一項の規定により前条第一項第一号、第二号若しくは第七号又は第二項の違反行為につき法人又は人に罰金刑を科する場合における時効の期間は、これらの規定の罪についての時効の期間による。

第6回秘密保全のための法制の在り方に関する有識者会議　座席表

平成23年6月10日(金)午前10時～正午　於:官邸4階大会議室



機密性２情報　取扱注意

秘密保全のための法制の在り方について（報告書）

【案】

平成23年６月　日

秘密保全のための法制の在り方に関する有識者会議

目次

はじめに

当会議は、本年１月、政府における情報保全に関する検討委員会から、我が国における秘密保全のための法制の在り方について意見を示すよう要請を受けた。

我が国では、近年、国民主権の理念の下、情報公開法制の整備をはじめ、行政の透明性の確保のための取組について積極的な検討がなされ、一定の成果を上げてきた。同時に、我が国を取り巻く厳しい国際情勢の下で国及び国民の利益を守るためには、政府による秘密保全を徹底することが極めて重要であり、当会議は、政府による秘密保全に係る措置が一面において国民の知る権利等と緊張関係に立ち得ることに留意しつつ、数次にわたる会議において議論を重ねてきた。

本報告書は、これらの議論を踏まえ、我が国の秘密保全法制の在り方について、当会議としての意見を示すものである。

第１　秘密保全法制の必要性・目的

我が国では、外国情報機関等の情報収集活動により、情報が漏えいし、又はそのおそれが生じた事案が従来から発生している。加えて、ＩＴ技術やネットワーク社会の進展に伴い、政府の保有する情報がネットワーク上に流出し、極めて短期間に世界規模で広がる事案が発生している。

我が国の利益を守り、国民の安全を確保するためには、政府が保有する重要な情報の漏えいを防止する制度を整備する必要がある。

また、政府の政策判断が適切に行われるためには、政府部内や外国との間での相互信頼に基づく情報共有の促進が不可欠であり、そのためには、秘密保全に関する制度を法的基盤に基づく確固たるものとすることが重要である。

しかし、秘密保全に関する我が国の現行法令をみると、防衛の分野では、自衛隊法上の防衛秘密や、日米相互防衛援助協定等に伴う秘密保護法（以下「MDA 秘密保護法」という。）上の特別防衛秘密に関する保全制度が

あるが[*1]、必ずしも包括的なものではない上、防衛以外の分野ではそのような法律上の制度がない。また、国家公務員法等において一般的な守秘義務が定められているが、秘密の漏えいを防止するための管理に関する規定がない上、守秘義務規定に係る罰則の懲役刑が１年以下とされており、その抑止力も十分とはいえない。

以上のことを踏まえると、国の利益や国民の安全を確保するとともに、政府の秘密保全体制に対する信頼を確保する観点から、政府が保有する特に秘匿を要する情報の漏えいを防止することを目的として、秘密保全法制を早急に整備すべきである。

第２　秘密の範囲

１　秘密とすべき事項の範囲

ある事項を秘密として厳格な保全措置の対象とすることは、これにより得られる利益がある反面、国の説明責任への影響や行政コストの増大も考えられる。このため、行政機関等が保有する秘密情報の中でも、国の存立にとって重要なもののみを厳格な保全措置の対象とすることが適当である（以下、本法制で厳格な保全措置の対象とする、特に秘匿を要する秘密を便宜的に「特別秘密」と呼ぶこととする。）。

特別秘密として取り扱うべき事項について、防衛秘密の制度を参考としつつ、関係省庁の意見を基に検討すると、

① 国の安全
② 外交
③ 公共の安全及び秩序の維持

の３分野を対象とすることが適当である。

２　事項の限定列挙・秘匿の必要性による絞り込み

前記の３分野のいずれかに属する事項であっても、内容によりその重要度には差異があるところ、特別秘密として厳格な保全措置の対象とする情

---

*1　自衛隊法は、自衛隊についての一定の事項であって公になっていないもののうち、我が国の防衛上特に秘匿することが必要であるものを、防衛大臣が防衛秘密として指定することとしている（同法第96条の２第１項）。

MDA 秘密保護法は、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一定の事項を特別防衛秘密としている（同法第１条第３項）。

報は特に秘匿の必要性が高いものに限られるべきであるから、これらの分野のいずれかに属する事項の中から特別秘密に該当し得る事項を更に限定する必要がある。

そこで、本法制を整備する際には、自衛隊法の防衛秘密の仕組みと同様に、特別秘密に該当し得る事項を別表等であらかじめ具体的に列挙した上で、高度の秘匿の必要性が認められる情報に限定する趣旨が法律上読み取れるように規定しておくことが適当であり、例えば「我が国の防衛上、外交上又は公共の安全及び秩序の維持上特に秘匿することが必要である場合」（自衛隊法第96条の2第1項参照[*2]）、「その漏えいにより国の重大な利益を害するおそれがある場合」などを要件とすることが考えられる。

3　秘密の作成又は取得の主体

特別秘密の範囲を画するに当たっては、事項を絞り込むのみならず、誰が作成・取得した情報を本法制の適用対象とすべきかという観点からの検討が必要である。

(1)　国の行政機関

前記のような本法制の目的に照らし、国の行政機関が作成・取得する情報は当然に本法制の適用対象とすべきである。

(2)　独立行政法人等[*3]

独立行政法人等は、例えば人工衛星の研究開発、大量破壊兵器に転用可能なロケットに係る機微技術の研究開発等に関して、国の安全等に関する情報を作成・取得する例がある。

独立行政法人等が、国と密接な関係を有し、実質的には国の行政の一端を担う公的機関であることを踏まえ、その独立性等にも配慮しつつ、独立行政法人等が作成・取得する情報についても本法制の適用対象に含めることが適当である。

(3)　地方公共団体

地方公共団体については、警察事務において、公共の安全及び秩序の

---

*2　自衛隊法第96条の2第1項（抄）

防衛大臣は、自衛隊についての別表第四に掲げる事項であつて、公になつていないもののうち、我が国の防衛上特に秘匿することが必要であるもの…を防衛秘密として指定するものとする。

*3　国立大学法人については、学問の自由等の観点で私立大学と区別する理由がないことから、後述(4)の大学に含めて考えることが適当である。

維持に関して特に秘匿を要する情報を作成・取得する例がある。

そして、地方公共団体が、国と密接な関係を有しつつ地域における行政を実施する公的機関であることに鑑みると、地方公共団体が作成・取得する情報についても本法制の適用対象に含めることが適当である。

ただし、地方公共団体が通常取り扱う特別秘密は警察事務に関連するものと考えられることから、地方公共団体に対する本法制の適用範囲を都道府県警察に限定することも考えられる。

(4) 民間事業者・大学

前述のとおり、本法制は、政府が保有する特に秘匿を要する情報の漏えいの防止を基本とするが、政府とは直接関係を有しない民間事業者や大学においても、国の安全等に関し保護されるべき情報を作成・取得することがあり得る。

そこで検討すると、

① 民間事業者や大学が作成・取得する情報を本法制の適用対象とすると、経済活動の自由や学問の自由の観点から国家による過度の干渉にもつながりかねないこと

② 民間における情報漏えいに関しては、不正競争防止法において従業員等による営業秘密の開示等に対する処罰を規定していること*4

等に照らし、民間事業者や大学が作成・取得する情報については本法制の適用対象としないことが適当である。

ただし、民間事業者及び大学（以下「民間事業者等」という。）が行政機関等（国の行政機関、地方公共団体及び独立行政法人等をいう。）から事業委託を受ける場合には、当該民間事業者等は、当該事業に関しては委託をした行政機関等と実質的に一体と考えられるから、このような場合に限っては、民間事業者等が作成・取得する情報も本法制の適用

---

*4 不正競争防止法は、営業秘密（秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの）に該当するものについて、これを開示した従業員等に対する処罰を規定している（同法第 21 条第 1 項）。

なお、外国為替及び外国貿易法は、国際的な平和及び安全の維持を妨げることになる特定貨物の特定地域への輸出や特定技術の特定地域での提供を目的とする取引を行う場合には経済産業大臣の許可を受けることを義務付け、違反した場合の罰則を設けている（同法第 25 条第 1 項、第 48 条第 1 項、第 69 条の 6 第 1 項）。

対象とすることが適当である[*5]。

第３　秘密の管理

１　秘密の指定

(1)　指定行為

本法制の対象とする特別秘密については、厳格な保全措置の対象とするものであるから、対象となる範囲を明確に特定することが適当である。このため、標記(標記が困難な場合は通知）による指定を要件とすること、すなわち、特別秘密については、実質秘であることを前提に、要式行為たる指定行為により保全対象たる秘密の外縁を明確化し、その範囲で厳格な管理を行うことが適当である。

(2)　指定権者

各行政機関等が独自に情報の作成・取得を行っている現状にあることや、秘密指定の要否の判断は当該情報の作成・取得の原因となった具体的事務に即して行うことが適当であることに照らすと、秘密指定の権限は、原則として、特別秘密の作成・取得の主体である各行政機関等に付与することとするのが適当である。

また、行政機関等から事業の委託を受けた民間事業者等が作成・取得した情報については、当該委託をした行政機関等が、情報の流出による当該事業への影響等を最も的確に判断できると考えられることから、原則として、当該委託をした行政機関等が秘密指定を行うこととするのが適当である。

(3)　秘密指定の効果

特別秘密の指定がなされた情報は、特別秘密としての取扱いを受けることになる。

具体的には、特別秘密の指定の趣旨に照らし、これを取り扱う者が限定され、必要のない者が当該特別秘密を知得することがないよう、後述のとおり厳重な人的管理及び物的管理が求められることとするのが適当である。

なお、特別秘密の作成・取得の趣旨に照らし、他の行政機関等や民間

---

*5　現行法令上、防衛秘密に係る物件の製造又は役務の提供の委託を受けた民間業者は、防衛秘密の管理体制につき一定の基準に適合する必要があるなどその適切な管理を義務付けられるほか、民間業者が防衛秘密を漏らした場合には防衛省の職員と同じ罰則が適用される。

事業者等との共有が必要な場合には、特別秘密の外部への伝達を認めることが適当である[*6]。

ただし、特別秘密の漏えいを防ぐために、共有先の行政機関等又は民間事業者等において、法令等により特別秘密の適切な管理が確保されていることを前提とすることが適当である。

(4) 他の行政目的等のための秘密の伝達

特別秘密を保有する行政機関等が、その作成・取得の趣旨に照らし伝達が想定されない行政機関等に特別秘密を伝達する必要性を認めるべき場合があると考えられる[*7]。具体的には、許認可、会計検査、捜査等の業務の遂行のための伝達が考えられるが、この場合、伝達先の行政機関等において法令等に基づき特別秘密の管理が確保されていることを前提とすることが適当である。

(5) 指定の解除

高度の秘匿の必要性が認められなくなった特別秘密について、指定を迅速に解除すべきことは当然であり、秘密保全法制に対する国民の理解を得る上でも重要である。このため、本法制の対象となる特別秘密がその要件に該当しなくなった場合には、指定権者において速やかに指定を解除することが適当である。

高度の秘匿の必要性がなくなった情報がなお特別秘密扱いされる弊害を防止するための制度的担保としては、指定の有効期限を定め、一定期間ごとに指定の要否を再検討する機会を設ける更新制が有効な手段のひとつと考えられる。行政実務の実情を踏まえ、その導入の可否を検討すべきである。

(6) 指定の調整等

特別秘密は、その性格上、統一的に指定され、解除されることが必要であるから、国の行政機関の間で特別秘密の指定及び解除についてそごが生じないように、複数の機関で判断が異なる場合の調整の仕組みを整理することが必要である。

また、国の行政機関以外の行政機関等が指定又は解除を行う場合において、国との間でそごが生じないよう、国が一定の関与を行う枠組みを設けることが必要である。

---

*6 自衛隊法上の防衛秘密も、一定の要件の下で防衛省外の者への伝達が認められている。

*7 同一の行政機関等の他の部門に伝達する場合を含む。

2　人的管理

特別秘密を保全するためには、特別秘密を取り扱う者自体の管理を徹底することが重要である。具体的には、以下に述べるとおり、特別秘密を取り扱うにつき適性を有すると認められた者に取り扱わせること、真に必要のある者に限って取り扱わせること、管理責任を明確化すること、及び特別秘密を取り扱う者の保全意識を高めることが必要である。

(1) 適性評価制度

ア　適性評価制度の整備

(ｱ)　適性評価制度とは

特別秘密の取扱者から秘密を漏えいする一般的リスクがあると認められる者をあらかじめ除外する仕組みがあれば、特別秘密が漏えいする可能性を制度的に低減することが可能となる。適性評価制度とは、秘密情報を取り扱わせようとする者（以下「対象者」という。）について、日ごろの行いや取り巻く環境を調査し、対象者自身が秘密を漏えいするリスクや、対象者が外部からの漏えいの働きかけに応ずるリスクの程度を評価することにより秘密情報を取り扱う適性を有するかを判断する制度である。

(ｲ)　諸外国の適性評価制度

このような制度は、米、英、独、仏等の諸外国において、国にとって重大な秘密情報を保全する制度の一部として既に導入・運用されている。その共通点としては

①　法令等により制度が根拠付けられていること

②　対象者は原則として秘密の取扱者全てであり、その中には国の行政機関から事業の委託を受ける民間事業者等の職員も含まれていること

③　実施に当たっては本人の同意を得て本人から調査票等により情報を収集することとし、情報の収集・裏付けのために公私の団体に対して渡航履歴等の照会を行っていること

④　各行政機関の長が実施していること

⑤　評価の結果を本人に通知するとともに、定期的に改めて評価を行っていること

等を挙げることができる。

(ｳ)　我が国の現行制度の課題と法制の必要性

我が国では、「カウンターインテリジェンス機能の強化に関する基本方針」（平成19年8月9日カウンターインテリジェンス推進会

議決定）に基づき、政府統一基準として、平成21年4月から国の行政機関の職員を対象に秘密情報（特別管理秘密）の取扱者に対して適性の評価を実施している。しかし、この制度では、

① 法令上の位置付けが必ずしも明確でないこと

② 国の行政機関の職員のみが対象となっており、国の行政機関からの委託により秘密情報を取り扱う民間事業者等の職員が対象となっていないこと

③ 対象者本人から十分な情報が得られない場合に、適性評価の実施権者（対象者が適性を有していると認める権限がある者をいう。）が公私の団体に照会する権限が明確でないこと

などの課題がある。

適性評価制度を本法制の中で明確に位置付け、必要な規定を設けることは、特別秘密の保全の実効性を高める観点から極めて重要である。

なお、適性評価制度の設計においては、諸外国の先行事例を参考としつつ、我が国の実情に沿うものとするよう十分考慮する必要がある。

イ 適性評価の対象者

行政機関等や民間事業者等において、特別秘密を作成・取得する業務、あるいはその作成・取得の趣旨に従い特別秘密の伝達を受ける業務に従事する者は、特別秘密の取扱いが業務上当然に想定される。また、行政機関等においては、特別秘密の作成・取得の趣旨に照らし特別秘密の取扱いが想定されない業務の遂行のために特別秘密の伝達を受けることがあり得る。いずれの業務についても、特別秘密の重要性にかんがみ、あらかじめ適性評価を実施し、適性を有すると認められた者のみに特別秘密を取り扱わせることが適当である。

その際、常に後述の一連の評価プロセスが全て完了しなければならないこととすると、特別秘密を取り扱う業務の遂行に著しく支障を来す場合があると考えられることから、このような場合には、一連の評価プロセスの完了前に、暫定的に適性を評価し、一定期間に限り特別秘密を取り扱わせることができることとすることが適当である。

ただし、特別秘密を取り扱うことが事前に予測されておらず、かつ、緊急に特別秘密を取り扱わせなければ業務の遂行に著しく支障を来す者については、あらかじめ適性評価を実施することが困難であることから、例外的に適性評価に代替する措置を講じた上、一定期間に限り

特別秘密を取り扱わせることができることとすること等が考えられる。なお、この者に一定期間経過後も特別秘密を取り扱わせることとなる場合における適性評価の要否については、今後検討すべきである。

一方、内閣を組織する内閣総理大臣及び国務大臣にあっては、極めて高度な政治的性格を有する職であることから、適性評価の対象外とすることが考えられる。また、その他特別の任免の要件・手続が採用されている職については、それぞれの職の性格を踏まえ、適性評価の必要性を個別に判断することが適当である[*8]。

ウ　実施権者

国の存立にとって重要な秘密情報として国が特別秘密に指定したものについて、これを厳重な管理に服せしめるのは国の責務と考えられる。この考え方を踏まえ、特別秘密を取り扱う機関の実施権者については以下のとおりとすることが適当である。

(ア)　国の行政機関

国の行政事務が、法令の定める任務・所掌事務について各行政機関ごとに処理されていることを踏まえ、国の行政機関の職員についての適性評価は、原則として各行政機関の長をその実施権者とする。

(イ)　独立行政法人等

独立行政法人等が主務大臣の関与の下で業務を実施していることから、独立行政法人等の職員についての適性評価は、主務大臣を実施権者とする。

(ウ)　都道府県警察

警察事務は、本来、住民の日常生活の安全の確保という地方的性格と国全体の安全等に係る国家的性格とを併せ持つものであり、我が国の警察制度では、都道府県警察に一定の国家的性格を付与している。こうした警察事務の性格と現行警察制度を踏まえ、都道府県警察の職員の適性評価は、警視総監・道府県警察本部長を実施権者とする。

(エ)　民間事業者等

民間事業者等は、行政機関等から事業委託を受けることで特別秘密を取り扱うこととなるため、民間事業者等の職員の適性評価の実施権者は、事業を委託した機関における実施権者とする。

---

*8　米では大統領及び副大統領、英では首相及び大臣、独及び仏では大統領、首相及び大臣について、それぞれ適性評価の対象から除外されている。

エ　評価の観点及び調査事項

秘密漏えいのリスクとの関連が深い、例えば以下の観点から対象者の適性を評価することが考えられる。

① 我が国の不利益となる行動をしないこと。

② 外国情報機関等の情報収集活動に取り込まれる弱点がないこと。

③ 自己管理能力があること又は自己を統制できない状態に陥らないこと。

④ ルールを遵守する意思及び能力があること。

⑤ 情報を保全する意思及び能力があること。

したがって、適性評価においては、上記の観点からの評価に必要な事項を調査する必要があり、具体的な調査事項としては、例えば、①身元（氏名、生年月日、住所、国籍、帰化、本籍、親族、職歴等）、②対日有害活動その他これに類する反社会的活動への関与、③外国への渡航、④犯罪経歴、⑤懲戒処分、⑥信用状態、⑦薬物・アルコールの影響、濫用及び依存、⑧精神状態、⑨秘密情報の取扱いに係る非違、⑩秘密情報の保全が確実に行われることを疑わせる特異な言動、といったものが考えられる。

また、配偶者のように、対象者の身近にあって対象者の行動に影響を与え得る者については、外国への渡航や信用状態等について調査することも考えられる。

オ　調査事項の公開及び評価基準の非公開

適性評価の実施に当たっては、様々な個人情報を取得し、利用する必要があることに鑑み、調査事項を法令上明示し、いかなる個人情報が取り扱われることとなるのかを明らかにすることが、適性評価制度への国民の理解を得る観点から適当である。

一方、評価基準を明らかにすると、漏えいのリスクがあることを不当に隠そうとする者に対抗措置を講ずる機会を与えるおそれがあることから、評価基準は、その性質上、公開にはそぐわないものと考えられる。

カ　プロセス

(ｱ)　対象者の同意と調査票の提出

適性評価では実施権者が対象者の個人情報を調査し、把握する必要があるが、対象者のプライバシーに深く関わる調査となることから、調査については、対象者の同意を得て、調査票の任意の提出を待って手続を開始、進めることが肝要である。

(イ)　対象者への面接

実施権者は、調査票への回答の真偽等を確認するため、必要に応じ、対象者に面接することとすることが適当である。

(ウ)　第三者に対する照会等

調査票や面接における回答の真偽を確認する必要がある場合において、対象者本人から提出を受けた資料では十分な情報が得られないときには、実施権者が金融機関、医療機関その他の公私の団体に調査事項に関して照会する必要があることも考えられるため、実施権者にその権限を付与することが適当である。

また、対象者の日ごろの行い等を調査するため、職場の上司や同僚等の対象者をよく知る者に対して質問する必要がある場合も考えられることから、実施権者にその権限を付与することが適当である。

なお、第三者に対する照会等については、個人情報を手厚く保護するよう配慮する観点や照会先の公私の団体が照会に協力しやすい環境を整備する観点から、慎重を期すため、対象者本人から同意を得て行うことが適当である。

(エ)　適性の判断

適性評価では、対象者による秘密漏えいのリスクの程度を全ての調査事項の調査を通じて総合的に評価する必要があり、適性を有するかどうかは、実施権者の裁量的判断に委ねられるべきものと考えられる。

本制度のこのような性格を踏まえると、実施に当たっては必要に応じて対象者本人から詳細な説明を求めるなど、慎重かつ細心の注意を払うことが必要である。

また、複数の実施権者がそれぞれの裁量的判断により適性評価を行うこととなるため、各実施権者の判断が大きく異なることのないよう、政府において統一的な評価基準を作成してこれを共有することも検討する必要がある。

(オ)　結果の通知

実施権者は、適性評価の結果を対象者に通知することが適当である。

なお、適性を有しないと評価された場合は、支障のない範囲で理由を付して通知することを検討する必要がある。

キ　評価結果の有効期限

評価結果には有効期限を設け、有効期限後も引き続き特別秘密を取

り扱わせる必要があるときは、改めて適性評価を実施しなければならないこととすることが適当である。

ク　適性の見直し

適性評価を実施した後、当該対象者について、その結果を覆すおそれのある事情の存在が疑われる場合には、実施権者は速やかに適性評価を再度実施し、結果に応じて適性の評価を見直すことが適当である。

ケ　関係資料の適切な取扱い

適性評価の実施に当たっては様々な個人情報を取り扱う必要があるところ、実施権者は対象者の個人情報の保護が確実に図られるよう必要かつ適切な措置を講じなければならないことは言をまたない[*9]。

(2)　取扱者の指定

特別秘密が漏えいする可能性を低減させるため、特別秘密を取り扱わせる者は、適性を有すると認めた者の中から、業務上の必要性から真に必要のある者を指定することによって、これらの者に限ることが適当である。

(3)　管理責任体制

特別秘密を取り扱う機関の長は、その職員の中から、特別秘密の取扱いの業務を管理させる取扱管理者等を指名するなどして組織内において適切に役割・責任を分担する体制を構築することが適当である。

(4)　研修

特別秘密を職員に適切に取り扱わせるためには、秘密保全の意識を啓発するとともに、秘密保全に係る個別具体的な手続等に関する知識を習得させる必要があることから、特別秘密を取り扱う機関の長は、特別秘密を取り扱わせる職員に研修を実施することが適当である。

3　物的管理

上記の人的管理の各措置に加え、特別秘密を保全するためには、作成・取得から廃棄・移管までの各段階において、個別具体的な保全措置を日常

---

*9　具体的には、個人情報の保護に係る法令に基づき、1）収集した個人情報を適性評価以外の目的で利用・提供してはならないこと、2）適性を評価するという目的の達成に必要な範囲を超えて個人情報の提供を対象職員に求め、又は公務所その他の公私の団体に照会してはならないこと、3）取り扱う個人情報の漏えいの防止その他の適切な管理のための措置を講ずること、4）個人情報を取り扱うこととなる担当職員に対して、個人情報の安全管理に係る必要かつ適切な監督を行うこと、が必要と考えられる。

的に講ずる必要がある。

具体的には、例えば以下のような事項について保全措置を講じることが適当である。

① 特別秘密に係る文書・図画・物件の作成・取得、運搬・交付、保管・利用、廃棄・移管の手続及び方法

② 特別秘密の保管場所等への携帯型情報通信・記録機器の持込み

③ 特別秘密に係る電子計算機情報の取扱い方法

④ 特別秘密の保全の状況についての検査

第４ 罰則

１ 罰則に関する基本的な考え方

特別秘密の漏えいを防止するためには、前述のとおり厳格な人的管理及び物的管理を行うのみならず、漏えい行為など本来特別秘密を知る立場にない者が特別秘密を知ることにつながる行為について、刑罰をもって臨むことが必要である。

そして、特別秘密の漏えいを防ぐには、その保全状態を保護することが効果的と考えられること、及び処罰の範囲を必要最小限に抑えることが、本法制に対する国民の理解を得る上で重要と考えられることから、特別秘密を現に保全する者、すなわち業務によりこれを取り扱う者による漏えいを処罰し、特別秘密の漏えいを根元から抑止することを基本的な考え方とすることが適当である。

また、法定刑については、上記行為を抑止するとともに、特別秘密の漏えい等という重い罪責に応じた処罰を可能にするような刑を定めることが適当である。

２ 禁止行為

(1) 故意の漏えい行為

処罰すべき行為として、まず、故意に秘密を漏えいする行為が考えられるところ、処罰すべき者の範囲が問題となる。

ア 業務により特別秘密を取り扱う者

業務により特別秘密を取り扱う者は、自己の業務上の権限や地位に基づき特別秘密を知る者で、その業務性に応じた高度の保全義務を負うこととなるから、これらの者による故意の漏えい行為を処罰することが適当である。

ところで、このような者には、特別秘密を取り扱うことを業務とする者、すなわち特別秘密の作成・取得の趣旨に従い特別秘密を取り扱う者[*10]（以下「取扱業務者」という。）と、特別秘密の作成・取得の趣旨に従い特別秘密を取り扱うのではなく、自己の業務の遂行のために必要性が認められて特別秘密の伝達を受け、これを知得する者[*11][*12]（以下「業務知得者」という。）がある。

このうち、業務知得者による特別秘密の漏えい行為について、故意行為であり、かつ特別秘密の秘密性が現実に害される点では取扱業務者による漏えい行為と変わらないし、行政機関等の業務に関して国の重要な秘密の伝達を受ける以上、漏えいした場合には取扱業務者と同等の責任を負うべきとの考えがある。

他方、自衛隊法及びMDA秘密保護法では、国の重要な秘密である防衛秘密ないし特別防衛秘密の漏えいについて、取扱業務者と業務知得者との間で取扱いに差異を設けている[*13]。これは、業務知得者が特別秘密の取扱いそのものを業務とする者ではなく、取扱業務者に比して特別秘密を取り扱う機会も少ないなどの事情に照らし、取扱業務者に対する刑よりも軽い刑を定めるべきとの考え方に立っているものと解されるところ、本法制においても同様に両者の取扱いに差異を設けるべきとの考え方もある。

このように、業務知得者の処罰の程度については両様の考え方があることから、更に検討すべきである。

イ　その他の者

例えば取扱業務者の漏えい行為により特別秘密を知った者など、取扱業務者又は業務知得者以外の者（以下「業務外知得者」という。）

---

*10　防衛秘密の例では、武器の調達等にかかわる防衛省の職員や、同省から武器の製造等の委託を受けた民間事業者の従業員が挙げられる。

*11　例えば、捜査の過程で特別秘密に触れる検察官・警察官や、予算案の作成過程で特別秘密に触れる財務省の担当官が挙げられる。自衛隊法上の防衛秘密制度においても、これらの者は、「防衛秘密を取り扱うことを業務とする者」に該当しないと解されている。

*12　記者が取扱業務者に取材をして特別秘密を知得した場合、記者は自己の業務として取材をしているが、記者は秘密の伝達を受ける業務上の権限や地位を有しておらず、その業務に基づいて秘密を知得したとはいえないから、業務知得者には該当しないと解される。

*13　自衛隊法では、取扱業務者による漏えい行為のみを処罰し、業務知得者による漏えい行為は処罰対象としていない。また、MDA秘密保護法では、取扱業務者による漏えい行為を業務知得者による漏えい行為よりも重く処罰している。

が特別秘密を第三者に漏えいした場合、これを処罰すべきかが問題となる[*14]。

このような行為は、特別秘密をより広範囲に拡散する行為ではあるが、そもそも業務外知得者は業務として特別秘密を取り扱う者ではないため、業務外知得者への伝達の時点で特別秘密は既に保全状態から流出しており、上記行為を処罰しても漏えいの根元からの抑止にはつながらない。また、これを処罰の対象とすると、例えば特別秘密文書をたまたま拾った一般人まで処罰対象になり得るなど処罰対象が広がる上、正当な報道活動も構成要件に該当し得るため報道活動への影響も懸念される。

このため、業務外知得者による漏えい行為については、特別秘密の漏えいを根元から抑止するとの基本的な考え方に基づき、その行為自体を処罰するのではなく、その前段階にある、業務により特別秘密を取り扱う者による漏えい行為の処罰を徹底することが適当である。

(2) 過失の漏えい行為

特別秘密の性格に照らせば、過失による漏えいであっても、国の利益や国民の安全の確保に大きな影響を及ぼすことは、故意による場合と変わりがない。業務により特別秘密を取り扱う者は、その業務に応じ、特別秘密を厳格に保全し漏えいを防ぐ責任を有しているのであるから、漏えいを防ぐ注意義務が認められ、過失による漏えいを処罰することが適当と考えられる[*15]。

他方、業務知得者の過失による漏えい行為については、MDA 秘密保護法では取扱業務者のそれより軽い刑が定められ、また、自衛隊法ではそもそも処罰対象とされていない。さらに、業務知得者には高度の注意義務を認めるべき基礎が十分ではないとの考えや、過失犯を厳格に処罰すれば、当該業務の遂行それ自体よりも特別秘密の管理に業務の重点が移行し、その結果当該業務の遂行に支障を来すおそれがあるとの考えもあり得る。【第１案：このため、業務知得者については処罰の程度につき検討する必要がある。】【第２案：このため、業務知得者の処罰については更に検討する必要がある。】

(3) 特別秘密を取得する行為

---

*14 不正競争防止法第 21 条第 1 項第 7 号は、違法な開示により営業秘密を取得した者による当該営業秘密の使用及び開示を処罰の対象としている。

*15 自衛隊法は、取扱業務者による防衛秘密の過失の漏えいを処罰の対象としている。

特別秘密の漏えいを防ぐには、特別秘密の保全状態からの流出を防ぎ、秘密の漏えいを根元から抑止することが重要であるところ、業務によりこれを取り扱う者、すなわち取扱業務者及び業務知得者による漏えい行為を処罰対象とすることで、特別秘密の保全状態からの流出に最低限の歯止めをかけることは可能である。

しかし、特別秘密の保全状態からの流出には、取扱業務者等による漏えい行為の処罰では抑止できない取得行為を原因とする場合がある。すなわち、

① 財物の窃取、不正アクセス又は特別秘密の管理場所への侵入など、管理を害する行為を手段として特別秘密を直接取得する場合

には、取扱業務者等による漏えい行為が介在しないため、漏えい行為の処罰ではこれを抑止できない。また、

② 欺罔により適法な伝達と誤信させ、あるいは暴行・脅迫によりその反抗を抑圧して、取扱業務者等から特別秘密を取得する場合

には、取扱業務者等に漏えいの故意がないなど、漏えい行為の処罰が困難な場合がある[*16]（以下、上記①②に該当する行為を便宜的に「特定取得行為」という[*17]。）。

特定取得行為を処罰することとすれば、特別秘密の保全にかかわらない一般人を新たに処罰対象とすることとなるため、前述の基本的な考え方からすれば慎重な検討を要する。

しかし、特定取得行為は、犯罪行為や犯罪に至らないまでも社会通念上是認できない行為を手段とするもので、適法な行為との区別は明確であるから、特定取得行為を処罰対象に加えても、正当な取材活動など本来許容されるべき行為が捜査や処罰の対象とされるおそれはないと考えられる。

また、特定取得行為は、特別秘密を保全状態から流出させる点で取扱

---

*16 参考 不正競争防止法第21条第1項（抄）

次の各号のいずれかに該当する者は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。

一 不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為その他の保有者の管理を害する行為をいう。）により、営業秘密を取得した者

*17 秘密を取得する行為について、刑事特別法等では、情報（無形物）の取得を「探知」、文書、物件等（有形物）の取得を「収集」とそれぞれ呼んでいる。

業務者等による漏えい行為と同様の悪質性、危険性が認められる行為であり、その行為が取扱業務者等によるものでないということのみをもって処罰の対象から外されるとすれば、特別秘密の保全を目的とする本法制の趣旨を損ねることになると考えられる。

このため、処罰の範囲を必要最小限に抑えるという基本的な考え方の下でも、特定取得行為を処罰対象とすることには理由がある。

なお、特定取得行為の中には他の犯罪が成立する行為もあるが、特別秘密の保全の観点からは、同行為は取扱業務者等による漏えい行為と同様の悪質性、危険性が認められる行為であるから、本法制において、特定取得行為として処罰対象とすることが適当である。

(4) 未遂行為

故意の漏えい行為の未遂は、特別秘密の漏えいの危険を現実化させる悪質性の高い行為であり、処罰対象とすることが適当である。

また、特定取得行為は漏えい行為と同様に秘密を漏えいさせる高い危険性を有することから、同行為の未遂も処罰することが適当である。

(5) 共謀行為

故意の漏えい行為の共謀は、漏えい行為について共謀者間で具体性、特定性、現実性を持った合意がなされる上、共謀者の一人の意思の変化では犯罪行為の遂行を容易に変更できないこととなり、単独犯における犯行の決意に比べて犯罪実現の危険性が飛躍的に高まるため、特別秘密の保全の重要性に照らせば共謀段階での処罰の必要性が認められる。そこで、他の立法例も考慮し[*18]、漏えい行為の共謀行為を処罰対象とすることが適当である。

また、特定取得行為は漏えい行為と同様に秘密を漏えいさせる高い危険性を有することから、同行為の共謀も処罰することが適当である。

(6) 独立教唆行為及び煽動行為

取扱業務者等に対し、特別秘密を漏えいするよう働きかける行為は、その漏えいの危険を著しく高める行為であって悪質性が高い。他の立法例も考慮すると[*19]、正犯者の実行行為を待つことなく、特別秘密の漏えいの独立教唆及び煽動を処罰対象とすることが適当である。

また、特定取得行為は漏えい行為と同様に秘密を漏えいさせる高い危険性を有することから、同行為の独立教唆及び煽動を処罰することが適

---

*18 自衛隊法は、防衛秘密の漏えいの共謀を処罰の対象としている。

*19 自衛隊法は、防衛秘密の漏えいの独立教唆及び煽動を処罰の対象としている。

当である。

(7)　自首減免規定

刑法第４２条は自首した者に対する刑の任意的減軽を規定しているが、さらに、自首した者に対する必要的な刑の減軽又は免除を規定すれば、現実の漏えいに至る前に自首することを促し、ひいては実害の発生を未然に防ぐことを期待できる。

そこで、いまだ実害が発生していない時点での自首を促し、実害の発生を防止する観点から、他の立法例も考慮し[*20]、漏えい行為及び特定取得行為の未遂及び共謀について、自首による刑の必要的減免規定を置くことが適当である。

(8)　国外犯処罰規定

特別秘密の保全を徹底する観点からは、我が国の領域外における漏えい行為や特定取得行為についても処罰対象とすることが適当である。

そして、特別秘密の漏えい行為等は、日本国外において日本国民のみならず日本国民以外の者によっても敢行され得るところ、漏えい行為等は我が国の重大な利益を害する行為であるから、行為者の国籍を問わず我が国において処罰できるようにすることが適当と考えられる。したがって、特別秘密の漏えい行為等については、刑法第２条の例により、日本国外において罪を犯したすべての者を処罰することとすることが適当である。

３　法定刑

特別秘密の漏えい行為等に対する十分な抑止力を確保し、また、漏えい行為等を敢行した者に対してその罪責に応じた十分な刑罰を科し得るようにするためには、他の立法例を参考にするとともに、罪刑の均衡を前提としつつ、法定刑を相当程度高いものとすることが必要である。

本法制で処罰対象とする漏えい行為等のうち、最も重い刑をもって臨むべき行為は、業務により特別秘密を取り扱う者による故意の漏えい行為、及び特定取得行為と考えられる。そこで、以下、それらの行為に対する法定刑を検討する。

(1)　自由刑について

これまでの検討内容に照らすと、防衛秘密に相当する事項は特別秘密

---

*20　自衛隊法は、防衛秘密の漏えい未遂及び漏えいの共謀につき自首による刑の必要的減免を規定している。

に該当するものと考えられる。そして、防衛秘密の漏えい行為に対する最高刑が懲役５年であることからすれば、本法制における最高刑も懲役５年とすることが考えられる。

しかしながら、立法例を見ると、刑事特別法及びMDA秘密保護法では最高刑が懲役１０年であるほか、不正競争防止法においても営業秘密の開示行為等に対する最高刑は懲役１０年である。さらに、特定取得行為においては窃盗罪（最高刑は懲役１０年）などが手段として敢行されることがあることも考慮すると、本法制における最高刑を懲役１０年とすることも考えられる。

さらに、法定刑を相当程度高いものとする観点からは、懲役刑の下限を設けることも検討に値する。

(2)　罰金刑について

特別秘密の漏えい行為等は、特別秘密が保全状態から流出するという重大な結果を発生させるものであるから、その刑事責任は重く、罰金刑のみを科すことは適当でない[*21]。

他方、これまでに敢行された秘密漏えい事案においては、金銭的対価を伴うものが少なくないことから、この種事案に対する抑止効果の観点からは、懲役刑に加え、相当程度の罰金刑の併科が考えられる。

ただし、金銭的対価を伴わない事案や少額の対価を伴うに過ぎない事案もあること、漏えい等に対する報酬であれば没収・追徴も可能と考えられることを踏まえると、自由刑と罰金刑とは任意的併科とすることが適当と考えられる[*22]。

---

*21　自衛隊法、MDA秘密保護法及び刑事特別法では、最も重い犯罪類型に対しては自由刑のみを規定している。また、国家公務員法では罰金刑（５０万円以下）を選択刑として規定している。

*22　なお、秘密保持の観点からは、特別秘密の漏えい等事件の公判において、特別秘密の内容を公判廷で明らかにしないことが重要であるところ、現在、実務では、確立された立証方法として、いわゆる外形立証が行われている。外形立証とは、争点となっている秘密が実質秘であることを立証するに当たり、①秘密の指定基準（指定権者、指定される秘密の範囲、指定及び解除の手続）が定められていること、②当該秘密が国家機関内部の適正な運用基準に則って指定されていること、③当該秘密の種類、性質、秘扱いをする由縁等を立証することにより、当該秘密が実質秘であることを推認するもので、これにより実務では秘密を守りつつ公判での立証を支障なく行うことができている。

第５　法形式

本法制における特別秘密のうち、外交あるいは公共の安全及び秩序の維持に関する秘密については、国の安全に関する秘密についての自衛隊法のような受け皿となり得る既存の法律は見い出し難い。また、本法制は、国の利益や国民の安全の確保といった観点から特別秘密の漏えいを防止することを目的としており、主に服務規律の維持を目的として守秘義務を定める国家公務員法等とは趣旨が異なるため、国家公務員法等の改正により本法制を実現することは適当ではない。したがって、本法制は新規立法によることとすることが適当である。

その際、運用の統一性や制度の一覧性を確保するという観点から、単一の法制によることとするのが適当である。

なお、防衛秘密及び特別防衛秘密については、いずれも本法制の対象とする秘密との間で秘密として保護する理由に異なるところはないが、他方、ＭＤＡ秘密保護法は、日米相互防衛援助協定等に伴うものという特別な性格を有している。そこで、両者のうち、特別防衛秘密については引き続きＭＤＡ秘密保護法によるものとし、防衛秘密に限って本法制に取り込み、統一的に運用することが適当である[*23]。

第６　国民の知る権利等との関係

国民の知る権利は、健全な民主主義の根幹を支える極めて重要な権利である。

国民が積極的に政府に対してその保有する情報の開示を求める権利としての知る権利に関しては、具体的な権利性を持たない抽象的な権利であるとしながらも、憲法上の権利として認める裁判例が近年出てきている。[*24][*25]。

また、国民の知る権利と報道の自由及び取材の自由との関係について、最高裁は、報道機関の報道が、民主主義社会において国民が国政に関与す

---

*23　日米地位協定の実施に伴う刑事特別法における合衆国軍隊の機密については、同法が米国のために在日米軍の秘密情報を保護するものであり、我が国の存立にとって重要な秘密情報を保護する本法制とは保護法益が異なることから、引き続き同法によることが適当である。

*24　このような裁判例においては、情報の開示を請求するためには具体的な権利性を付与する実定法上の根拠が必要であるとしている。

*25　また、第 177 回通常国会に出された情報公開法の改正案においては、同法の目的規定に国民の「知る権利」が明記されている。

るにつき重要な判断の資料を提供し、国民の知る権利に奉仕するものとして、報道の自由が憲法により保障される旨判示し、また、報道機関の報道が正しい内容を持つための取材の自由についても、憲法の趣旨に照らし十分尊重に値する旨判示している[*26]。

本法制は、国民の知る権利や取材の自由との関係で一定の緊張関係に立ち得ることから、本法制と両者との関係について慎重に検討し、以下のとおり整理したところである。

第一に、国民の知る権利について、その趣旨に鑑みれば、政府はその諸活動に関する情報を国民に提供していくことが望ましい。しかしながら、本法制における特別秘密は、政府の保有する秘密情報の中でも国の存立にとって重要なものであり、秘匿の利益が特に大きいものと考えられることから、特別秘密を厳格な保全措置の下に置き、その秘匿性を維持することをもって、国民の知る権利との関係で問題になるものではないと考えられる。

なお、行政機関が保有する情報の公開に関する法律（以下「情報公開法」という。）は、行政文書の開示を請求する権利を具体的に定めている。本法制において特別秘密として保護される情報を情報公開法に当てはめた場合、特別秘密は国の安全、外交並びに公共の安全及び秩序の維持の分野の秘密情報の中で特に秘匿性が高いものであることから、同法第５条第３号（国の安全等に関する情報）及び第４号（公共の安全等に関する情報）の不開示情報に含まれるものと解される。したがって、本法制は、情報公開法に基づく行政文書の開示に影響を与えるものではないと考えられる。

第二に、取材の自由について、本法制に特別秘密の漏えいの教唆罪や特定取得罪を設けることで、取材の自由が不当に制限されるのではないかとの指摘があり得る。

この点、漏えいの教唆と取材の自由の関係については、最高裁が、取材の手段・方法が刑罰法令に触れる場合や社会観念上是認できない態様のも

---

*26　いわゆる博多駅事件判決（最大決昭44・11・26）。

のである場合には刑罰の対象となる旨判示しており[*27]、このような手段・方法による取材行為が取材の自由を前提としても保護されない反面、正当な取材活動は処罰対象とならないことが判例上確立している。

また、本法制における特定取得罪は、既に述べたとおり、当該行為自体が現行法上の犯罪に該当するか、該当しないまでも社会通念上是認できない行為に限って処罰対象とするものであるから、上記の最高裁の立場に照らすと、取材の自由の下で保護されるべき取材活動を刑罰の対象とするものではないと考えられる。

したがって、漏えいの教唆や特定取得行為を処罰することとしても、取材の自由を不当に制限することにはならないと考えられる。

以上から、本法制は、その趣旨に従って運用されれば、国民の知る権利との関係で問題を生じたり、取材の自由を不当に制限したりするものではないと考えられる。

第７　立法府及び司法府

特別秘密は行政目的で作成・取得されるものであり、立法府及び司法府に対し、行政目的で特別秘密が伝達されることは想定されない。他方、立法府及び司法府がそれぞれの業務上の必要性から特別秘密の伝達を受け、国会議員や裁判官等がそれを知得することが想定し得る[*28]ため、然るべき保全措置が取られることが本来適当である。

---

*27　いわゆる外務省機密漏洩事件では、「取材の手段・方法が贈賄、脅迫、強要等の一般の刑罰法令に触れる行為を伴う場合は勿論、その手段・方法が一般の刑罰法令に触れないものであつても、取材対象者個人としての人格の尊厳を著しく蹂躙する等法秩序全体の精神に照らし社会観念上是認することのできない態様のものである場合にも、正当な取材活動の範囲を逸脱し違法性を帯びるものといわなければならない」と判示されている（最決昭和 53・5・31）。

*28　立法府が国政調査権（憲法第 62 条）の行使として特別秘密の伝達を求めた場合、行政府はこれに応じるか否かを判断することとなるが、これに応じた場合には、国会議員及び国会職員が特別秘密を知得することとなる。また、司法府については、例えば、民事訴訟における原告や刑事訴訟における被告人・弁護人が、特別秘密に係る訴訟で特別秘密についての証拠開示等を求めた場合、裁判所がその必要性を判断するため、国・検察官に対して特別秘密の提示を命じることがあり得るが、このような場合には、裁判官や裁判所職員が特別秘密を知得することとなる。

米、英、独、仏等の諸外国では、行政府から立法府及び司法府に伝達された秘密について、法令や規則等に従った取扱いが求められ、また、当該秘密を知得した者が守秘義務に違反して漏えいした場合には罰則が適用され得ることとなっている。

この点、まず、立法府については、国会議員にはそもそも法律上守秘義務が課せられておらず[*29]、また、憲法上、議院で行った発言について免責特権が認められている。

このようなことに鑑みれば、特別秘密に係る国会議員の守秘義務の在り方を検討するためには、国会議員の活動の在り方も踏まえつつ、立法府における秘密保全の在り方全般と特別秘密の保全の在り方との関係を整理する必要があると考えられる。しかし、このような検討は、行政府とは独立の地位を有する立法府の在り方の根幹に関わることから、立法府に委ねることが適当と考えられる[*30]。

次に、司法府については、裁判官には罰則を伴う守秘義務が設けられていない一方、弾劾裁判及び分限裁判の手続が設けられている[*31]。

特別秘密に係る裁判官の守秘義務の在り方を検討するためには、上記のことも踏まえ、司法府における秘密保全の在り方全般と特別秘密の保全の在り方との関係を整理する必要があると考えられる。しかし、このような検討は、行政府とは独立の地位を有する司法府の在り方に多大な影響を及

---

*29　国会議員の守秘義務に関して、憲法及び国会法に規定されている秘密会において公表しないとされたものを他に漏らした者について、参議院規則では院内の懲罰手続が整備されている（衆議院規則には同様の規定がない）が、国会議員の守秘義務及び秘密漏えい行為に対する罰則を定める法令はない。

*30　国会議員であっても、内閣総理大臣、国務大臣、副大臣及び大臣政務官（以下「大臣等」という。）として特別秘密を取り扱う場合には、行政府の職員として本法制の対象とすることが適当である。自衛隊法においても、大臣等は防衛秘密の取扱業務者に該当し、同法の適用対象とされている。

また、大臣秘書官となる国会議員の秘書についても同様の考え方で対応することが適当である。

*31　裁判官には、官吏服務紀律により職務上知り得た秘密に守秘義務が課されているが、高度な職業倫理に基づく行動ができる又は期待でき、それを担保するものとして弾劾裁判及び分限裁判の手続が設けられていることから、罰則で担保された守秘義務は課されていない（平成16年4月9日の衆議院法務委員会における司法制度改革推進本部事務局長答弁）。

ぼし得るため、司法制度全体への影響を踏まえて別途検討されることが適当と考えられる。

おわりに

特別秘密の漏えいにより国や国民が受ける被害の重大さに鑑みれば、その保全体制の整備は喫緊の課題である。知る権利など国民の権利利益との適切なバランスを確保しつつ守るべき秘密を確実に保全する制度を構築することは、国民の利益の一層の実現に資するものである。

当会議は、早期に法制化することを念頭に検討を進め、本報告書を取りまとめた。今後、この報告書の内容を十分に踏まえ、速やかな法制化が図られることを希望するものである。

［別添１］

本有識者会議の開催経緯・開催経過等

○　秘密保全のための法制の在り方に関する有識者会議委員名簿

○　秘密保全のための法制の在り方に関する有識者会議開催状況

○　政府における情報保全に関する検討委員会の開催について

○　秘密保全のための法制の在り方に関する有識者会議の開催について

秘密保全のための法制の在り方に関する有識者会議
委員名簿

（五十音順　／　○：座長）

○	縣（あがた）　公一郎（こういちろう）	早稲田大学政治経済学術院　教授
	櫻井（さくらい）　敬子（けいこ）	学習院大学法学部　教授
	長谷部（はせべ）　恭男（やすお）	東京大学大学院法学政治学研究科　教授
	藤原（ふじわら）　静雄（しずお）	中央大学法科大学院　教授
	安冨（やすとみ）　潔（きよし）	慶應義塾大学法科大学院　教授

秘密保全のための法制の在り方に関する有識者会議
開催状況

第１回　平成２３年１月５日
秘密保全法制の意義等

第２回　平成２３年２月１８日
秘密の範囲、秘密の管理等

第３回　平成２３年４月８日
秘密の管理等

第４回　平成２３年４月２２日
罰則等

第５回　平成２３年５月１３日
法形式等

第６回　平成２３年６月１０日
報告書（案）について

政府における情報保全に関する検討委員会の開催について

［平成22年12月7日
内閣総理大臣決裁］

1　政府における情報保全に関し、秘密保全に関する法制の在り方及び特に機密性の高い情報を取り扱う政府機関の情報保全システムにおいて必要と考えられる措置について検討するため、政府における情報保全に関する検討委員会（以下「委員会」という。）を開催する。

2　委員会の構成は、次のとおりとする。ただし、委員長は、必要があると認めるときは、委員を追加し、又は関係者に出席を求めることができる。

委員長　内閣官房長官
副委員長　内閣官房副長官
委員　内閣危機管理監
内閣官房副長官補（内政担当）
内閣官房副長官補（外政担当）
内閣官房副長官補（安全保障・危機管理担当）
内閣情報官
警察庁警備局長
公安調査庁次長
外務省国際情報統括官
海上保安庁警備救難監
防衛省防衛政策局長

3　委員会は、必要に応じ、関係行政機関の職員による検討部会を開催することができる。検討部会の構成員は、委員長が指名する。

4　委員会は、必要に応じ、有識者会議を開催することができる。有識者会議の出席者は、委員長が参集を求める。

5　委員会の庶務は、関係行政機関の協力を得て、内閣官房において処理する。

6　前各項に定めるもののほか、委員会の運営に関する事項その他必要な事項は、委員長が定める。

秘密保全のための法制の在り方に関する有識者会議の開催について

［平成２３年１月４日
政府における情報保全に
関する検討委員会委員長決定］

1　開催の趣旨

「政府における情報保全に関する検討委員会の開催について」（平成２２年１２月７日内閣総理大臣決裁）第４項の規定に基づき、政府における情報保全に関する検討委員会（以下「委員会」をいう。）における検討に資するため、各界の有識者から御意見をいただくことを目的として、秘密保全のための法制の在り方に関する有識者会議（以下「会議」という。）を開催する。

2　構成

（１）会議は、別紙に掲げる委員により構成し、委員会の委員長が開催する。
（２）委員会の委員長は、別紙に掲げる委員の中から、会議の座長を依頼する。
（３）座長は、必要に応じ、関係者の出席を求めることができる。

3　その他

会議の庶務は、関係行政機関の協力を得て、内閣官房において処理する。

別紙

秘密保全のための法制の在り方に関する有識者会議の委員

縣 公一郎（あがた こういちろう）	早稲田大学政治経済学術院　教授
櫻井 敬子（さくらい けいこ）	学習院大学法学部　教授
長谷部 恭男（はせべ やすお）	東京大学大学院法学政治学研究科　教授
藤原 靜雄（ふじわら しずお）	筑波大学法科大学院　教授
安冨 潔（やすとみ きよし）	慶應義塾大学法科大学院　教授

（五十音順）

［別添２］
参考資料（事務局作成）

○　主要な情報漏えい事件等の概要

○　諸外国（米、英、独、仏）における適性評価制度（セキュリティ・クリアランス）の概要

○　現行法制の罰則との比較

○　各国の秘密保全法制における罰則の概要（米、英、独、仏）

○　諸外国（米、英、独、仏）の立法府及び司法府における秘密保全

主要な情報漏えい事件等の概要

事件名	検挙年	事案概要	罪名・処分結果等
ボガチョンコフ事件	平成12年	在日ロシア大使館に勤務する海軍武官から工作を受けた海上自衛隊三等海佐が、現金等の報酬を得て、海上自衛隊の秘密資料を提供したもの	○ 自衛隊法違反（懲役10月） ○ 懲戒免職
シェルコノゴフ事件	平成14年	在日ロシア通商代表部員が、現金等の謝礼を対価に、防衛機器販売会社社長（元航空自衛官）に米国製戦闘機用ミサイル等の資料の入手・提供を要求したもの	○ MDA秘密保護法違反（起訴猶予処分）
国防協会事件	平成15年	在日中国大使館駐在武官の工作を受けた日本国防協会役員（元自衛官）が、その求めに応じて防衛関連資料を交付したもの	○ 電磁的公正証書原本不実記録及び不実記録電磁的公正証書原本供用罪（起訴猶予処分）
イージスシステムに係る情報漏えい事件	平成19年	海上自衛隊三等海佐が、イージスシステムに係るデータをコンパクトディスクに記録の上、海上自衛隊の学校教官であった別の三等海佐に送付し、当該データが別の海上自衛官3名に渡り、更に他の自衛官に渡ったもの	○ MDA秘密保護法違反（懲役2年6月・執行猶予4年） ○ 懲戒免職
内閣情報調査室職員による情報漏えい事件	平成20年	在日ロシア大使館書記官から工作を受けた内閣情報調査室職員が、現金等の謝礼を対価に、職務に関して知った情報を同書記官に提供したもの	○ 国家公務員法違反 収賄（起訴猶予処分） ○ 懲戒免職
中国潜水艦の動向に係る情報漏えい事案	平成20年	情報本部所属の一等空佐が、職務上知り得た「中国潜水艦の動向」に関する情報を、防衛秘密に該当する情報を含むことを認識した上で、部外者に口頭により伝達したもの	○ 自衛隊法違反（不起訴処分） ○ 懲戒免職
尖閣沖漁船衝突事件に係る情報漏えい事案	平成22年	神戸海上保安部の海上保安官（巡視艇乗組員）が、中国漁船による巡視船衝突事件に係る捜査資料として石垣海上保安部が作成したビデオ映像をインターネット上に流出させたもの	○ 国家公務員法違反（起訴猶予処分） ○ 停職12か月（辞職）
国際テロ対策に係るデータのインターネット上への掲出事案	平成22年	国際テロ対策に係るデータがインターネット上へ掲出されたもの。当該データには、警察職員が取り扱った蓋然性が高い情報が含まれていると認められた。	（捜査中）

諸外国（米、英、独、仏）における適性評価制度（セキュリティ・クリアランス）の概要

※　以下の記載は、現時点で事務局において把握しているものである。また、取り扱うに当たって適性評価を受けなければならない秘密は、各国で概ね三区分に分かれているところ、そのうち機密性が最も高い区分の秘密を取り扱う際に必要となる適性評価手続について記載している。

1　アメリカ

(1)　根拠

合衆国法典及び行政命令において定められている。

(2)　対象者及び例外

秘密を取り扱う者全てが対象者である。業務遂行上必須の場合、特別に適性評価終了前の暫定的な秘密の取扱いを認めている。また、生命への差し迫った脅威や国土防衛の必要性がある緊急時に、適性評価を受けていない者に対する最小限の秘密の開示を認めている。

ただし、大統領・副大統領は対象外とされているほか、行政以外の分野にある連邦議会議員、連邦最高裁判所裁判官・大統領に任命を受けた連邦裁判所裁判官が対象外とされている。

(3)　実施権者

各連邦官庁が、その構成員及び契約事業者に対して適性評価を行う。

なお、適性評価のための調査については他の連邦官庁の機関（連邦人事局）に委託することが可能である。

(4)　評価の観点

対象者が、国家に対する忠誠心、人格的強靭さ、信用性、正直さ、信頼性、思慮分別、判断力、相反する忠誠及び強要される潜在的可能性からの自由及び情報保全の意思・能力を有しているかを確認する。

なお、評価基準は開示されている。

(5)　調査事項

ア　対象者本人

人定事項（氏名、住所歴、生年月日、国籍（帰化情報）、出生地及び社会保障番号、身体的特徴等）、学歴・職歴・軍歴、テロリズム・政府転覆活動への参加・関与、外国渡航歴・活動歴、逮捕歴、信用状態、民事訴訟歴、薬物への関与・アルコールに係る通院歴、精神状態に係る通院歴、親族（養父母・同居人を含む。）の人定事項、本人をよく知る者（友人、同僚、上司、近隣者等）の連絡先並びに過去の適性評価記録等について本人が調査票に記入するほか、セキュリティ関係の非違歴並びに性的な面における振る舞い等について調査する。

イ　配偶者（同様の事情にある者、前配偶者を含む。）

人定事項（氏名、住所歴、生年月日、国籍（帰化情報）、出生地、社会保障番号等）、婚姻及び離婚の期日及び届出地等について本人が調査票に記入する。

(6)　プロセス

対象者から自発的に提供を受ける調査票、対象者への面接、対象者の個人情報の

照会及び対象者をよく知る者からの聴取により調査事項に係る個人情報を調査・把握する。公私の団体への照会は、対象者が同意する旨の書面の提出を得て行う。

なお、適性評価の結果は対象者に通知され、適性を欠くと判断された場合には、国家安全保障上の利益及び他の法令が許容する限りにおいて包括的かつ詳細に理由を付して通知される。

(7) **有効期間**

５年

(8) **その他**

連邦政府全体での適性評価の約９割を実施する連邦人事局は、スタッフ１万人近くの体制で運営され、年間調査件数は約200万件となっている。

2 イギリス

(1) **根拠**

人的セキュリティと国家安全クリアランスの方針に関する政府声明及びセキュリティ・ポリシーの枠組み（政府統一基準で各省に義務的履行を求めるものとされている。）において定められている。

(2) **対象者及び例外**

秘密を取り扱う者全てが対象者である。

ただし、首相及び大臣（閣外大臣及び政務次官を含む。）は対象外とされているほか、行政以外の分野にある国会議員、裁判官・陪審員が対象外とされている。

(3) **実施権者**

国の各官庁及び警察機関が、その構成員及び契約事業者等に対して適性評価を行う。

なお、適性評価のための調査については国の他の官庁の機関（国防調査庁及び外務省）に委託することが可能である。

(4) **評価の観点**

対象者が、信用性、誠実性、信頼性を有しているかを確認する。

なお、評価基準はその一端が開示されている。

(5) **調査事項**

ア 対象者本人

人定事項（氏名、住所歴、生年月日、国籍（帰化情報）、出生地、旅券番号等）、学歴・職歴・軍歴、スパイ・テロリズム・議会制民主主義転覆活動への参加・関与の有無、外国居住歴、犯罪歴、財務状況、信用状態、薬物への関与・アルコールに係る通院歴、健康状態・精神状態に係る通院歴、親族、同居人及び雇用主の人定事項並びに本人をよく知る者の連絡先等について本人が調査票に記入する。

イ 配偶者（同様の事情にある者、前配偶者を含む。）

人定事項（氏名、住所歴、生年月日、国籍（帰化情報）、出生地等）、外国居住歴、財務状況、信用状態等について対象者本人が調査票に記入する。

(6) **プロセス**

対象者から自発的に提出を受ける調査票、対象者への面接、対象者の個人情報の照会及び対象者をよく知る者等からの聴取のほか、調査事項に係る個人情報を調査

・把握する。公私の団体への照会は、対象者が同意する旨の書面の提出を得て行う。

なお、適性評価の結果は対象者に通知され、適性を欠くと判断された場合には、可能な場合、理由を付して通知される。

(7) **有効期間**

7年（初回は5年）

3 ドイツ

(1) **根拠**

セキュリティ審査法において定められている。

(2) **対象者及び例外**

秘密を取り扱う者全て及びその配偶者（当事者と永久に共同の生活を営む者を含む。）が対象者である。必要に応じて適性評価終了前でも、一段階機密性が低い秘密を取り扱う適性評価手続が終了していれば、暫定的な秘密の取扱いも認めている。

ただし、連邦大統領、連邦首相及び連邦大臣は対象外とされているほか、行政以外の分野にある連邦憲法機関（連邦議会、連邦参議院及び連邦憲法裁判所）の構成員、裁判官等が対象外とされている。

(3) **実施権者**

各連邦官庁が、その構成員及び民間事業者等に対して適性評価を行う。

なお、適性評価のための調査については、他の連邦官庁の機関（連邦憲法擁護庁及び軍防諜局）に委託することが可能である。

(4) **評価の観点**

対象者の信用に疑念がないか、対象者が外国情報機関から圧力をかけられるおそれがないか及び自由で民主的な基本秩序を支持していることに疑いがないかを確認する。

なお、評価基準は開示されていない。

(5) **調査事項（配偶者も対象者と同様の事項について調査票を提出する。）**

人定事項（氏名、住所歴、生年月日、国籍（帰化情報）、出生地及び身分証明書番号等）、学歴・職歴・軍歴、反憲法組織・旧東独情報機関への関与、セキュリティ上懸念される国家への渡航歴・滞在歴及び当該国における近親者の人定事項、継続中の刑事・懲戒手続、信用状態、強制執行措置歴、親族の人定事項、本人をよく知る者の連絡先並びに過去の適性評価等について本人及び配偶者が調査票に記入する。

(6) **プロセス**

対象者から提出を受ける調査票、対象者の個人情報の照会及び対象者をよく知る者等からの聴取のほか、必要な場合には対象者への面接を行い、調査事項に係る個人情報を調査・把握する。調査票の提出と公私の団体への照会は、これらに対象者が同意する旨の書面の提出を得て行う。

なお、適性評価の結果は対象者に通知される。

(7) **有効期間**

10年(全ての対象者について5年ごとに調査票を送付して状況を更新させている。)

4　フランス

(1)　根拠

国防法典及び国防秘密保全に関する政府間通達において定められている。

(2)　対象者及び例外

国防秘密を取り扱う者全てが対象者である。予期せぬ活動、通常の適性評価期間の遵守が不可能な条件で活動に従事することとなった者には、15日以内に可否が決定される仮の適性評価により、６ヶ月を超えない範囲での国防秘密の取扱いを認めている。

ただし、大統領、首相及び大臣は対象外とされているほか、行政以外の分野にある議会の上下両院合同の情報委員会を構成する議員が対象外とされている。また、裁判官は国防秘密を取り扱うことはない（国防秘密指定を解除した上で取り扱うこととなるため）。

(3)　実施権者

首相の委任を受けた者が行う。

なお、国防省に係る者以外の者への適性評価のための調査については、国の他の官庁の機関（内務省中央国内情報局）に委託される。

(4)　評価の観点

対象者が、国防秘密を漏えいする危険性を有していないか、国益を害するような脅し又は圧力にさらされていないかを確認する。

なお、評価基準は開示されていない。

(5)　調査事項

ア　対象者本人

人定事項（氏名、住所歴、生年月日、国籍（帰化情報）、出生地並びに身分証明書番号等）、学業レベル（学位、外国語能力等）、職歴、外国渡航歴及び親族の人定事項等について対象者本人に調査票に記載させ、調査する。

イ　配偶者

対象者本人と同様の事項について対象者本人が調査票に記入する。

(6)　プロセス

対象者から自発的に提出を受ける調査票、対象者の個人情報の照会及び対象者をよく知る者等からの聴取のほか、調査事項に係る個人情報を調査・把握する。

なお、適性評価の結果は対象者に通知される。

(7)　有効期間

最長５年（その職の在任期間中のみ有効）

現行法制の罰則との比較

	本報告書（案） （特別秘密）	自衛隊法 （防衛秘密）	ＭＤＡ秘密保護法 （特別防衛秘密）	刑事特別法 （合衆国軍隊の機密）	国家公務員法
漏えい	○ 業務により特別秘密を取り扱う者 ・ 取扱業務者 ・ 業務知得者 【5年以下／10年以下の懲役】 【罰金刑の任意的併科】	○ 防衛秘密を取り扱うことを業務とする者 【5年以下の懲役】	① 特別防衛秘密を取り扱うことを業務とする者 【10年以下の懲役】 ② 我が国の安全を害する目的 【10年以下の懲役】 ③ ①・②以外の者 【5年以下の懲役】	○ 通常不当な方法によらなければ探知し、又は収集することができないようなものを他人に漏らした者 【10年以下の懲役】	○ 職務上知ることのできた秘密を漏らした者 【1年以下の懲役又は50万円以下の罰金】
過失漏えい	○ 業務により特別秘密を取り扱う者 ・ 取扱業務者 ・ 業務知得者	○ 防衛秘密を取り扱うことを業務とする者 【1年以下の禁錮又は3万円以下の罰金】	④ 特別防衛秘密を取り扱うことを業務とする者 【2年以下の禁錮又は5万円以下の罰金】 ⑤ ④以外で業務により特別防衛秘密を知得・領有した者 【1年以下の禁錮又は3万円以下の罰金】		
取得	○ 管理侵害行為又は詐欺等行為による特別秘密の取得 【特定取得行為】 【5年以下／10年以下の懲役】 【罰金刑の任意的併科】		○ 不当な方法による探知収集 【10年以下の懲役】 ○ 我が国の安全を害すべき用途に供する目的による探知収集 【10年以下の懲役】	○ 不当な方法による探知収集 【10年以下の懲役】 ○ 合衆国軍隊の安全を害すべき用途に供する目的による探知収集 【10年以下の懲役】	
周辺的行為	○ 未遂 （漏えい・特定取得）	○ 未遂 （漏えい）	○ 未遂 （漏えい・探知収集）	○ 未遂 （漏えい・探知収集）	
	○ 共謀 （漏えい・特定取得）	○ 共謀 （漏えい）	○ 陰謀 （漏えい・探知収集）	○ 陰謀 （漏えい・探知収集）	○ 企て （共謀に相当する場合）
	○ 独立教唆 （漏えい・特定取得）	○ 独立教唆 （漏えい）	○ 独立教唆 （漏えい・探知収集）	○ 独立教唆 （漏えい・探知収集）	○ そそのかし
	○ 煽動 （漏えい・特定取得）	○ 煽動 （漏えい）	○ せん動 （漏えい・探知収集）	○ せん動 （漏えい・探知収集）	
					○ 企て（単独犯）・命令・故意の容認・ほう助

各国の秘密保全法制における罰則の概要（米、英、独、仏）

国家秘密の漏えい

米
国防情報の漏えい
【10年以下の自由刑若しくは罰金又はこれらの併科】

英
①防諜・諜報情報、②防衛情報、③国際関係情報、④犯罪を惹起する情報、⑤通信傍受に関する情報等の公務員等による漏えい
【2年（略式手続の場合は6月）以下の自由刑若しくは罰金又はこれらの併科】

独
国家機密の漏えい
【6月以上5年以下の自由刑（犯情の特に重い事案では、1年以上10年以下の自由刑）】
公務員による秘密の漏えい
【5年以下の自由刑又は罰金】

仏
公務員等による国防上の秘密の漏えい
【7年以下の自由刑及び罰金】

加重類型（外国勢力への漏えい等）

米
外国政府への国防情報の漏えい
戦時における、敵への伝達を意図した国防情報の漏えい
【死刑、無期刑又は有期刑（上限なし）】

英
国の治安・利益を損なう目的による、敵に有用な情報の漏えい
【3年以上14年以下の自由刑】

独
国家機密の外国勢力への漏えい
国家機密とはならない秘密の外国勢力への漏えい
【1年以上の自由刑（犯情の特に重い事案では、無期又は5年以上の自由刑）】

仏
国民の基本的利益に関する情報の外国勢力への漏えい
【15年以下の自由刑及び罰金】

諸外国（米、英、独、仏）の立法府及び司法府における秘密保全

※　以下の記載は現時点で事務局において把握しているものである。

（立法府）

1　アメリカ

○　行政府の秘密を取り扱うプログラムを監視する情報委員会[*1]等において行政府から秘密の伝達を受けるところ、当該委員会等に関係する議員、議会職員、議員スタッフが秘密を取り扱うことが想定される。

○　議会に秘密が伝達される場合、通常、委員会の長と行政機関の長は個別の協定又は規則に同意する。

○　適性評価（セキュリティ・クリアランス）について、議員は不要、議会職員及び議員スタッフについては上院では必要である。一方、下院では各委員会ごとの規定によるところ、例えば情報委員会に関係する議会職員及び議員スタッフは必要とされている。

○　国防情報の無権限の開示について、合衆国法典による処罰の対象となる。

2　イギリス

○　議会が政府の秘密を取り扱うことは基本的にはないものの、各特別委員会において行政府の秘密の伝達を受ける可能性があり[*2]、当該委員会に関係する議員、議員補佐官が秘密を取り扱うことが想定される一方、議会職員が秘密を取り扱うことは想定されていない。

○　議会に秘密が伝達される場合、議会は、政府が定める「セキュリティ・ポリシーの枠組み」に基づく秘密保全措置を講じる必要がある。

○　適性評価について、議員は不要、議員補佐官は必要である[*3]。

○　無権限かつ害を及ぼす秘密の開示について、1989年公務秘密法が適用となり、処罰の対象となる。

3　ドイツ

○　連邦議会監視委員会[*4]等において行政府から秘密の伝達を受けることがあるところ、当該委員会に関係する議員、議会職員、議員秘書が秘密を取り扱うことが想定

---

*1　上下各院に設置され、15名以下の上院議員、21名以下の下院議員から構成される。政府のインテリジェンス活動の調査を行い、その諸活動についての報告を受ける。

*2　議会の機関ではないが、情報保安委員会（内閣府職員が事務局を務める）は、上下両院の議員９名で構成され、情報機関の支出、運営及び政策の審査等を任務とする。情報機関の長は、同委員会に対し、機微情報又は担当大臣が非開示決定をしている情報を除き、同委員会から要求された情報を提供する。

*3　議会職員については秘密の取扱いは想定されておらず、その意味で適性評価の対象とはならないが、それとは別に、議会建物内への立入りに係る適性評価を受けることが必要とされている。

*4　特別法に基づき設置され、連邦議員９名で構成される。連邦政府は同委員会に対して活動内容・重要案件等の報告義務があり、同委員会の要求に基づいて情報を提供する。

される。
○　議会に秘密が伝達される場合、連邦議会事務規則に基づいた秘密保全措置が講じられている。
○　適性評価について、議員は不要、議会職員及び議員秘書は必要である。
○　連邦議会議員については連邦議会事務規則、議会職員については連邦公務員法、議員秘書については連邦公務員法あるいは労働契約によって守秘義務が課される。いずれも無権限の秘密の開示については、重要な公益を害する場合、刑法による処罰の対象となる。連邦議員が守秘義務違反に問われるには、委員会の決議及び連邦議会議長の同意が必要とされる。

4　フランス

○　議会情報委員会[*5]に対して行政府から国防秘密が伝達され、議会情報委員会を構成する議員、同議員を補助するために指定を受けた議会職員が秘密を取り扱うことが想定される。
○　国防秘密の伝達を受ける場合、その取り扱いに係る法律及び規則の遵守が求められる。
○　適性評価について、議会情報委員会を構成する議員は不要、右を補助する議会職員は必要である。
○　国防秘密の無権限の開示について刑法による処罰の対象となる。

（司法府）

1　アメリカ

○　秘密が開示される司法手続において行政府の秘密が取り扱われることがあり、上記手続に関係する裁判官、裁判所職員、弁護士が秘密を取り扱うことが想定される。
○　適性評価について裁判官は不要、裁判所職員及び弁護士は必要である。
○　国防情報の無権限の開示について、合衆国法典による処罰の対象となる。

2　イギリス

○　1989年公務秘密法に基づく訴追など、秘密が開示される司法手続において行政府の秘密が取り扱われることがあり[*6]、上記手続に関係する裁判官、裁判所職員、弁護士等（法廷弁護人・特別代弁人・その他の法的代理人）が秘密を取り扱うことが想定される。
○　適性評価について、裁判官は不要、裁判所職員及び弁護士等は必要である。
○　無権限かつ害を及ぼす秘密の開示について、1989年公務秘密法が適用となり、処罰の対象となる。

3　ドイツ

---

*5　2007年に新設された上下両院合同の委員会で、上下両院議員各４名で構成される。情報機関の一般的な活動及び会計・組織を精査することを任務とする。

*6　この他に、裁判官は、政府によって特別に任命される役職（例：通信傍受に関する不服申し立てを取り扱う行政審判所の所長）等に関し、秘密を取り扱うことがある。

○　民事・刑事裁判手続等において、行政府の秘密が取り扱われることがあり、上記手続に関係する裁判官、裁判所職員、弁護士が秘密を取り扱うことが想定される。
○　適性評価について、裁判官及び弁護士[*7]は不要、裁判所職員は必要である。
○　裁判官及び裁判所職員は、無権限の秘密の開示について、重要な公益を害する場合、刑法による処罰の対象となる。弁護士は秘密を開示しない旨の誓約書に署名した場合は同様に刑法による処罰の対象となる。

4　フランス

○　行政府からの秘密の伝達は想定されない。
（司法府が国防秘密の伝達を要請する場合、主務大臣は国防秘密の指定の解除につき判断し、解除が認められたもののみ司法府に伝達される。）

---

*7　弁護士は適性評価の対象とされていないが、秘密を開示しないことを誓約する文書への署名が求められる。

［別添３］
関係法令

○　国家公務員法（抄）

○　自衛隊法（抄）

○　自衛隊法施行令（抄）

○　日米相互防衛援助協定等に伴う秘密保護法（抄）

○　日米相互防衛援助協定等に伴う秘密保護法施行令（抄）

○　日本国とアメリカ合衆国との間の相互防衛援助協定（抄）

○　日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法（抄）

○　日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定（抄）

○国家公務員法（昭和22年法律第120号）（抄）

（秘密を守る義務）

第百条　職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。

②～⑤　（略）

第百九条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

一～十一　（略）

十二　第百条第一項若しくは第二項又は第百六条の十二第一項の規定に違反して秘密を漏らした者

十三～十八　（略）

第百十一条　第百九条第二号より第四号まで及び第十二号又は前条第一項第一号、第三号から第七号まで、第九号から第十五号まで、第十八号及び第二十号に掲げる行為を企て、命じ、故意にこれを容認し、そそのかし又はそのほう助をした者は、それぞれ各本条の刑に処する。

○自衛隊法（昭和29年法律第165号）（抄）

（防衛秘密）

第九十六条の二　防衛大臣は、自衛隊についての別表第四に掲げる事項であつて、公になつていないもののうち、我が国の防衛上特に秘匿することが必要であるもの（日米相互防衛援助協定等に伴う秘密保護法（昭和二十九年法律第百六十六号）第一条第三項に規定する特別防衛秘密に該当するものを除く。）を防衛秘密として指定するものとする。

2　前項の規定による指定は、次の各号のいずれかに掲げる方法により行わなければならない。

一　政令で定めるところにより、前項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に標記を付すこと。

二　前項に規定する事項の性質上前号の規定によることが困難である場合において、政令で定めるところにより、当該事項が同項の規定の適用を受けることとなる旨を当該事項を取り扱う者に通知すること。

3　防衛大臣は、自衛隊の任務遂行上特段の必要がある場合に限り、国の行政機関の職員のうち防衛に関連する職務に従事する者又は防衛省との契約に基づき防衛秘密に係る物件の製造若しくは役務の提供を業とする者に、政令で定めるところにより、防衛秘密の取扱いの業務を行わせることができる。

4　防衛大臣は、第一項及び第二項に定めるもののほか、政令で定めるところにより、第一項に規定する事項の保護上必要な措置を講ずるものとする。

第百二十二条　防衛秘密を取り扱うことを業務とする者がその業務により知得した防衛秘密を漏らしたときは、五年以下の懲役に処する。防衛秘密を取り扱うことを業務としなくなつた後においても、同様とする。

2　前項の未遂罪は、罰する。

3　過失により、第一項の罪を犯した者は、一年以下の禁錮又は三万円以下の罰金に処する。

4　第一項に規定する行為の遂行を共謀し、教唆し、又は煽動した者は、三年以下の懲役に処する。

5　第二項の罪を犯した者又は前項の罪を犯した者のうち第一項に規定する行為の遂行を共謀したものが自首したときは、その刑を減軽し、又は免除する。

6　第一項から第四項までの罪は、刑法第三条の例に従う。

別表第四　（第九十六条の二関係）

一　自衛隊の運用又はこれに関する見積り若しくは計画若しくは研究

二　防衛に関し収集した電波情報、画像情報その他の重要な情報

三　前号に掲げる情報の収集整理又はその能力

四　防衛力の整備に関する見積り若しくは計画又は研究

五　武器、弾薬、航空機その他の防衛の用に供する物（船舶を含む。第八号及び第九号において同じ。）の種類又は数量

六　防衛の用に供する通信網の構成又は通信の方法

七　防衛の用に供する暗号

八　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの仕様、性能又は使用方法

九　武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの製作、検査、修理又は試験の方法

十　防衛の用に供する施設の設計、性能又は内部の用途（第六号に掲げるものを除く。）

○自衛隊法施行令（昭和29年政令第179号）（抄）

（標記の方法）

第百十三条の二　法第九十六条の二第二項第一号の規定による標記は、別表第十一に掲げる様式に従い、同条第一項に規定する事項を記録する文書、図画若しくは物件又は当該事項を化体する物件の見やすい箇所に、印刷、押印又は刻印その他これらに準ずる確実な方法により付さなければならない。この場合において、当該文書、図画又は物件のうち同項に規定する事項を記録し、又は化体する部分を容易に区分することができるときは、当該標記は、当該部分に付さなければならない。

（通知の方法）

第百十三条の三　法第九十六条の二第二項第二号の規定による通知は、同条第一項に規定する事項を特定して記載した書面により行わなければならない。

（他の行政機関における防衛秘密の取扱いの業務）

第百十三条の四　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する職務に従事する者に防衛秘密の取扱いの業務を行わせるときは、次に掲げる事項について、あらかじめ、当該行政機関の長と協議するものとする。

一　防衛秘密の取扱いの業務を管理する者の指名に関すること。

二　防衛秘密の取扱いの業務に従事する職員の範囲の指定に関すること。

三　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

四　防衛秘密の伝達（文書、図画又は物件の交付以外の方法によるものに限る。以下この節において同じ。）の手続に関すること。

五　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

六　当該行政機関以外の者への防衛秘密の提供の制限に関すること。

七　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

八　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（契約業者における防衛秘密の取扱いの業務）

第百十三条の五　防衛省との契約に基づき防衛秘密に係る物件の製造又は役務の提供を業とする者（次項及び第百十三条の十一において「契約業者」という。）は、次に掲げる基準に適合していなければならない。

一　防衛秘密の保護上必要な措置に関し役員及び職員が遵守すべき規則を定めていること。

二　防衛秘密の取扱いの業務を管理する者を選任していること。

三　防衛秘密の取扱いの業務に従事する役員及び職員に防衛秘密の保護上必要な措置に

関する教育を行つていること。

四　防衛秘密に係る文書、図画又は物件を保管するための施設設備その他防衛秘密の保護上必要な施設設備を設置していること。

2　契約業者との契約においては、次に掲げる事項を定めなければならない。

一　防衛秘密の取扱いの業務に従事する役員及び職員の範囲の指定に関すること。

二　防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱いの手続に関すること。

三　防衛秘密の伝達の手続に関すること。

四　防衛秘密の取扱いの業務の状況の検査の実施に関すること。

五　当該契約業者以外の者への防衛秘密の提供の制限に関すること。

六　防衛秘密の漏えいその他の事故が生じた場合の措置に関すること。

七　前各号に掲げるもののほか、防衛秘密の保護上必要な措置に関すること。

（防衛秘密管理者）

第百十三条の六　防衛大臣は、防衛省の職員のうちから、防衛秘密の取扱いの業務を管理する者（以下この節において「防衛秘密管理者」という。）を指名するものとする。

（防衛秘密の指定に伴う措置）

第百十三条の七　防衛大臣は、法第九十六条の二第一項に規定する事項を防衛秘密として指定したときは、指定に関する記録を作成するとともに、防衛秘密として指定した事項を当該事項に係る防衛秘密管理者に通報するものとする。

（防衛秘密の表示）

第百十三条の八　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定された場合において、第百十三条の二の規定により標記が付されたもの以外に当該防衛秘密として指定された事項を記録する文書、図画若しくは物件又は当該事項を化体する物件があるときは、当該文書、図画又は物件に、同条の規定の例により、防衛秘密の表示をする措置を講じなければならない。ただし、当該物件の性質上表示をすることが困難である場合は、この限りでない。

（防衛秘密の周知）

第百十三条の九　防衛秘密管理者は、法第九十六条の二第一項に規定する事項が防衛秘密として指定されたときは、当該事項の取扱いの業務に従事する防衛省の職員にその旨を周知させなければならない。

（職員の範囲の指定）

第百十三条の十　防衛秘密の取扱いの業務に従事する防衛省の職員の範囲は、防衛秘密管理者が定める。

（他の行政機関等における防衛秘密の取扱いの業務に伴う措置）

第百十三条の十一　防衛大臣は、防衛省以外の国の行政機関の職員のうち防衛に関連する職務に従事する者又は契約業者に防衛秘密の取扱いの業務を行わせるときは、防衛秘密管理者に防衛秘密に係る文書、図画若しくは物件を交付させ、又は防衛秘密を伝達させるものとする。

2　前項の交付又は伝達は、防衛秘密として指定された事項を特定して行うものとする。

（防衛秘密が要件を欠くに至つた場合の措置）

第百十三条の十二　防衛大臣は、防衛秘密として指定した事項が法第九十六条の二第一項に規定する要件を欠くに至つたときは、速やかに、当該事項に係る防衛秘密管理者に当該事項が防衛秘密でなくなつた旨を通報するものとする。

2　前項の通報を受けた防衛秘密管理者は、直ちに、当該通報に係る事項を記録する文書、図画若しくは物件又は当該事項を化体する物件に付された第百十三条の二の規定による標記及び第百十三条の八の規定による表示を抹消する措置を講ずるとともに、当該事項の取扱いの業務に従事する防衛省の職員及び前条第一項の規定により当該事項に係る文書、図画若しくは物件を交付し、又は当該事項を伝達した相手方に当該事項が防衛秘密でなくなつた旨を周知させなければならない。

（防衛秘密の取扱いの管理のための措置）

第百十三条の十三　防衛秘密管理者は、第百十三条の八から前条までに規定するもののほか、防衛大臣の定めるところにより、防衛秘密に係る文書、図画又は物件の作成、運搬、交付、保管、廃棄その他の取扱い及び防衛秘密の伝達を適切に管理するための措置を講じなければならない。

（委任規定）

第百十三条の十四　この節に規定するもののほか、防衛秘密の保護上必要な措置に関する細目は、防衛大臣が定める。

○日米相互防衛援助協定等に伴う秘密保護法（昭和29年法律第166号）（抄）

（定義）

第一条　この法律において「日米相互防衛援助協定等」とは、日本国とアメリカ合衆国との間の相互防衛援助協定、日本国とアメリカ合衆国との間の船舶貸借協定及び日本国に対する合衆国艦艇の貸与に関する協定をいう。

2　この法律において「装備品等」とは、船舶、航空機、武器、弾薬その他の装備品及び資材をいう。

3　この法律において「特別防衛秘密」とは、左に掲げる事項及びこれらの事項に係る文書、図画又は物件で、公になつていないものをいう。

一　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された装備品等について左に掲げる事項

イ　構造又は性能

ロ　製作、保管又は修理に関する技術

ハ　使用の方法

ニ　品目及び数量

二　日米相互防衛援助協定等に基き、アメリカ合衆国政府から供与された情報で、装備品等に関する前号イからハまでに掲げる事項に関するもの

（特別防衛秘密保護上の措置）

第二条　特別防衛秘密を取り扱う国の行政機関の長は、政令で定めるところにより、特別防衛秘密について、標記を附し、関係者に通知する等特別防衛秘密の保護上必要な措置を講ずるものとする。

（罰則）

第三条　左の各号の一に該当する者は、十年以下の懲役に処する。

一　わが国の安全を害すべき用途に供する目的をもつて、又は不当な方法で、特別防衛秘密を探知し、又は収集した者

二　わが国の安全を害する目的をもつて、特別防衛秘密を他人に漏らした者

三　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を他人に漏らしたもの

2　前項第二号又は第三号に該当する者を除き、特別防衛秘密を他人に漏らした者は、五年以下の懲役に処する。

3　前二項の未遂罪は、罰する。

第四条　特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らしたものは、二年以下の禁こ又は五万円以下の罰金に処する。

2　前項に掲げる者を除き、業務により知得し、又は領有した特別防衛秘密を過失により他人に漏らした者は、一年以下の禁こ又は三万円以下の罰金に処する。

第五条　第三条第一項の罪の陰謀をした者は、五年以下の懲役に処する。

2　第三条第二項の罪の陰謀をした者は、三年以下の懲役に処する。

3　第三条第一項の罪を犯すことを教唆し、又はせん動した者は、第一項と同様とし、同

条第二項の罪を犯すことを教唆し、又はせん動した者は、前項と同様とする。

4　前項の規定は、教唆された者が教唆に係る犯罪を実行した場合において、刑法（明治四十年法律第四十五号）総則に定める教唆の規定の適用を排除するものではない。

（自首減免）

第六条　第三条第一項第一号若しくは第三項又は前条第一項若しくは第二項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

（この法律の解釈適用）

第七条　この法律の適用にあたつては、これを拡張して解釈して、国民の基本的人権を不当に侵害するようなことがあつてはならない。

○日米相互防衛援助協定等に伴う秘密保護法施行令（昭和29年政令第149号）（抄）

（秘密区分）

第一条　日米相互防衛援助協定等に伴う秘密保護法第一条第三項に規定する特別防衛秘密は、その秘密の保護の必要度に応じて、機密、極秘又は秘のいずれかに区分しなければならない。

2　前項の「機密」とは、秘密の保護が最高度に必要であつて、その漏えいが我が国の安全に対し、特に重大な損害を与えるおそれのあるものをいう。

3　第一項の「極秘」とは、秘密の保護が高度に必要であつて、その漏えいが我が国の安全に対し、重大な損害を与えるおそれのあるものをいう。

4　第一項の「秘」とは、秘密の保護が必要であつて、機密及び極秘に該当しないものをいう。

（秘密区分の指定、変更及び解除）

第二条　国の行政機関（内閣府並びに内閣府設置法（平成十一年法律第八十九号）第四十九条第一項及び第二項に規定する機関並びに国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関をいう。以下同じ。）の長（以下「各省庁の長」という。）で、アメリカ合衆国政府から特別防衛秘密に属する事項又は文書、図画若しくは物件の供与を受けたものは、その特別防衛秘密につき、前条に規定する秘密区分の指定を行わなければならない。

2　前項の国の行政機関の長は、同項の規定により指定した秘密区分を変更することができる。

3　第一項の国の行政機関の長は、特別防衛秘密として秘匿する必要がなくなつたとき、又は公になつたものがあるときは、その部分に限り、速やかに、秘密区分の指定を解除しなければならない。

4　第一項の国の行政機関の長は、特別防衛秘密について、前三項の規定により秘密区分を指定し、変更し、又は解除したときは、必要に応じ、その旨を関係行政機関に通知しなければならない。

（標記）

第三条　各省庁の長は、その取り扱う特別防衛秘密に属する文書、図画又は物件につき、これらが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨

の標記をしなければならない。

2　各省庁の長は、前条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、速やかに、前項の標記を変更し、又は抹消しなければならない。

3　第一項の標記の様式は、別記様式のとおりとする。

（通知）

第四条　各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図画若しくは物件であつて、前条の規定による標記ができないもの若しくは標記をすることが適当でないものについては、関係者に対し、文書又は口頭により、これが特別防衛秘密に属し、かつ、機密、極秘又は秘のいずれかに区分されている旨の通知をしなければならない。

2　各省庁の長は、第二条第二項若しくは第三項の規定により秘密区分を変更し、若しくは解除し、又は同条第四項の規定による秘密区分の変更若しくは解除の通知を受けたときは、必要に応じ、速やかに、その旨を関係者に対し、文書により、通知しなければならない。

（掲示）

第五条　各省庁の長は、その管理する施設内にある特別防衛秘密に属する物件について、必要があるときは、その物件に近接してはならない旨の掲示を行うものとする。

（委託中における特別防衛秘密保護上の措置）

第六条　各省庁の長は、その取り扱う特別防衛秘密を製作、修理、実験、調査研究、複製等のため政府機関以外の者に委託する場合は、委託中における秘密の漏えいの危険を防止するため、契約条項に秘密保持に関する規定を設ける等必要な措置を講じなければならない。

（特別防衛秘密保護上の措置の実施細目）

第七条　第二条から前条までに規定するもののほか、各省庁の長は、その取り扱う特別防衛秘密に属する事項又は特別防衛秘密に属する文書、図面若しくは物件の複製、送達、伝達、接受、保管、破棄等その取扱いに関し、特別防衛秘密の保護上必要な措置を講じなければならない。

1　前項に規定する特別防衛秘密の保護上必要な措置の実施細目については、各省庁の長が定める。

（注）日本国とアメリカ合衆国との間の相互防衛援助協定（抄）

第三条

1　各政府は、この協定に従つて他方の政府が供与する秘密の物件、役務又は情報についてその秘密の漏せつ又はその危険を防止するため、両政府の間で合意する秘密保持の措置を執るものとする。

2　（略）

○日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法（昭和27年法律第138号）（抄）

（定義）

第一条　この法律において「協定」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定をいう。

2　この法律において「合衆国軍隊」とは、日本国とアメリカ合衆国との間の相互協力及び安全保障条約に基づき日本国にあるアメリカ合衆国の陸軍、空軍及び海軍をいう。

3　この法律において「合衆国軍隊の構成員」、「軍属」又は「家族」とは、協定第一条に規定する合衆国軍隊の構成員、軍属又は家族をいう。

（合衆国軍隊の機密を侵す罪）

第六条　合衆国軍隊の機密（合衆国軍隊についての別表に掲げる事項及びこれらの事項に係る文書、図画若しくは物件で、公になつていないものをいう。以下同じ。）を、合衆国軍隊の安全を害すべき用途に供する目的をもつて、又は不当な方法で、探知し、又は収集した者は、十年以下の懲役に処する。

2　合衆国軍隊の機密で、通常不当な方法によらなければ探知し、又は収集することができないようなものを他人に漏らした者も、前項と同様とする。

3　前二項の未遂罪は、罰する。

第七条　前条第一項又は第二項の罪の陰謀をした者は、五年以下の懲役に処する。

2　前条第一項又は第二項の罪を犯すことを教唆し、又はせん動した者も、前項と同様とする。

3　前項の規定は、教唆された者が、教唆に係る犯罪を実行した場合において、刑法総則に定める教唆の規定の適用を排除するものではない。

第八条　第六条第一項の罪、同項に係る同条第三項の罪又は同条第一項に係る前条第一項の罪を犯した者が自首したときは、その刑を減軽し、又は免除する。

別表

一　防衛に関する事項

イ　防衛の方針若しくは計画の内容又はその実施の状況

ロ　部隊の隷属系統、部隊数、部隊の兵員数又は部隊の装備

ハ　部隊の任務、配備又は行動

ニ　部隊の使用する軍事施設の位置、構成、設備、性能又は強度

ホ　部隊の使用する艦船、航空機、兵器、弾薬その他の軍需品の種類又は数量

二　編制又は装備に関する事項

イ　編制若しくは装備に関する計画の内容又はその実施の状況

ロ　編制又は装備の現況

ハ　艦船、航空機、兵器、弾薬その他の軍需品の構造又は性能

三　運輸又は通信に関する事項

イ　軍事輸送の計画の内容又はその実施の状況

ロ　軍用通信の内容
ハ　軍用暗号

（注）日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定【日米地位協定】（抄）

第二十三条

（前略）　日本国政府は、その領域において合衆国政府の設備、備品、財産、記録及び公務上の情報の十分な安全及び保護を確保するため、並びに適用されるべき日本国の法令に基づいて犯人を罰するため、必要な立法を求め、及び必要なその他の措置を執ることに同意する。

はじめに

当会議は、本年１月、政府における情報保全に関する検討委員会から、我が国における秘密保全のための法制の在り方について意見を示すよう要請を受けた。

我が国では、近年、国民主権の理念の下、情報公開法制の整備をはじめ、行政の透明性の確保のための取組について積極的な検討がなされ、一定の成果を上げてきた。同時に、我が国を取り巻く厳しい国際情勢の下で国及び国民の利益を守るためには、政府による秘密保全を徹底することが極めて重要であり、当会議は、政府による秘密保全に係る措置~~の徹底~~が一面において国民の知る権利等と緊張関係に立ち得ることに留意しつつ、数次にわたる会議において議論を重ねてきた。

本報告書は、これらの議論を踏まえ、我が国の秘密保全法制の在り方について、当会議としての意見を示すものである。

第１　秘密保全法制の必要性・目的

我が国では、外国情報機関等の情報収集活動により、情報が漏えいし、又はそのおそれが生じた事案が従来から発生している。加えて、ＩＴ技術やネットワーク社会の進展に伴い、政府の保有する情報がネットワーク上に流出し、極めて短期間に世界規模で広がる事案が発生している。

我が国の利益を守り、国民の安全を確保するためには、政府が保有する重要な情報の漏えいを防止する制度を整備~~確立~~する必要がある。

また、政府の政策判断が適切に行われるためには、政府部内や外国との間での相互信頼に基づく情報共有の促進が不可欠であり、そのためには、秘密保全に関する制度を法的基盤に基づく確固たるものとすることが重要である。

しかし、秘密保全に関する我が国の現行法令をみると、防衛の分野では、自衛隊法上の防衛秘密や、日米相互防衛援助協定等に伴う秘密保護法（以下「MDA 秘密保護法」という。）上の特別防衛秘密に関する保全制度があるが[*1]、必ずしも包括的なものではない上、防衛以外の分野ではそのよ

---

*1　自衛隊法は、自衛隊についての一定の事項であって公になっていないもののうち、我が国の防衛上特に秘匿することが必要であるものを、防衛大臣が防衛秘密として指定することとしている（同法第 96 条の 2 第 1 項）。

MDA 秘密保護法は、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一定の事項を特別防衛秘密としている（同法第 1 条第 3 項）。

うな法律上の制度がない。また、国家公務員法等において一般的な守秘義務が定められているが、秘密の漏えいを防止するための管理に関する規定がない上、守秘義務規定に係る罰則の懲役刑が１年以下とされており、その抑止力も十分とはいえない。

以上のことを踏まえると、国の利益や国民の安全を確保するとともに、政府の秘密保全体制に対する信頼を確保する観点から、政府が保有する特に秘匿を要する情報の漏えいを防止することを目的として、秘密保全法制を早急に整備すべきである。

第２　秘密の範囲

１　秘密とすべき事項の範囲

ある事項を秘密として厳格な保全措置の対象とすることは、これにより得られる利益がある反面、国の説明責任への影響や行政コストの増大も考えられる。このため、行政機関等が保有する秘密情報の中でも、国の存立にとって重要なもののみを厳格な保全措置の対象とすることが適当である（以下、本法制で厳格な保全措置の対象とする、特に秘匿を要する秘密を便宜的に「特別秘密」と呼ぶこととする。）。

特別秘密として取り扱うべき事項について、防衛秘密の制度を参考としつつ、関係省庁の意見を基に検討すると、

①　国の安全

②　外交

③　公共の安全及び秩序の維持

の３分野を対象とすることが適当である。

２　事項の限定列挙・秘匿の必要性による絞り込み

前記の３分野のいずれかに属する事項であっても、内容によりその重要度には差異があるところ、特別秘密として厳格な保全措置の対象とする情報は特に秘匿の必要性が高いものに限られるべきであるから、これらの分野のいずれかに属する事項の中から特別秘密に該当し得る事項を更に限定する必要がある。

そこで、本法制を整備する際には、自衛隊法の防衛秘密の仕組みと同様に、特別秘密に該当し得る事項を別表等であらかじめ~~に~~具体的に~~かつ明確な事項を~~列挙した上で~~するとともに~~、高度の秘匿の必要性が認められる情報に限定する趣旨が法律上読み取れるように規定しておくことが適当であ

り、例えば「我が国の防衛上、外交上又は公共の安全及び秩序の維持上特に秘匿することが必要である場合」（自衛隊法第96条の2第1項参照[*2]）、「その漏えいにより国の重大な利益を害するおそれがある場合」など、~~秘匿の必要性が特に高いこと~~を要件とすることが考えられる~~適当である~~。

3　秘密の作成又は取得の主体

特別秘密の範囲を画するに当たっては、事項を絞り込むのみならず、誰が作成・取得した情報を本法制の適用対象とすべきかという観点からの検討が必要である。

(1)　国の行政機関

前記のような本法制の目的に照らし、国の行政機関が作成・取得する情報は当然に本法制の適用対象とすべきである。

(2)　独立行政法人等[*3]

独立行政法人等は、例えば人工衛星の研究開発、大量破壊兵器に転用可能なロケットに係る機微技術の研究開発等に関して、国の安全等に関する情報を作成・取得する例がある。

独立行政法人等が、国と密接な関係を有し、実質的には国の行政の一端を担う公的機関であることを踏まえ、その独立性等にも配慮しつつ、独立行政法人等が作成・取得する情報についても本法制の適用対象に含めることが適当である。

(3)　地方公共団体

地方公共団体については、警察事務において、公共の安全及び秩序の維持に関して特に秘匿を要する情報を作成・取得する例がある。

そして、地方公共団体が、国と密接な関係を有しつつ地域における行政を実施する公的機関であることに鑑みると、地方公共団体が作成・取得する情報についても本法制の適用対象に含めることが適当である。

ただし、地方公共団体が通常取り扱う特別秘密は警察事務に関連するものと考えられることから、地方公共団体に対する本法制の適用範囲を

---

*2　自衛隊法第96条の2第1項（抄）

防衛大臣は、自衛隊についての別表第四に掲げる事項であつて、公になつていないもののうち、我が国の防衛上特に秘匿することが必要であるもの…を防衛秘密として指定するものとする。

*3　国立大学法人については、学問の自由等の観点で私立大学と区別する理由がないことから、後述(4)の大学に含めて考えることが適当である。

都道府県警察に限定することも考えられる。

(4)　民間事業者・大学

前述のとおり、本法制は、政府が保有する特に秘匿を要する情報の漏えいの防止を基本とするが、政府とは直接関係を有しない民間事業者や大学においても、国の安全等に関し保護されるべき情報を作成・取得することがあり得る。

そこで検討すると、

①　民間事業者や大学が作成・取得する情報を本法制の適用対象とすると、経済活動の自由や学問の自由の観点から国家による過度の干渉にもつながりかねないこと

②　民間における情報漏えいに関しては、不正競争防止法において従業員等による営業秘密の開示等に対する処罰を規定していること[*4]等に照らし、民間事業者や大学が作成・取得する情報については本法制の適用対象としないことが適当である。

ただし、民間事業者及び大学（以下「民間事業者等」という。）が行政機関等（国の行政機関、地方公共団体及び独立行政法人等をいう。）から事業委託を受ける場合には、当該民間事業者等は、当該事業に関しては委託をした行政機関等と実質的に一体と考えられるから、このような場合に限っては、民間事業者等が作成・取得する情報も本法制の適用対象とすることが適当である[*5]。

第３　秘密の管理

１　秘密の指定

---

*4　不正競争防止法は、営業秘密（秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの）に該当するものについて、これを開示した従業員等に対する処罰を規定している（同法第 21 条第 1 項）。

なお、外国為替及び外国貿易法は、国際的な平和及び安全の維持を妨げることになる特定貨物の特定地域への輸出や特定技術の特定地域での提供を目的とする取引を行う場合には経済産業大臣の許可を受けることを義務付け、違反した場合の罰則を設けている（同法第 25 条第 1 項、第 48 条第 1 項、第 69 条の 6 第 1 項）。

*5　現行法令上、防衛秘密に係る物件の製造又は役務の提供の委託を受けた民間業者は、防衛秘密の管理体制につき一定の基準に適合する必要があるなどその適切な管理を義務付けられるほか、民間業者が防衛秘密を漏らした場合には防衛省の職員と同じ罰則が適用される。

(1)　指定行為

本法制の対象とする特別秘密については、厳格な保全措置の対象とするものであるから、対象となる範囲を明確に特定することが適当である。このため、標記（標記が困難な場合は通知）による指定を要件とすること、すなわち、~~本法制における~~特別秘密については、実質秘であることを前提に、要式行為たる指定行為により保全対象たる秘密の~~となる~~外縁~~が~~を明確化し、その範囲で厳格な管理を行う~~されたものに限定する~~ことが適当である。

(2)　指定権者

各行政機関等が独自に~~独立して~~情報の作成・取得を行っている現状にあることや、秘密指定の要否の判断は当該情報の作成・取得の原因となった具体的事務に即して行うことが適当であることに照らすと、秘密指定の権限は、原則として、特別秘密の作成・取得の主体である各行政機関等に付与することとするのが適当である。

また、行政機関等から事業の委託を受けた民間事業者等が作成・取得した情報については、当該委託をした行政機関等が、情報の流出による当該事業への影響等を最も的確に判断できると考えられることから、原則として、当該委託をした行政機関等が秘密指定を行うこととするのが適当である。

(3)　秘密指定の効果

特別秘密の指定がなされた情報は、特別秘密としての取扱いを受けることになる。

具体的には、特別秘密の指定の趣旨に照らし、これを取り扱う者が限定され、必要のない者が当該特別秘密を知得することがないよう、後述のとおり厳重な人的管理及び物的管理が求められることとするのが適当である。

なお、特別秘密の作成・取得の趣旨に照らし、他の行政機関等や民間事業者等との共有が必要な場合には、特別秘密の外部への伝達を認めることが適当である[*6]。

ただし、特別秘密の漏えいを防ぐために、共有先の行政機関等又は民間事業者等において、法令等により特別秘密の適切な管理が確保されていることを前提とすることが適当である。

(4)　他の行政目的等のための秘密の伝達

---

*6　自衛隊法上の防衛秘密も、一定の要件の下で防衛省外の者への伝達が認められている。

特別秘密を保有する行政機関等が、~~許認可、会計検査、捜査等の他の行政機関等[*7]の業務の遂行のために、特別秘密を~~その作成・取得の趣旨に照らし伝達が想定されない~~当該他の~~行政機関等に特別秘密を伝達する必要性を~~が~~認め~~られ~~るべき場合があると考えられ~~る得~~る[*8]。~~が、~~具体的には、許認可、会計検査、捜査等の業務の遂行のための伝達が考えられるが、この場合、伝達先の行政機関等において法令等に基づき特別秘密の管理が確保されていることを前提とすることが適当である。

(5)　指定の解除

高度の秘匿の必要性が認められなくなった~~指定の要件に該当しなくなった~~特別秘密について、指定を迅速に解除すべきことは当然であり、秘密保全法制に対する国民の理解を得る上でも重要である。このため、本法制の対象となる特別秘密がその要件に該当しなくなった場合には、指定権者において速やかに指定を解除することが適当である。

高度の秘匿の必要性がなくなった情報がなお特別秘密扱いされる弊害を防止するための制度的担保としては、~~また、特別秘密の指定の解除を徹底する観点からは、~~指定の有効期限を定め、一定期間ごとに指定の要否を再検討する機会を設ける更新制が~~も~~有効な手段のひとつと考えられる。行政実務の実情を踏まえ、~~もかし、指定する特別秘密の数が増えるにつれて更新に要する事務負担の問題もあることから、このようなメリット・デメリットを勘案しつつ、~~その導入の可否を検討すべきである。

(6)　指定の調整等

特別秘密は、その性格上、統一的に指定され、解除されることが必要であるから、国の行政機関の間で特別秘密の指定及び解除についてそごが生じないように、複数の機関で判断が異なる場合の調整の仕組みを整理することが必要である。

また、国の行政機関以外の行政機関等が指定又は解除を行う場合において、国との間でそごが生じないよう、国が一定の関与を行う枠組みを設けることが必要である。

2　人的管理

特別秘密を保全するためには、特別秘密を取り扱う者自体の管理を徹底することが重要である。具体的には、以下に述べるとおり、特別秘密を取

~~*7　同一の行政機関等の他の部門に伝達する場合を含む。~~

*8　同一の行政機関等の他の部門に伝達する場合を含む。

り扱わせるうに足るつき適性を有すると認められた者に取り扱わせること、真に必要のある者に限って取り扱わせること、管理責任を明確化すること、及び特別秘密を取り扱う者の保全意識を高めることが必要である。

(1) 適性評価制度

ア　適性評価制度の整備

(ｱ)　適性評価制度とは

特別秘密の取扱者から秘密を漏えいする一般的リスクがあると認められる者をあらかじめ除外できればする仕組みがあれば、特別秘密が漏えいする可能性を制度的に低減することができる可能となる。適性評価制度とは、秘密情報を取り扱わせようとする者（以下「対象者」という。）について、日ごろの行いや取り巻く環境を調査し、対象者自身が秘密を漏えいするリスクや、対象者が外部からの漏えいの働きかけに応ずるリスクの程度を評価することにより秘密情報を取り扱う適性を有するかを判断する制度である。

(ｲ)　諸外国の適性評価制度

このような制度は、米、英、独、仏等の諸外国において、国にとって重大な秘密情報を保全する制度の一部として既に導入・運用されている。その共通点としては

①　法令等により制度が明らかにき根拠付けられていること

②　対象者は原則として秘密の取扱者全てであり、その中には国の行政機関から事業の委託を受ける民間事業者等の職員も含まれていること

③　実施に当たっては本人の同意を得て本人から調査票等により情報を収集することとし、情報の収集・裏付けのために公私の団体に対して渡航履歴等の照会を行っていること

④　各行政機関の長が実施していること

⑤　評価の結果を本人に通知するとともに、定期的に改めて評価を行っていること

等を挙げることができる。

(ｳ)　我が国の現行制度の課題と法制の必要性

我が国では、「カウンターインテリジェンス機能の強化に関する基本方針」（平成19年8月9日カウンターインテリジェンス推進会議決定）に基づき、政府統一基準として、平成21年4月から国の行政機関の職員を対象に秘密情報（特別管理秘密）の取扱者に対して適性の評価を実施している。しかし、この制度では、

① 法令上の位置付けが必ずしも明確でないこと
② 国の行政機関の職員のみが対象となっており、国の行政機関からの委託により秘密情報を取り扱う民間事業者等の職員が対象となっていないこと
③ 対象者本人から十分な情報が得られない場合に、適性評価の実施権者（対象者が適性を有していると認める権限がある者をいう。）が公私の団体に照会する権限が明確でないこと

などの課題がある。

適性評価制度を本法制の中で明確に位置付け、必要な規定を設けることは、特別秘密の保全の実効性を高める観点から極めて重要である。

なお、適性評価制度の設計においては、諸外国の先行事例を参考としつつ、我が国の実情に沿うものとするよう十分考慮する必要がある。

イ 適性評価の対象者

行政機関等や民間事業者等において、特別秘密を作成・取得する業務、あるいはその作成・取得の趣旨に従い特別秘密の伝達を受ける業務に従事する者は、特別秘密の取扱いが業務上当然に想定される。また、行政機関等においては、特別秘密の作成・取得の趣旨に照らし特別秘密の取扱いが想定されない業務の遂行のために特別秘密の伝達を受けることがあり得る。いずれの業務についても、特別秘密の重要性にかんがみ、あらかじめ適性評価を実施し、適性を有すると認められた者のみに特別秘密を取り扱わせることが適当である。

その際、常に後述の一連の評価プロセスが全て完了しなければならないこととすると、特別秘密を取り扱う業務の遂行に著しく支障を来す場合があると考えられることから、このような場合には、一連の評価プロセスの完了前に、暫定的に適性を評価し、一定期間に限り特別秘密を取り扱わせることができることとすることが適当である。

ただし、特別秘密を取り扱うことが事前に予測されておらず、かつ、緊急に特別秘密を取り扱わせなければ業務の遂行に著しく支障を来す者については、あらかじめ適性評価を実施することが困難であることから、例外的に適性評価に代替する措置を講じた上、一定期間に限り特別秘密を取り扱わせることができることとすること等が考えられる。なお、この者に一定期間経過後も特別秘密を取り扱わせることとなる場合における適性評価の要否については、今後検討すべきである。

一方、内閣を組織する内閣総理大臣及び国務大臣にあっては、極めて高度な政治的性格を有する職であることから、適性評価の対象外とすることが考えられる。また、その他特別の任免の要件・手続が採用されている職については、それぞれの職の性格を踏まえ、適性評価の必要性を個別に判断することが適当である[*9]。

ウ　実施権者

国の存立にとって重要な秘密情報として国が特別秘密に指定したものについて、これを厳重な管理に服せしめるのは国の責務と考えられる。この考え方を踏まえ、特別秘密を取り扱う機関の実施権者については以下のとおりとすることが適当である。

(ｱ)　国の行政機関

国の行政事務が、法令の定める任務・所掌事務について各行政機関ごとに~~それぞれ任務・所掌事務が定められ、系統的に~~処理されていることを踏まえ、国の行政機関の職員についての適性評価は、原則として各行政機関の長をその実施権者とする。

(ｲ)　独立行政法人等

独立行政法人等が主務大臣の関与の下で業務を実施していることから、独立行政法人等の職員についての適性評価は、主務大臣を実施権者とする。

(ｳ)　都道府県警察

警察事務は、本来、住民の日常生活の安全の確保という地方的性格と国全体の安全等に係る国家的性格とを併せ持つものであり、我が国の警察制度では、都道府県警察に一定の国家的性格を付与している。こうした警察事務の性格と~~我が国の~~現行警察制度を踏まえ、都道府県警察の職員の適性評価は、警視総監・道府県警察本部長を実施権者とする。

(ｴ)　民間事業者等

民間事業者等は、行政機関等から事業委託を受けることで特別秘密を取り扱うこととなるため、民間事業者等の職員の適性評価の実施権者は、事業を委託した機関における実施権者とする。

エ　評価の観点及び調査事項

秘密漏えいのリスクとの関連が深い、例えば以下の観点から対象者

---

*9　米では大統領及び副大統領、英では首相及び大臣、独及び仏では大統領、首相及び大臣について、それぞれ適性評価の対象から除外されている。

の適性を評価することが考えられる。

① 我が国の不利益となる行動をしないこと。

② 外国情報機関等の情報収集活動に取り込まれる弱点がないこと。

③ 自己管理能力があること又は自己を統制できない状態に陥らないこと。

④ ルールを遵守する意思及び能力があること。

⑤ 情報を保全する意思及び能力があること。

したがって、適性評価においては、上記の観点からの評価に必要な事項を調査する必要があり、具体的な調査事項としては、例えば、①身元（氏名、生年月日、住所、国籍、帰化、本籍、親族、職歴等）、②対日有害活動その他これに類する反社会的活動への関与、③外国への渡航、④犯罪経歴、⑤懲戒処分、⑥信用状態、⑦薬物・アルコールの影響、濫用及び依存、⑧精神状態、⑨秘密情報の取扱いに係る非違、⑩秘密情報の保全が確実に行われることを疑わせる特異な言動、といったものが考えられる。

また、配偶者のように、対象者の身近にあって対象者の行動に影響を与え得る者については、外国への渡航や信用状態等について調査することも考えられる。

オ　調査事項の公開及び評価基準の非公開

適性評価の実施に当たっては、様々な個人情報を取得し、利用する必要があることに鑑み、調査事項を法令上~~明らかにすることで~~明示し、いかなる個人情報が取り扱われることとなるのかを明らかにすることが、適性評価制度への国民の理解を得る観点から適当である。

一方、評価基準を明らかにすると、漏えいのリスクがあることを不当に隠そうとする者に対抗措置を講ずる機会を与えるおそれがあることから、評価基準は~~明らかにしないことが適当である~~、その性質上、公開にはそぐわないものと考えられる。

カ　プロセス

(ｱ)　対象者の同意と調査票の提出

適性評価では実施権者が対象者の個人情報を調査し、把握する必要があるが、~~まずは~~対象者のプライバシーに深く関わる調査となることから、調査については、対象者の同意を得て、調査票の~~を~~任意の提出~~させる~~を待って手続を開始、進めることが~~適当~~肝要である。

(ｲ)　対象者への面接

実施権者は、調査票への回答の真偽等を確認するため、必要に応

じ、対象者に面接することとすることが適当である。

(ｳ)　第三者に対する照会等

調査票や面接における回答の真偽を確認する必要がある場合において、対象者本人から提出を受けた資料では十分な情報が得られないときには、実施権者が金融機関、医療機関その他の公私の団体に調査事項に関して照会する必要があることも考えられるため、実施権者にその権限を付与することが適当である。

また、対象者の日ごろの行い等を調査するため、職場の上司や同僚等の対象者をよく知る者に対して質問する必要がある場合も考えられることから、実施権者にその権限を付与することが適当である。

なお、第三者に対する照会等については、個人情報を手厚く保護するよう配慮する観点や照会先の公私の団体が照会に協力しやすい環境を整備する観点から、慎重を期すため、対象者本人から同意を得て行うことが適当である[*10]。

(ｴ)　適性の判断

適性評価では、対象者による秘密漏えいのリスクの程度を全ての調査事項の調査を通じて総合的に評価する必要があり、適性を有するかどうかは、実施権者の~~高度に~~裁量的~~な~~判断に委ねられるべきものと考えられる。

本制度のこのような性格を踏まえると、実施に当たっては必要に応じて対象者本人から詳細な説明を求めるなど、慎重かつ細心の注意を払うことが必要である。

また、複数の実施権者がそれぞれの裁量的~~な~~判断により適性評価を行うこととなるため、各実施権者の判断が大きく異なることのないよう、政府において統一的な評価基準を作成してこれを共有することも検討する必要がある。

(ｵ)　結果の通知

実施権者は、適性評価の結果を対象者に通知することが適当である。

なお、適性を有しないと評価された場合は、支障のない範囲で理由を付して通知することを検討する必要がある。

~~*10　実施権者に個人情報の照会権限を付与した上で、さらに照会について本人の同意も必要とする制度とするのは、慎重な手続きにすることにより個人情報を手厚く保護するよう配慮する観点や照会先の公私の団体が照会に協力しやすい環境を整備する観点からである。~~

キ　評価結果の有効期限

評価結果には有効期限を設け、有効期限後も引き続き特別秘密を取り扱わせる必要があるときは、改めて適性評価を実施しなければならないこととすることが適当である。

ク　適性の見直し

適性評価を実施した後、当該対象者について、その結果を覆すおそれのある事情の存在が疑われる場合には、実施権者は速やかに適性評価を再度実施し、結果に応じて適性の評価を見直すことが適当である。

ケ　関係資料の適切な取扱い

適性評価の実施に当たっては様々な個人情報を取り扱う必要があるところ、実施権者は対象者の個人情報の保護が確実に図られるよう必要かつ適切な措置を講じなければならないことは言をまたない[*11]。

(2)　取扱者の指定

特別秘密が漏えいする可能性を低減させるため、特別秘密を取り扱わせる者は、適性を有すると認めた者の中から、業務上の必要性から真に必要のある者を指定することによって、これらの者に限ることが適当である。

(3)　管理責任体制

特別秘密を取り扱う機関の長は、その職員の中から、特別秘密の取扱いの業務を管理させる取扱管理者等を指名するなどして組織内において適切に役割・責任を分担する体制を構築することが適当である。

(4)　研修

特別秘密を職員に適切に取り扱わせるためには、秘密保全の意識を啓発するとともに、秘密保全に係る個別具体的な手続等に関する知識を習得させる必要があることから、特別秘密を取り扱う機関の長は、特別秘密を取り扱わせる職員に研修を実施することが適当である。

3　物的管理

*11　具体的には、個人情報の保護に係る法令に基づき、1）収集した個人情報を適性評価以外の目的で利用・提供してはならないこと、2）適性を評価するという目的の達成に必要な範囲を超えて個人情報の提供を対象職員に求め、又は公務所その他の公私の団体に照会してはならないこと、3）取り扱う個人情報の漏えいの防止その他の適切な管理のための措置を講ずること、4）個人情報を取り扱うこととなる担当職員に対して、個人情報の安全管理に係る必要かつ適切な監督を行うこと、が必要と考えられる。

上記の人的管理の各措置に加え、特別秘密を保全するためには、作成・取得から廃棄・移管までの各段階において、個別具体的な保全措置を日常的に講ずる必要がある。

具体的には、例えば以下のような事項について保全措置を講じることが適当である。

① 特別秘密に係る文書・図画・物件の作成・取得、運搬・交付、保管・利用、廃棄・移管の手続及び方法

② 特別秘密の保管場所等への携帯型情報通信・記録機器の持込み

③ 特別秘密に係る電子計算機情報の取扱い方法

④ 特別秘密の保全の状況についての検査

第４ 罰則

１ 罰則に関する基本的な考え方

特別秘密の漏えいを防止するためには、前述のとおり厳格な人的管理及び物的管理を行うのみならず、漏えい行為など本来特別秘密を知る立場にない者が特別秘密を知ることにつながる行為について、刑罰をもって臨むことが必要である。

そして、特別秘密の漏えいを防ぐには、その保全状態を保護することが効果的と考えられること、及び処罰の範囲を必要最小限に抑えることが、本法制に対する国民の理解を得る上で重要と考えられることから、特別秘密を現に保全する者、すなわち業務によりこれを取り扱う者による漏えいを処罰し、特別秘密の漏えいを根元から抑止することを基本的な考え方とすることが適当である。

また、法定刑については、上記行為を抑止するとともに、特別秘密の漏えい等という重い罪責に応じた処罰を可能にするような刑を定めることが適当である。

２ 禁止行為

(1) 故意の漏えい行為

処罰すべき行為として、まず、故意に秘密を漏えいする行為が考えられるところ、処罰すべき者の範囲が問題となる。

ア 業務により特別秘密を取り扱う者

業務により特別秘密を取り扱う者は、自己の業務上の権限や地位に基づき特別秘密を知る者で、その業務性に応じた高度の保全義務を負

うこととなるから、これらの者による故意の漏えい行為を処罰することが適当である。

ところで、このような者には、特別秘密を取り扱うことを業務とする者、すなわち特別秘密の作成・取得の趣旨に従い特別秘密を取り扱う者[*12]（以下「取扱業務者」という。）と、特別秘密の作成・取得の趣旨に従い特別秘密を取り扱うのではなく、自己の業務の遂行のために必要性が認められて特別秘密の伝達を受け、これを知得する者[*13][*14]（以下「業務知得者」という。）がある。

このうち、業務知得者による特別秘密の漏えい行為について、故意行為であり、かつ特別秘密の秘密性が現実に害される点では取扱業務者による漏えい行為と変わらないし、行政機関等の業務に関して国の重要な秘密の伝達を受ける以上、漏えいした場合には取扱業務者と同等の責任を負うべきとの考えがある。

他方、自衛隊法及びMDA秘密保護法では、国の重要な秘密である防衛秘密ないし特別防衛秘密の漏えいについて、取扱業務者と業務知得者との間で取扱いに差異を設けている[*15]。これは、業務知得者が特別秘密の取扱いそのものを業務とする者ではなく、取扱業務者に比して特別秘密を取り扱う機会も少ないなどの事情に照らし、取扱業務者に対する刑よりも軽い刑を定めるべきとの考え方に立っているものと解されるところ、本法制においても同様に両者の取扱いに差異を設けるべきとの考え方もある。

このように、業務知得者の処罰の程度については両様の考え方があることから、更に検討すべきである。

イ　その他の者

---

*12　防衛秘密の例では、武器の調達等にかかわる防衛省の職員や、同省から武器の製造等の委託を受けた民間事業者の従業員が挙げられる。

*13　例えば、捜査の過程で特別秘密に触れる検察官・警察官や、予算案の作成過程で特別秘密に触れる財務省の担当官が挙げられる。自衛隊法上の防衛秘密制度においても、これらの者は、「防衛秘密を取り扱うことを業務とする者」に該当しないと解されている。

*14　記者が取扱業務者に取材をして特別秘密を知得した場合、記者は自己の業務として取材をしているが、記者は秘密の伝達を受ける業務上の権限や地位を有しておらず、その業務に基づいて秘密を知得したとはいえないから、業務知得者には該当しないと解される。

*15　自衛隊法では、取扱業務者による漏えい行為のみを処罰し、業務知得者による漏えい行為は処罰対象としていない。また、MDA秘密保護法では、取扱業務者による漏えい行為を業務知得者による漏えい行為よりも重く処罰している。

例えば取扱業務者の漏えい行為により特別秘密を知った者など、取扱業務者又は業務知得者以外の者（以下「業務外知得者」という。）が特別秘密を第三者に漏えいした場合、これを処罰すべきかが問題となる[*16]。

このような行為は、特別秘密をより広範囲に拡散する行為ではあるが、そもそも業務外知得者は業務として特別秘密を取り扱う者ではないため、業務外知得者への伝達の時点で特別秘密は既に保全状態から流出しており、上記行為を処罰しても漏えいの根元からの抑止にはつながらない。また、これを処罰の対象とすると、例えば特別秘密文書をたまたま拾った一般人まで処罰対象になり得るなど処罰対象が広がる上、正当な報道活動も構成要件に該当し得るため報道活動への影響も懸念される。

このため、業務外知得者による漏えい行為については、特別秘密の漏えいを根元から抑止するとの基本的な考え方に基づき、その行為自体を処罰するのではなく、その前段階にある、業務により特別秘密を取り扱う者による漏えい行為の処罰を徹底することが適当である。

(2)　過失の漏えい行為

特別秘密の性格に照らせば、過失による漏えいであっても、国の利益や国民の安全の確保に大きな影響を及ぼすことは、故意による場合と変わりがない。業務により特別秘密を取り扱う者は、その業務に応じ、特別秘密を厳格に保全し漏えいを防ぐ責任を有しているのであるから、漏えいを防ぐ注意義務が認められ、過失による漏えいを処罰することが適当と考えられる[*17]。

他方、業務知得者の過失による漏えい行為については、MDA 秘密保護法では取扱業務者のそれより軽い刑が定められ、また、自衛隊法ではそもそも処罰対象とされていない。さらに、業務知得者には高度の注意義務を認めるべき基礎が十分ではないとの考えや、過失犯を厳格に処罰すれば、当該業務の遂行それ自体よりも特別秘密の管理に業務の重点が移行し、その結果当該業務の遂行に支障を来すおそれがあるとの考えもあり得る。【第１案：このため、業務知得者については処罰の程度につき検討する必要がある。】【第２案：このため、業務知得者の処罰につ

*16　不正競争防止法第 21 条第 1 項第 7 号は、違法な開示により営業秘密を取得した者による当該営業秘密の使用及び開示を処罰の対象としている。

*17　自衛隊法は、取扱業務者による防衛秘密の過失の漏えいを処罰の対象としている。

いては更に検討する必要がある。】

(3)　特別秘密を取得する行為

特別秘密の漏えいを防ぐには、特別秘密の保全状態からの流出を防ぎ、秘密の漏えいを根元から抑止することが重要であるところ、業務によりこれを取り扱う者、すなわち取扱業務者及び業務知得者による漏えい行為を処罰対象とすることで、特別秘密の保全状態からの流出に最低限の歯止めをかけることは可能である~~相当程度対応し得る~~。

しかし、特別秘密の保全状態からの流出には、取扱業務者等による漏えい行為の処罰では抑止できない取得行為を原因とする場合がある。すなわち、

①　財物の窃取、不正アクセス又は特別秘密の管理場所への侵入など、管理を害する行為を手段として特別秘密を直接取得する場合

には、取扱業務者等による漏えい行為が介在しないため、漏えい行為の処罰ではこれを抑止できない。また、

②　欺罔により適法な伝達と誤信させ、あるいは暴行・脅迫によりその反抗を抑圧して、取扱業務者等から特別秘密を取得する場合

には、取扱業務者等に漏えいの故意がないなど、漏えい行為の処罰が困難な場合がある[*18]（以下、上記①②に該当する行為を便宜的に「特定取得行為」という[*19]。）。

特定取得行為を処罰することとすれば、特別秘密の保全にかかわらない一般人を新たに処罰対象とすることとなるため、前述の基本的な考え方からすれば慎重な検討を要する。

しかし、特定取得行為は、犯罪行為や犯罪に至らないまでも社会通念上是認できない行為を手段とするもので、適法な行為との区別は明確であるから、特定取得行為を処罰対象に加えても、正当な取材活動など本来許容されるべき行為が捜査や処罰の対象とされるおそれはないと考え

---

*18　参考　不正競争防止法第21条第1項（抄）

次の各号のいずれかに該当する者は、十年以下の懲役若しくは千万円以下の罰金に処し、又はこれを併科する。

一　不正の利益を得る目的で、又はその保有者に損害を加える目的で、詐欺等行為（人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。）又は管理侵害行為（財物の窃取、施設への侵入、不正アクセス行為その他の保有者の管理を害する行為をいう。）により、営業秘密を取得した者

*19　秘密を取得する行為について、刑事特別法等では、情報（無形物）の取得を「探知」、文書、物件等（有形物）の取得を「収集」とそれぞれ呼んでいる。

られる。

また、特定取得行為は、特別秘密を保全状態から流出させる点で取扱業務者等による漏えい行為と同様の悪質性、危険性が認められる行為であり、その行為が取扱業務者等によるものでないということのみをもって処罰の対象から外されるとすれば、特別秘密の保全を目的とする本法制の趣旨を損ねることになると考えられる。

このため、処罰の範囲を必要最小限に抑えるという基本的な考え方の下でも、特定取得行為を処罰対象とすることには理由がある~~やむを得ない~~。

なお、特定取得行為の中には他の犯罪が成立する行為もあるが、特別秘密の保全の観点からは、同行為は取扱業務者等による漏えい行為と同様の悪質性、危険性が認められる行為であるから、本法制において、特定取得行為として処罰対象とすることが適当である。

(4) 未遂行為

故意の漏えい行為の未遂は、特別秘密の漏えいの危険を現実化させる悪質性の高い行為であり、処罰対象とすることが適当である。

また、特定取得行為は漏えい行為と同様に秘密を漏えいさせる高い危険性を有することから、同行為の未遂も処罰することが適当である。

(5) 共謀行為

故意の漏えい行為の共謀は、漏えい行為について共謀者間で具体性、特定性、現実性を持った合意がなされる上、共謀者の一人の意思の変化では犯罪行為の遂行を容易に変更できないこととなり、単独犯における犯行の決意に比べて犯罪実現の危険性が飛躍的に高まるため、特別秘密の保全の重要性に照らせば共謀段階での処罰の必要性が認められる。そこで、他の立法例も考慮し[*20]、漏えい行為の共謀行為を処罰対象とすることが適当である。

また、特定取得行為は漏えい行為と同様に秘密を漏えいさせる高い危険性を有することから、同行為の共謀も処罰することが適当である。

(6) 独立教唆行為及び煽動行為

取扱業務者等に対し、特別秘密を漏えいするよう働きかける行為は、その漏えいの危険を著しく高める行為であって悪質性が高い。他の立法例も考慮すると[*21]、正犯者の実行行為を待つことなく、特別秘密の漏え

---

*20 自衛隊法は、防衛秘密の漏えいの共謀を処罰の対象としている。

*21 自衛隊法は、防衛秘密の漏えいの独立教唆及び煽動を処罰の対象としている。

いの独立教唆及び煽動を処罰対象とすることが適当である。

また、特定取得行為は漏えい行為と同様に秘密を漏えいさせる高い危険性を有することから、同行為の独立教唆及び煽動を処罰することが適当である。

(7)　自首減免規定

刑法第４２条は自首した者に対する刑の任意的減軽を規定しているが、さらに、自首した者に対する必要的な刑の減軽又は免除を規定すれば、現実の漏えいに至る前に自首することを促し、ひいては実害の発生を未然に防ぐことを期待できる。

そこで、いまだ実害が発生していない時点での自首を促し、実害の発生を防止する観点から、他の立法例も考慮し[*22]、漏えい行為及び特定取得行為の未遂及び共謀について、自首による刑の必要的減免規定を置くことが適当である。

(8)　国外犯処罰規定

特別秘密の保全を徹底する観点からは、我が国の領域外における漏えい行為や特定取得行為についても処罰対象とすることが適当である。

そして、特別秘密の漏えい行為等は、日本国外において日本国民のみならず日本国民以外の者によっても敢行され得るところ、漏えい行為等は我が国の重大な利益を害する行為であるから、行為者の国籍を問わず我が国において処罰できるようにすることが適当と考えられる。したがって、特別秘密の漏えい行為等については、刑法第２条の例により、日本国外において罪を犯したすべての者を処罰することとすることが適当である。

３　法定刑

特別秘密の漏えい行為等に対する十分な抑止力を確保し、また、漏えい行為等を敢行した者に対してその罪責に応じた十分な刑罰を科し得るようにするためには、他の立法例を参考にするとともに、罪刑の均衡を前提としつつ、法定刑を相当程度高いものとすることが必要である。

本法制で処罰対象とする漏えい行為等のうち、最も重い刑をもって臨むべき行為は、業務により特別秘密を取り扱う者による故意の漏えい行為、及び特定取得行為と考えられる。そこで、以下、それらの行為に対する法

*22　自衛隊法は、防衛秘密の漏えい未遂及び漏えいの共謀につき自首による刑の必要的減免を規定している。

定刑を検討する。

(1)　自由刑について

これまでの検討内容に照らすと、防衛秘密に相当する事項は特別秘密に該当するものと考えられる。そして、防衛秘密の漏えい行為に対する最高刑が懲役５年であることからすれば、本法制における最高刑も懲役５年とすることが考えられる。

しかしながら、立法例を見ると、刑事特別法及びMDA秘密保護法では最高刑が懲役１０年であるほか、不正競争防止法においても営業秘密の開示行為等に対する最高刑は懲役１０年である。さらに、特定取得行為においては窃盗罪（最高刑は懲役１０年）などが手段として敢行されることがあることも考慮すると、本法制における最高刑を懲役１０年とすることも考えられる。

さらに、法定刑を相当程度高いものとする観点からは、懲役刑の下限を設けることも検討に値する。

(2)　罰金刑について

特別秘密の漏えい行為等は、特別秘密が保全状態から流出するという重大な結果を発生させるものであるから、その刑事責任は重く、罰金刑のみを科すことは適当でない[*23]。

他方、これまでに敢行された秘密漏えい事案においては、金銭的対価を伴うものが少なくないことから、この種事案に対する抑止効果の観点からは、懲役刑に加え、相当程度の罰金刑の併科が考えられる。

ただし、金銭的対価を伴わない事案や少額の対価を伴うに過ぎない事案もあること、漏えい等に対する報酬であれば没収・追徴も可能と考えられることを踏まえると、自由刑と罰金刑とは任意的併科とすることが

*23　自衛隊法、MDA秘密保護法及び刑事特別法では、最も重い犯罪類型に対しては自由刑のみを規定している。また、国家公務員法では罰金刑（５０万円以下）を選択刑として規定している。

適当と考えられる[*24]。

第５　法形式

本法制における特別秘密のうち、外交あるいは公共の安全及び秩序の維持に関する秘密については、国の安全に関する秘密についての自衛隊法のような受け皿となり得る既存の法律は見い出し難い。また、本法制は、国の利益や国民の安全の確保といった観点から特別秘密の漏えいを防止することを目的としており、主に服務規律の維持を目的として守秘義務を定める国家公務員法等とは趣旨が異なるため、国家公務員法等の改正により本法制を実現することは適当ではない。したがって、本法制は新規立法によることとすることが適当である。

その際、運用の統一性や制度の一覧性を確保するという観点から、単一の法制によることとするのが適当である。

なお、防衛秘密及び特別防衛秘密については、いずれも本法制の対象とする秘密との間で秘密として保護する理由に異なるところはないが、他方、ＭＤＡ秘密保護法は、日米相互防衛援助協定等に伴うものという特別な性格を有している。そこで、両者のうち、特別防衛秘密については引き続きＭＤＡ秘密保護法によるものとし、防衛秘密に限って本法制に取り込み、統一的に運用することが適当である[*25]。

第６　国民の知る権利等との関係

国民の知る権利は、健全な民主主義の根幹を支える極めて重要な権利で

---

*24　なお、秘密保持の観点からは、特別秘密の漏えい等事件の公判において、特別秘密の内容を公判廷で明らかにしないことが重要であるところ、現在、実務では、確立された立証方法として、いわゆる外形立証が行われている。外形立証とは、争点となっている秘密が実質秘であることを立証するに当たり、①秘密の指定基準（指定権者、指定される秘密の範囲、指定及び解除の手続）が定められていること、②当該秘密が国家機関内部の適正な運用基準に則って指定されていること、③当該秘密の種類、性質、秘扱いをする由縁等を立証することにより、当該秘密が実質秘であることを推認するもので、これにより実務では秘密を守りつつ公判での立証を支障なく行うことができている。

*25　日米地位協定の実施に伴う刑事特別法における合衆国軍隊の機密については、同法が米国のために在日米軍の秘密情報を保護するものであり、我が国の存立にとって重要な秘密情報を保護する本法制とは保護法益が異なることから、引き続き同法によることが適当である。

ある。

国民が積極的に政府に対してその保有する情報の開示を求める権利としての知る権利に関しては、具体的な権利性を持たない抽象的な権利であるとしながらも、憲法上の権利として認める裁判例が近年出てきている。[*26][*27]。

また、国民の知る権利と報道の自由及び取材の自由との関係について、最高裁は、報道機関の報道が、民主主義社会において国民が国政に関与するにつき重要な判断の資料を提供し、国民の知る権利に奉仕するものとして、報道の自由が憲法により保障される旨判示し、また、報道機関の報道が正しい内容を持つための取材の自由についても、憲法の趣旨に照らし十分尊重に値する旨判示している[*28]。

本法制は、国民の知る権利や取材の自由との関係で一定の緊張関係に立ち得ることから、本法制と両者との関係について慎重に検討し、以下のとおり整理したところである。

第一に、国民の知る権利について、その趣旨に鑑みれば、政府はその諸活動に関する情報を国民に提供していくことが望ましい。しかしながら、本法制における特別秘密は、政府の保有する秘密情報の中でも国の存立にとって重要なものであり、秘匿の利益が特に大きいものと考えられることから、特別秘密を厳格な保全措置の下に置き、その秘匿性を維持することをもって、国民の知る権利との関係で問題になるものではないと考えられる。

なお、行政機関が保有する情報の公開に関する法律（以下「情報公開法」という。）は、行政文書の開示を請求する権利を具体的に定めている。本法制において特別秘密として保護される情報を情報公開法に当てはめた場合、特別秘密は国の安全、外交並びに公共の安全及び秩序の維持の分野の秘密情報の中で特に秘匿性が高いものであることから、同法第５条第３号（国の安全等に関する情報）及び第４号（公共の安全等に関する情報）の不開示情報に含まれるものと解される。したがって、本法制は、情報公開法に基づく行政文書の開示に影響を与えるものではないと考えられる。

---

*26　このような裁判例においては、情報の開示を請求するためには具体的な権利性を付与する実定法上の根拠が必要であるとしている。

*27　また、第 177 回通常国会に出された情報公開法の改正案においては、同法の目的規定に国民の「知る権利」が明記されている。

*28　いわゆる博多駅事件判決（最大決昭 44・11・26）。

第二に、取材の自由について、本法制に特別秘密の漏えいの教唆罪や特定取得罪を設けることで、取材の自由が不当に制限されるのではないかとの指摘があり得る。

この点、漏えいの教唆と取材の自由の関係については、最高裁が、取材の手段・方法が刑罰法令に触れる場合や社会観念上是認できない態様のものである場合には刑罰の対象となる旨判示しており[*29]、このような手段・方法による取材行為が取材の自由を前提としても保護されない反面、正当な取材活動は処罰対象とならないことが判例上確立している。

また、本法制における特定取得罪は、既に述べたとおり、当該行為自体が現行法上の犯罪に該当するか、該当しないまでも社会通念上是認できない行為に限って処罰対象とするものであるから、上記の最高裁の立場に照らすと、取材の自由の下で保護されるべき取材活動を刑罰の対象とするものではないと考えられる。

したがって、漏えいの教唆や特定取得行為を処罰することとしても、取材の自由を不当に制限することにはならないと考えられる。

以上から、本法制は、その趣旨に従って運用されれば、国民の知る権利との関係で問題を生じたり、取材の自由を不当に制限したりするものではないと考えられる。

第７　立法府及び司法府

特別秘密は行政目的で作成・取得されるものであり、立法府及び司法府に対し、行政目的で特別秘密が伝達されることは想定されない。他方、立法府及び司法府がそれぞれの業務上の必要性から特別秘密の伝達を受け、

*29　いわゆる外務省機密漏洩事件では、「取材の手段・方法が贈賄、脅迫、強要等の一般の刑罰法令に触れる行為を伴う場合は勿論、その手段・方法が一般の刑罰法令に触れないものであつても、取材対象者個人としての人格の尊厳を著しく蹂躙する等法秩序全体の精神に照らし社会観念上是認することのできない態様のものである場合にも、正当な取材活動の範囲を逸脱し違法性を帯びるものといわなければならない」と判示されている（最決昭和 53・5・31）。

国会議員や裁判官等がそれを知得することが想定し得る[*30]ため、然るべき保全措置が取られることが本来適当である。

米、英、独、仏等の諸外国では、行政府から立法府及び司法府に伝達された秘密について、法令や規則等に従った取扱いが求められ、また、当該秘密を知得した者が守秘義務に違反して漏えいした場合には罰則が適用され得ることとなっている。

この点、まず、立法府については、国会議員にはそもそも法律上守秘義務が課せられておらず[*31]、また、憲法上、議院で行った発言について免責特権が認められている。

このようなことに鑑みれば、特別秘密に係る国会議員の守秘義務の在り方を検討するためには、国会議員の活動の在り方も踏まえつつ、立法府における秘密保全の在り方全般と特別秘密の保全の在り方との関係を整理する必要があると考えられる。しかし、このような検討は、行政府とは独立の地位を有する立法府の在り方の根幹に関わることから、立法府に委ねることが適当と考えられる[*32]。

次に、司法府については、裁判官には罰則を伴う守秘義務が設けられて

---

*30　立法府が国政調査権（憲法第 62 条）の行使として特別秘密の伝達を求めた場合、行政府はこれに応じるか否かを判断することとなるが、これに応じた場合には、国会議員及び国会職員が特別秘密を知得することとなる。また、司法府については、例えば、民事訴訟における原告や刑事訴訟における被告人・弁護人が、特別秘密に係る訴訟で特別秘密についての証拠開示等を求めた場合、裁判所がその必要性を判断するため、国・検察官に対して特別秘密の提示を命じることがあり得るが、このような場合には、裁判官や裁判所職員が特別秘密を知得することとなる。

*31　国会議員の守秘義務に関して、憲法及び国会法に規定されている秘密会において公表しないとされたものを他に漏らした者について、参議院規則では院内の懲罰手続が整備されている（衆議院規則には同様の規定がない）が、国会議員の守秘義務及び秘密漏えい行為に対する罰則を定める法令はない。

*32　国会議員であっても、内閣総理大臣、国務大臣、副大臣及び大臣政務官（以下「大臣等」という。）として特別秘密を取り扱う場合には、行政府の職員として本法制の対象とすることが適当である。自衛隊法においても、大臣等は防衛秘密の取扱業務者に該当し、同法の適用対象とされている。

また、大臣秘書官となる国会議員の秘書についても同様の考え方で対応することが適当である。

いない一方、弾劾裁判及び分限裁判の手続が設けられている[*33]。

特別秘密に係る裁判官の守秘義務の在り方を検討するためには、上記のことも踏まえ、司法府における秘密保全の在り方全般と特別秘密の保全の在り方との関係を整理する必要があると考えられる。しかし、このような検討は、行政府とは独立の地位を有する司法府の在り方に多大な影響を及ぼし得るため、司法制度全体への影響を踏まえて別途検討されることが適当と考えられる。

おわりに

特別秘密の漏えいにより国や国民が受ける被害の重大さに鑑みれば、その保全体制の整備は喫緊の課題である。知る権利など国民の権利利益との適切なバランスを確保しつつ守るべき秘密を確実に保全する制度を構築することは、国民の利益の一層の実現に資するものである。

当会議は、早期に法制化することを念頭に検討を進め、本報告書を取りまとめた。今後、この報告書の内容を十分に踏まえ、速やかな法制化が図られることを希望するものである。

---

*33　裁判官には、官吏服務紀律により職務上知り得た秘密に守秘義務が課されているが、高度な職業倫理に基づく行動ができる又は期待でき、それを担保するものとして弾劾裁判及び分限裁判の手続が設けられていることから、罰則で担保された守秘義務は課されていない（平成16年4月9日の衆議院法務委員会における司法制度改革推進本部事務局長答弁）。

機密性２情報 取扱注意

第三次案に対する委員からの御意見等

１．「第２　秘密の範囲」「３　秘密の作成又は取得の主体」「(4)　民間事業者・大学」（報告書案４頁）

前述のとおり、本法制は、政府が保有する特に秘匿を要する情報の漏えいの防止を基本とするが、政府とは直接関係を有しない民間事業者や大学においても、国の安全等に関し保護されるべき情報を作成・取得することがあり得る。

しかしながらそこで検討すると、

①民間事業者や大学が作成・取得する情報を本法制の適用対象とすると、経済活動の自由や学問の自由の観点から国家による過度の干渉にもつながりかねないこと

②民間における情報漏えいに関しては、不正競争防止法において従業員等による営業秘密の開示等に対する処罰を規定していること*4

等に照らし、民間事業者や大学が作成・取得する情報については本法制の適用対象としないことが適当である。

【②の内容は、民間事業者を本法制の適用対象から外す理由として不明確であるため。】

*4 不正競争防止法は、営業秘密（秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの）に該当するものについて、これを開示した従業員等に対する処罰を規定している（同法第21条第1項）。

なお、外国為替及び外国貿易法は、国際的な平和及び安全の維持を妨げることになる特定貨物の特定地域への輸出や特定技術の特定地域での提供を目的とする取引を行う場合には経済産業大臣の許可を受けることを義務付け、違反した場合の罰則を設けている（同法第25条第1項、第48条第1項、第69条の6第1項）。

【②を削除すること等に伴う削除。】

ただし、民間事業者及び大学（以下「民間事業者等」という。）が行政機関等（国の行政機関、地方公共団体及び独立行政法人等をいう。）から事業委託を受ける場合には、当該民間事業者等は、当該事業に関しては委託をした行政機関等と実質的に一体と考えられるから、このような場合に限っては、民間事業者等が作成・取得する情報も本法制の適用対象とすることが適当である。

【このパラグラフが重要なので、「行政機関等と実質的に一体」の意味するところを敷衍しつつ詳細に記述すべき。これに先立つ前半部分は短めにすべき。】

２．「３　秘密の管理」「２　人的管理」「(1) 適性評価制度」（報告書案８頁）

イ　適性評価の対象者

行政機関等や民間事業者等において、特別秘密を作成・取得する業務、あるいはその作成・取得の趣旨に従い特別秘密の伝達を受ける業務に従事する者は、特別秘密の取扱いが業務上当然に想定される。また、行政機関等においては、特別秘密の作成・取得の趣旨に照らし特別秘密の取扱いが想定されない業務の遂行のために特別秘密の伝達を受けることがあり得る。いずれの業務についても、特別秘密の重要性にかんがみ、あらかじめ適性評価を実施し、適性を有すると認められた者のみに特別秘密を取り扱わせることが適当である。

その際、常に後述の一連の評価プロセスが全て完了しなければならないこととすると、特別秘密を取り扱う業務の遂行に著しく支障を来す場合があると考えられることから、このような場合には、一連の評価プロセスの完了前に、暫定的に適性を評価し、一定期間に限り特別秘密を取り扱わせることができることとすること等が考えられる~~が適当である~~。

~~ただし、特別秘密を取り扱うことが事前に予測されておらず、かつ、緊急に特別秘密を取り扱わせなければ業務の遂行に著しく支障を来す者については、あらかじめ適性評価を実施することが困難であることから、例外的に適性評価に代替する措置を講じた上、一定期間に限り特別秘密を取り扱わせることができることとすること等が考えられる。なお、この者に一定期間経過後も特別秘密を取り扱わせることとなる場合における適性評価の要否については、今後検討すべきである。~~

３．「第３　秘密の管理」「２　人的管理」「(1) 適性評価制度」（報告書案９－１０頁）

エ　評価の観点及び調査事項

秘密漏えいのリスクとの関連が深い、例えば以下の観点から対象者の適性を評価することが考えられる。

①　我が国の不利益となる行動をしないこと。
②　外国情報機関等の情報収集活動に取り込まれる弱点がないこと。
③　自己管理能力があること又は自己を統制できない状態に陥らないこと。
④　ルールを遵守する意思及び能力があること。
⑤　情報を保全する意思及び能力があること。

したがって、適性評価においては、上記の観点からの評価に必要な事項を調査する必要があり、具体的な調査事項としては、例えば、①身元（氏名、生年月日、住所、国籍、帰化、本籍、親族、職歴等）、②国益を害する~~対日有害活動その他これに類する~~反社会的活動への関与の有無、③特定国~~外国~~への渡航歴、④犯罪経歴、⑤懲戒処分歴、⑥信用状態、⑦薬物・アルコールに対する感受性ないし~~の影響、濫用及び~~依存度、⑧精神状態、⑨秘密情報の取扱いに係る非違行為の有無、⑩その他秘密情報の保全が確実に行われることを疑わせる特異な言動、といったものが考えられる。

また、配偶者のように、対象者の身近にあって対象者の行動に影響を与え得る者については、外国への渡航や信用状態等について調査することも考えられる。

【表現の適正化】

４．「第４　罰則」「１　禁止行為」「(2)　過失の漏えい行為」（報告書案１５頁）

特別秘密の性格に照らせば、過失による漏えいであっても、国の利益や国民の安全の確保に大きな影響を及ぼすことは、故意による場合と変わりがない。業務により特別秘密を取り扱う者は、その業務に応じ、特別秘密を厳格に保全し漏えいを防ぐ責任を有しているのであるから、漏えいを防ぐ注意義務が認められ、過失による漏えいについても~~を~~処罰対象に含め、秘密を取り扱う業務に対する特段の注意義務を喚起することが必要~~適当~~と考えられる。

他方、業務知得者の過失による漏えい行為については、MDA 秘密保護法では取扱業務者のそれより軽い刑が定められ、また、自衛隊法ではそもそも処罰対象とされていない。さらに、業務知得者には高度の注意義務を認めるべき基礎が十分ではないとの考え~~や、過失犯を厳格に処罰すれば、当該業務の遂行それ自体よりも特別秘密の管理に業務の重点が移行し、その結果当該業務の遂行に支障を来すおそれがあるとの考え~~もあり得る。【第１案：このため、業務知得者については処罰の程度につき検討する必要がある。】【第２案：このため、業務知得者の処罰については更に検討する必要がある。】

【過失による漏えいを処罰することについて、前向きに論じるべき。過失犯の処罰により公務に緊張感を与えることができることを、過失犯を処罰する理由として第１段落に記載すべき。】

５．「第６　国民の知る権利等との関係」（報告書案２０－２２頁）

第６　国民の知る権利等との関係

【表題に「政府の説明責任」を掲げ、第６を全体的に検討したほうがよいのではないか。】

第一に、国民の知る権利について、その趣旨に鑑みれば、政府はその諸活動に関する情報を国民に提供していくことが望ましい。しかしながら、本法制における特別秘密は、政府の保有する秘密情報の中でも国の存立にとって重要なものであり、秘匿の利益が特に大きいものと考えられることから、特別秘密を厳格な保全措置の下に置き、その秘匿性を維持することをもって、国民の知る権利との関係で問題になるものではないと考えられる。

【本パラグラフは、より丁寧な記述に努めるべきではないか。】

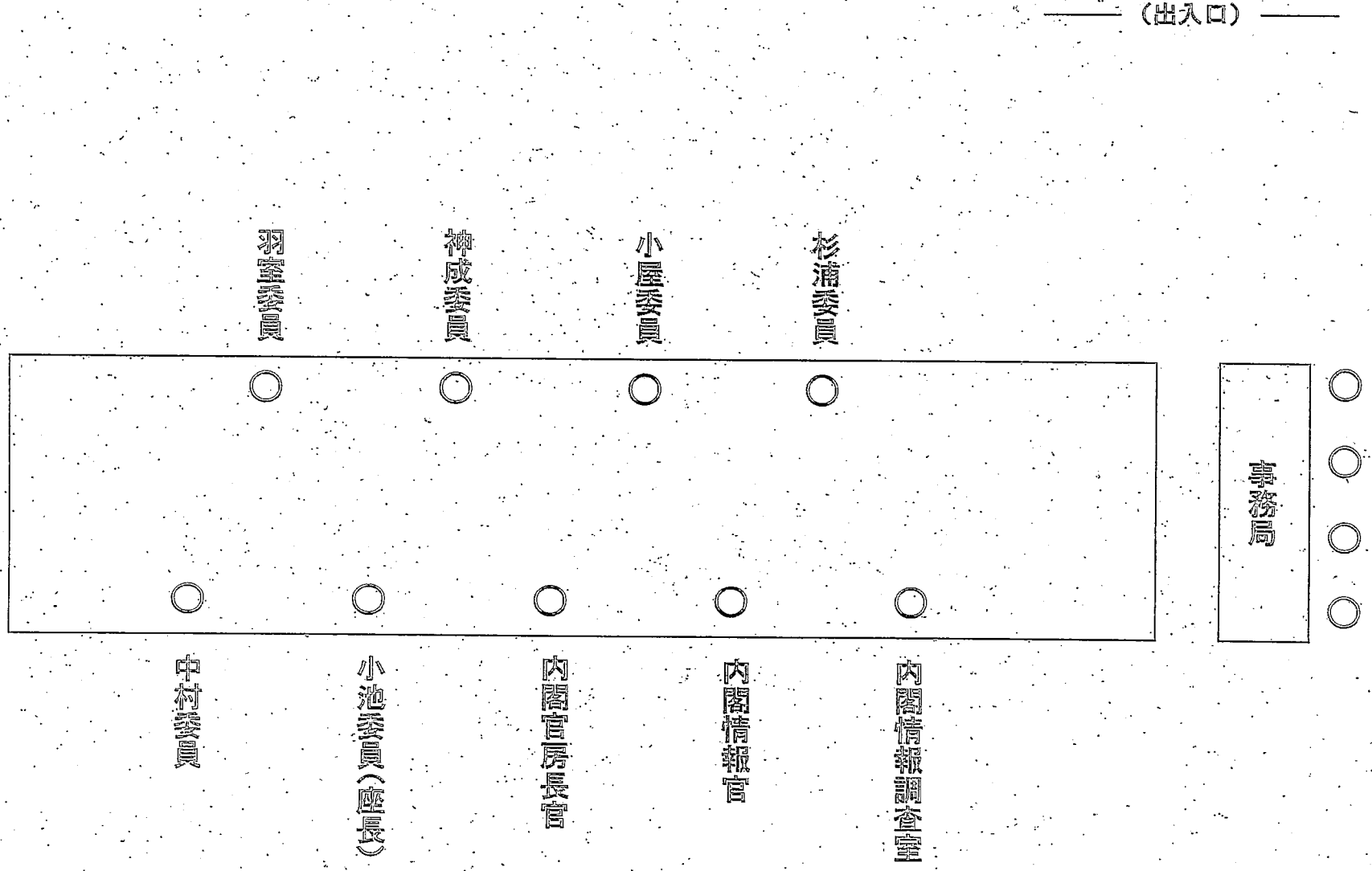
（中略）

以上述べたとおり~~から~~、本法制は政府の説明責任をあくまでも果たしながら国家の存立に関わる秘密についての一定の保全を図ろうとするものであり、原理上、国民の知る権利をないがしろにしたり、取材の自由を不当に制限することを意図するものでないことはいうまでもない。しかし、ひとたびその運用を誤れば、国民の重要な権利利益に対する制約する重大な脅威となる可能性が皆無であるとはいえず、国民主権のもと、国民による不断の監視が求められる制度であるということは、特に強調しておくべきであると考える~~、その趣旨に従って運用されれば、国民の知る権利との関係で問題を生じたり、取材の自由を不当に制限したりするものではないと考えられる~~。

【本法制が絶対に安全であるという論調はとり得ないことから、あらかじめ本法制の危険性を指摘しておくことで、本法制が国民の重要な権利利益を制約するものではないとの結論に説得力を持たせることが適当。】

第1回情報保全システムに関する有識者会議　座席表

平成22年12月17日(金)午後2時～午後3時　於:官邸4階大会議室



配付資料

資料１　政府における情報保全に関する検討委員会の開催について

資料２　情報保全システムに関する有識者会議の開催について

資料３　情報保全システムに関する有識者会議の運営について（案）

資料４　情報保全システムの検討スケジュール（案）

資料５　脅威に関する現状認識

資料６　「カウンターインテリジェンス機能の強化に関する基本方針」の概要

資料７　特別管理秘密に係る基準

資料８　政府機関の情報セキュリティ対策の枠組み

資料９　政府機関の情報セキュリティ対策のための統一基準（第４版）

対外非公表　取扱注意

機密性２情報　　配付資料３

（案）

情報保全システムに関する有識者会議の運営について

平成２２年１２月○○日
情報保全システムに関する有識者会議決定

情報保全システムに関する有識者会議（以下「会議」という。）の運営については、以下のとおりとする。

1　議事の非公開について
　会議は、非公開とする。

2　議事要旨の公開について
　会議の議事要旨は、原則として、会議終了後、発言者名を付さない形で、速やかに公開する。

3　配付資料の公開について
　会議における配付資料の公開については、内容に応じて可否を判断する。

4　記者ブリーフについて
　会議の内容については、会議終了後、事務局が記者ブリーフを実施する。

（了）

１．盗難や持出し等の脅威

(1) 可搬型電磁的記録媒体や文書の盗難等

○　庁舎外へ持ち出すことができるＵＳＢメモリ等の可搬型電磁的記録媒体が厳重に管理されていないことにより、それらが盗取され、また、盗取されても把握することが困難となるおそれがある。

○　行政事務従事者が特に機密性の高い情報を取り扱う情報システム（以下単に「情報システム」という。）から電磁的記録を媒体や書面へ不用意に出力するなど、管理されていない複製が作成されることにより、それが盗取され、また、盗取されても把握することが困難となるおそれがある。

○　執務を行っていないときには執務机の上に文書等を放置せず、端末のディスプレイにも情報を表示しないというポリシーが徹底されず、関係者以外に情報を盗み見られるおそれがある。

(2) 機器の盗難等

○　モバイルコンピュータに関する正規の使用方針が定められていないことにより、モバイルコンピュータの盗難又は紛失及びこれらに伴う情報流出のリスクがある。

(3) 秘密取扱い施設への不正侵入等

○　建物、ドア及び窓に対する物理的な防護水準が低い、秘密取扱い施設内の監視が不十分等の原因により、不正侵入や無許可立入りが発生するおそれがある。

○　秘密取扱い施設に入退室するすべての者について、適切な入退室管理が行われていない場合がある。

(4) 無許可機器による情報の持出し

○　管理区域内に無許可で持ち込まれたコンピュータ、電磁的記録媒体、デジタルカメラ、携帯電話等を使用され、情報が持ち出されるおそれがある。

2．無権限者等による不正な操作等の脅威

(1) 不適切な権限管理等

○ 情報システムの利用許可、ユーザ管理、権限管理及びアクセス制御が確実に実施されず、権限を与えられていない者による不正なシステム操作又は利用が発生するおそれがある。

○ 管理者権限行使による作業を監視する体制が必ずしも十分でない。

(2) 権限の詐称

○ 情報システムにアクセスする主体の識別及び認証メカニズムが不十分な場合がある。

○ ネットワーク上で暗号化せずパスワードを転送するなど、主体認証情報が適切に保護されていない場合がある。

○ パスワードを人目につきやすい場所に放置するなど、主体認証情報が適切に保護されていない場合がある。

(3) 情報システムの管理体制の不備

○ 権限を与えられていない者による不正アクセス行為又は基準に準拠しない行為を監視する体制が必ずしも十分でない。

○ 情報システムのセキュリティの維持・管理のために必要な技能を備えた十分な数の職員が割り当てられていない場合がある。

3．悪意のある者による情報システムに対する攻撃の脅威

(1) ネットワークを利用した外部からの侵入

○ ネットワークの構造上の脆弱性、不正に入手した認証情報、通信回線等の物理的な脆弱性等を悪用して情報システムに侵入され、情報の収集、破壊等が行われるおそれがある。

(2) ハードウェアの改ざん

○ 悪意のある者により電子計算機にセキュリティホールが組み込まれるなど、ハードウェアの改ざん行為によって情報が探知及び収集され、又は破壊されるおそれがある。

(3) ソフトウェアの改ざん

○ 独自に開発したソフトウェアに悪意のある者によりセキュリティホールが組み込まれるなど、ソフトウェアの改ざん行為によって情報が探知及び収集され、又は破壊されるおそれがある。

○　安全性が確認されていないソフトウェアが情報システムにインストールされることにより、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

(4) 情報流出のおそれのあるインタフェイス等の利用

○　情報の流出に利用されるおそれのあるインタフェイスや機能が利用可能な状態で放置され、悪意のある者がこれを利用することによって情報が探知及び収集され、又は破壊されるおそれがある。

4．情報システムの誤作動の脅威

(1) 機器の誤作動

○　安全性の確認されていない機器が接続されることによって情報システムが誤動作を起こし、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

(2) ソフトウェアの誤作動

○　意図せざる脆弱性によってソフトウェアが誤作動し、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

○　設定の変更等によってソフトウェアが誤作動し、情報の流出、データの破壊、セキュリティ機能の無効化などが生じるおそれがある。

5．操作ミスの脅威

○　情報システムの操作説明書が作成されていない、配付されていない又は周知されていないなどの理由で、行政事務従事者が情報システムの操作方法等を十分に理解しておらず、操作ミス、誤入力等が発生するおそれがある。

○　情報システムのユーザインタフェイスが複雑で、行政事務従事者の操作ミス、誤入力等が発生するおそれがある。

6．その他

(1) 部内者の情報セキュリティ違反行為

○　行政事務従事者のセキュリティ違反を監視するためのメカニズムが不十分であるため、セキュリティ違反に対する抑止効果が小さく、また、事故発生後に適切に対処することができないおそれがある。

○　データの不正処理、無許可アクセス、その他の情報セキュリティ関係規程の違反に対する制裁措置が明確でなく、行政事務従事者に対する抑止及び再発防止の効果が必ずしも十分でない。

(2) 廃棄又は再利用された電磁的記録媒体からの情報復元

○　特に機密性の高い情報の処理に使用した電磁的記録媒体を廃棄する場合や再利用する場合において、十分な破壊処置を行わなかったために当該電磁的記録媒体にデータが容易に回復できる状態で残されていたり、当該電磁的記録媒体に残されたデータの電磁的痕跡が抽出され、復元されたりすることによって情報が流出するおそれがある。

(3) 契約業者による情報セキュリティ侵害

○　情報システムの保守・点検契約を締結している業者の故意又は過失による行為によって情報が流出し、又はデータが破壊されるおそれがある。

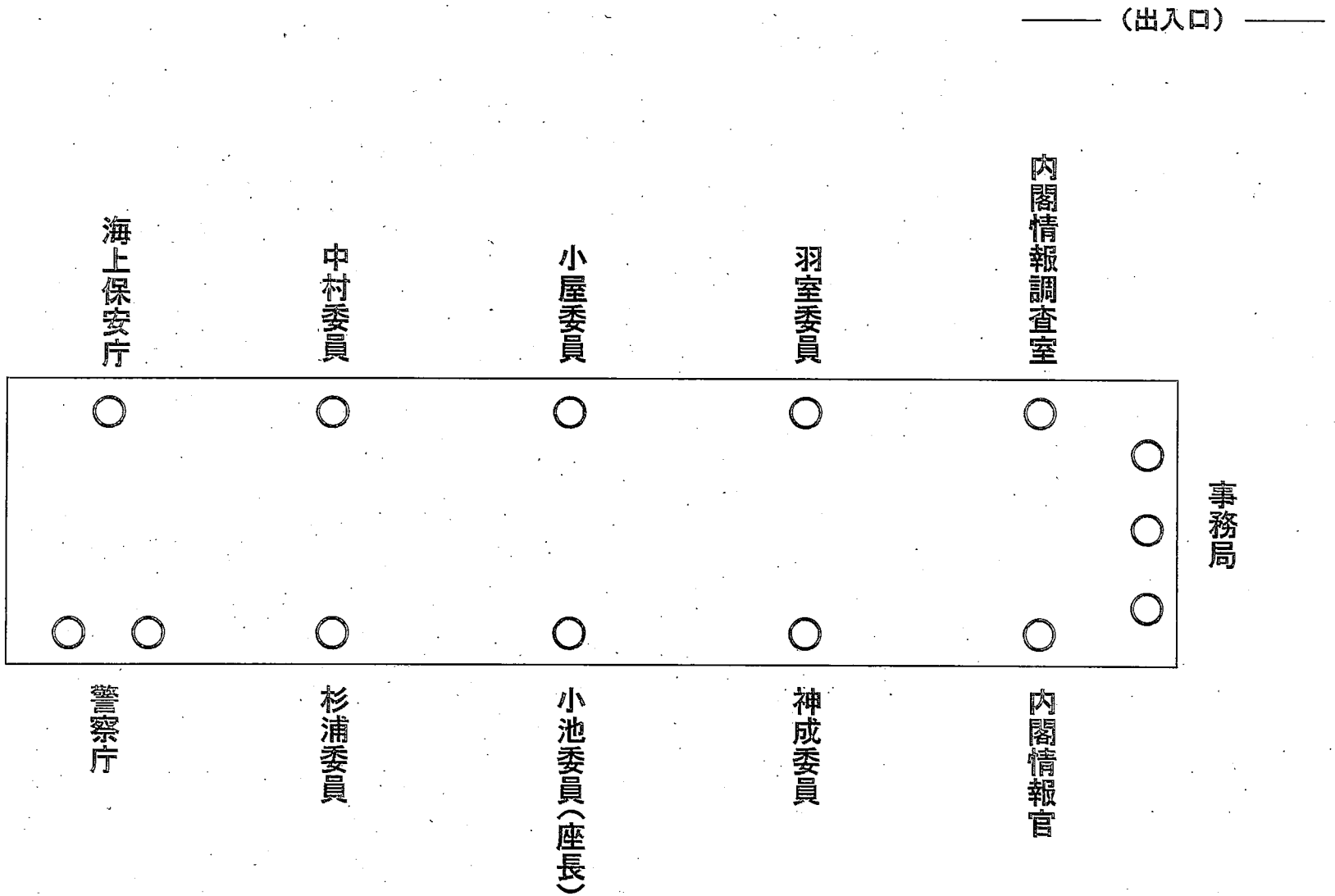
○　特に機密性の高い情報の処理業務を委託した業者との間で情報セキュリティ対策に関する契約条項を締結しておらず、委託先業者が不適切に情報を取り扱うおそれがある。

(4) セキュリティパッチの不適用

○　パッチを適用せず、ソフトウェアのバグ等を放置することにより、誤作動、データ破壊、セキュリティ機能の無効化等が発生するおそれがある。

第2回情報保全システムに関する有識者会議　座席表

平成23年2月4日（金）午前9時から概ね2時間　於：内閣府本府3階特別会議室



配付資料

資料１　情報流出事案及び事案発生後強化した対策について

資料２　特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状について【席上回収】

資料３　特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状（概念図）【席上回収】

資料４　特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状（概要図）

資料５　民間の情報保全システムの現状について

資料６　民間の情報保全システムの現状について（概要）

【機密性2情報】席上回収

配付資料2

特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状について

番号	項目			集計
1	配備している端末の状況	オープン系（A）		1人1台から5～10人に1台
		クローズ系（B）		1人1台から所属に1台
		スタンドアロン（C）		2人に1台から全体で数台 該当なしの省庁もある。
2	外部記録媒体への書き出し	A	暗号化、書き出し制限、ログの保存監査	
		B	暗号化、書き出し制限、ログの保存監査	
		C	暗号化、書き出し制限、ログの保存監査	
3	データの持出し	A		
		B		
		C		
4	私用外部記録媒体の使用制限	A		
		B		
		C		
5	通信ログ管理	A－インターネット	アクセスログ	
			アクセスログ保存期間	
		A→A	アクセスログ	
			アクセスログ保存期間	
		B→B	アクセスログ	
			アクセスログ保存期間	

特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状について

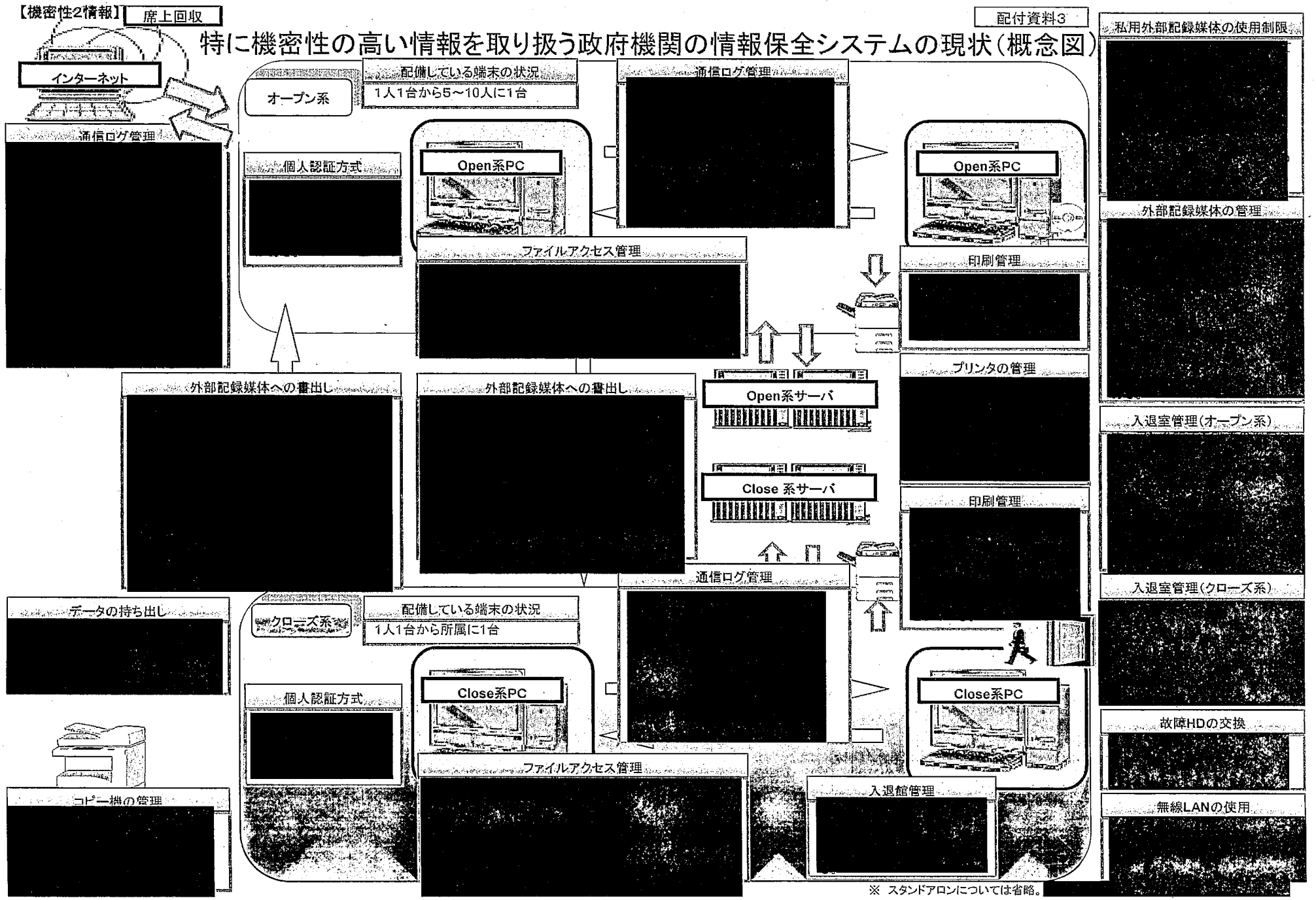
番号	項目			集計
6	ファイルアクセス管理	A	アクセスログ	
			アクセスログ保存期間	
			アクセス権限付与単位	
		B	アクセスログ	
			アクセスログ保存期間	
			アクセス権限付与単位	
		C	アクセスログ	
7	個人認証方式	A		
		B		
		C		
8	外部記録媒体の管理			
9	故障HDの交換	故障ＨＤの交換時の処理		
10	無線LAN使用の有無	A		
		B		
		C		
11	プリンタの管理	B	システム専用のプリンタか	
		C	システム専用のプリンタか	
12	コピー機の管理	外部接続されているコピー機でＢ及びＣのデータをコピーすることがあるか。		
13	印刷管理	A→紙		
		B→紙		
		C→紙		
14	入退館管理			
15	入退室管理	A	入退室記録	
			伴連れ防止の有無	
		B	入退室記録	
			伴連れ防止の有無	
		C	入退室記録	
			伴連れ防止の有無	

※オープン系（A）とは、Internetに接続可能な端末のことである。一方、クローズ系（B）とは、Internetに接続できない端末のことである。
　また、スタンドアロン（C）とは、ネットワークに接続していない端末のことである。
※ログの保存期間や監査の頻度等については、該当省庁のみ記載

【機密性2情報】 席上回収

配付資料3

特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状（概念図）



※ スタンドアロンについては省略。

【機密性2情報】(有識者会議終了時まで)

配付資料5

民間の情報保全システムの現状について

対策	概要説明
ガバナンス強化、サイバーアタック防御システム	・CodeRed,NIMDA等のワームの特性を分析し、被害の局所化を目指した統合システム 表の顔はウイルス対策システムであるが、本当の顔はガバナンス強化システムであり、社内のセキュリティ情報の把握(数の管理)を実現するコアシステム ・社内のPCとネットワークの情報を統合的に監視し、サイバー攻撃への対応や施策展開の見える化が可能 ・PCのセキュリティ対策としては、PCのシステム状況、パッチ適用状況、検疫、使用禁止ソフトの検出機能をもつ ・ネットワークのセキュリティ対策としては、攻撃監視(IDP)とネットワーク遮断システムから構成されている
情報漏洩防御システム	・過去に発生した情報漏洩事件を分析し、PCの盗難・紛失、媒体を利用したデータ持ち出し、メール誤送信、外注先からの情報漏洩などに対応可能なように設計 ・PCの全ドライブの暗号化機能(PCの盗難紛失対策) ・リムーバブルメディアの使用制限 ・ファイルの暗号化(メール誤送信対策,アクセス制御) ・ログ採取(内部犯罪の抑止) ・スクリーンロック、時刻変更禁止等
シンクライアント	・利用端末を問わないため、いつでもどこでも、情報に安全にアクセス可能 ・USBストレージの利用が不可能な特別USBポートのみを実装したPC USBフラッシュメモリなどへの持ち出しによる、外部記憶媒体経由の情報漏えいを防止 ・リモートデスクトップ接続経由のブレードサーバ利用 管理対象外プリンタからの印刷による、印刷物経由の情報漏えいを防止 ・ハードディスクレスの専用端末、データは全て社内サーバに集約 PC盗難・紛失時のハードディスク残存データの漏えいを防止 ・USBトークンを利用したPC利用者認証 なりすましによる、社内インフラへの不正アクセスを防止 ・情報漏洩対策(データの持ち出し対策)、社外でのPC盗難・紛失対策として導入 ・ID及びパスワード認証に加え、証明書(トークン、ICカード等)を利用した認証が可能 ・OTP(ワンタイムパスワード)等の様々な認証方式に対応可能
入退管理システム	・フラッパーゲートを利用した入退場管理 ・ICカード、指紋等を利用した入退室管理、監視カメラによる入出者監視
統合ログ解析/フォレンジック解析	・各種サーバ、PC、ネットワーク等のログを統合的に解析し、発生した事象の詳細を特定 ・PCやサーバの情報を解析し、発生した事象の詳細を特定
フィジカルセキュリティ	・手のひら静脈認証を用いたセキュリティネットワーク ・手のひら静脈認証を用いたPCログオン用ソフトウェア
統合ID管理基盤の構築による、グループ会社管理の一元化	・200社以上のグループ会社社員IDを統合管理。 ・統一ID管理基盤を利用し、グループ内でのWebインフラ、メールインフラの共同利用・効率化を実現
対社外通信におけるセキュリティ対策	・Webフィルタリングの実施 掲示板書き込み、フリーメール利用などによるWeb経由の情報漏えいを防止 ・メールフィルタリングの実施 上長への同報による社外メール送信許可(不正メール送信の抑止) 情報漏えいキーワードの有無によるメール送信制御
社内Webシステムのセキュリティ	・統合ID管理システムと連動したWebシングルサインオンによる、社内Webシステムへのアクセス制御 ・Webコンテンツ(Webファイル)閲覧権限設定によるアクセス制御 通常のアクセス制御に加え、コピー&ペースト、印刷可否も制御
業務ドキュメントのDRM保護の推進	・メール送信操作に統合された添付ファイルの利用権管理を実施 誤送信先の第三者による添付ファイルの閲覧を防止 ・グループでのネットワークインフラ共用により、効率的なDRMシステムの利用を実現
資産管理ツールによる、クライアントPC環境のセキュリティ維持	・Windowsセキュリティパッチ、ウイルスパターンファイル自動アップデートの統合管理 ・セキュリティ対策状況のレポートの提出
情報漏えい防止ソフトの早期からの導入と定期的な監査	・内部関係者からの漏えいを防止するソフト ・PCの操作や機能を禁止・制御するだけではなく、必要に応じて許可する事が可能 ・ログ取得や不正操作に対する警告などの監視機能 ・外部デバイス及びネットワーク上へ出力したファイルの本体を複製保存 ・無線通信、PDA、USBリンクケーブルなど多様なデバイスからの漏えいを防止可能 ・クライアント側でのアンインストール不可能 ・ハードウェア、ソフトウェアに変更があった場合、即座に管理者へアラート通知 ・柔軟なファイル出力権限とアクティブディレクトリの組織単位、グループ及びユーザーごとに対応したポリシー設定が可能 ・当該情報漏えい防止ソフトがインストールされていないPCからのネットワークアクセスを禁止 ・行動制御、行動監視、資産管理、リモート管理を一つのコンソール画面で管理 ・情報の出力制限、暗号化、通信機能やソフトウェアの制御、ネットワーク利用の制限、監査ログ取得・分析の対応により 情報漏洩防止を徹底しながら効率良い運用が可能 ・社内の従業員、協力会社社員のPCへの導入と定期的な持ち出し監査を実施
Webコンテンツフィルタリングの導入と定期的な監査	・情報漏洩を防止する強力なフィルタリング機能、Webメール、ファイル共有サイト等にファイルがアップされる際に、 ファイルの中身を検知し、制御。 ・豊富なWebセキュリティ機能として、コンテンツフィルタリングの他にアンチウイルス、アンチマルウェア機能、URLフィルタリングを提供。 ・レポーティング機能として、フィルタリングにて禁止されたリスト等を提供
電子メールセキュリティ	・情報漏洩を防止する強力なフィルタリング機能 ・暗号化機能:暗号化ソフトとの連携 ・メール保留機能 ・内部統制にも有効なモニタリング機能 ・レポーティング機能、送受信メールをリアルタイムに分析 違反や傾向を迅速に把握可能
端末の不正接続防止 検疫ネットワーク	・PC検疫 許可されていないPCのネットワーク接続を防止 ポリシーに従っていないPCは検疫ネットワークにて検疫、治療されるまで基幹ネットワークへの接続を防止する仕組みを提供
RFID 電子透かし 電子割符	・暗号化、電子割符によるデータ保護、公開ドキュメントへのアクセス制御、RFIDによる持出し管理、電子透かし印刷 ・重要書類にRFIDタグを付与して、持ち出し管理やトレーサビリティを実現、情報管理の徹底や棚卸作業の効率化が図れる書類管理システム ・書類を格納したボックスとひも付けて格納場所の検索や管理も可能 ・担当者による書類の持出しに際して、当該作業を行う担当者と、取り扱われる書類の種別、管理番号等を特定し、作業記録として蓄積、また権限を超過した作業に対して警告 ・書類の搬出入の履歴をもとに、万一の紛失や情報漏洩が発生した際の最終貸出先の特定や、漏洩元捜索(トレーサビリティ)を実現 ・センター内に格納されている書類の一覧、それぞれの書類の保管年数などを把握し、棚卸の際の固定資産等の確認や使用されている書類の交換指示、不正持出しの早期検出 ・搬入時に、書類と格納するボックスを紐付け、検索や格納場所の管理、書類の格納されたボックスの把握や誤って格納された書類を棚卸時に自動判別
認証局の構築運用	電子署名法に対応した電子認証局からイントラネット向け電子認証局まで、目的や規模に応じた認証局の企画およびから構築・運用をトータルサポート
セキュリティ強化カーネル	・Linuxサーバー向けのセキュリティ強化カーネル ・アクセス制御機能を強化することで、システムへの不正侵入を防止 ・システム管理者が許可したい操作を一通り行うだけで、その操作のみを許可し、それ以外の操作を禁止できるポリシーを自動生成し、セキュリティポリシー作成の労力を大幅に削減 ・アプリケーションレベルでのアクセス制御を行うシステム(Webサーバ、データベースサーバ等)に存在する未知のセキュリティホールを攻撃してシステムに侵入されるという脅威に対する保険として利用 ・システム管理者が作成したポリシー(管理者権限を与えるけれども、必要なコマンドのみを操作可能とする等)に基づきファイルの読み書きやプログラムの実行を制限することで、セキュリティホールに起因する不正侵入に対する耐性を向上 ・セキュリティ修正プログラムの適用頻度を減らすことができるようになるため、動作確認試験のための稼動を削減可能 ・ログイン認証の強化や管理者業務の分担も実現

平成23年2月4日
海 上 保 安 庁

中国漁船衝突事件映像情報流出事案の概要について

1. 事案の概要

第五管区海上保安本部神戸海上保安部巡視艇乗組員（当時）が、平成22年11月4日、神戸市内において、動画サイト「YouTube」に中国漁船衝突事件映像情報（以下「衝突事件映像」という。）をアップロードし、故意にインターネット上に流出させたもの。

この衝突事件映像を流出させた職員が、衝突事件映像を入手した経路は以下のとおりであった。

（1） 平成22年9月17日、事件捜査のため、第十一管区海上保安本部職員は、行政情報システムの海上保安大学校のパブリックフォルダを用いて、衝突事件映像を海上保安大学校に伝送しようとしたが、この際、当該第十一管区海上保安本部職員と海上保安大学校職員の間で、衝突事件映像の削除についてきちんと確認しなかったため、同年9月17日から9月22日までの間、衝突事件映像が海上保安大学校のパブリックフォルダに掲載されたままとなり、不特定多数の海上保安庁職員が入手可能な状態となっていた。

（2） 同年9月19日、衝突事件映像を流出させた職員の同僚職員が、たまたま別の用件で、海上保安大学校のパブリックフォルダにアクセスしたところ、衝突事件映像を発見し、巡視艇の行政情報端末機に保存した。

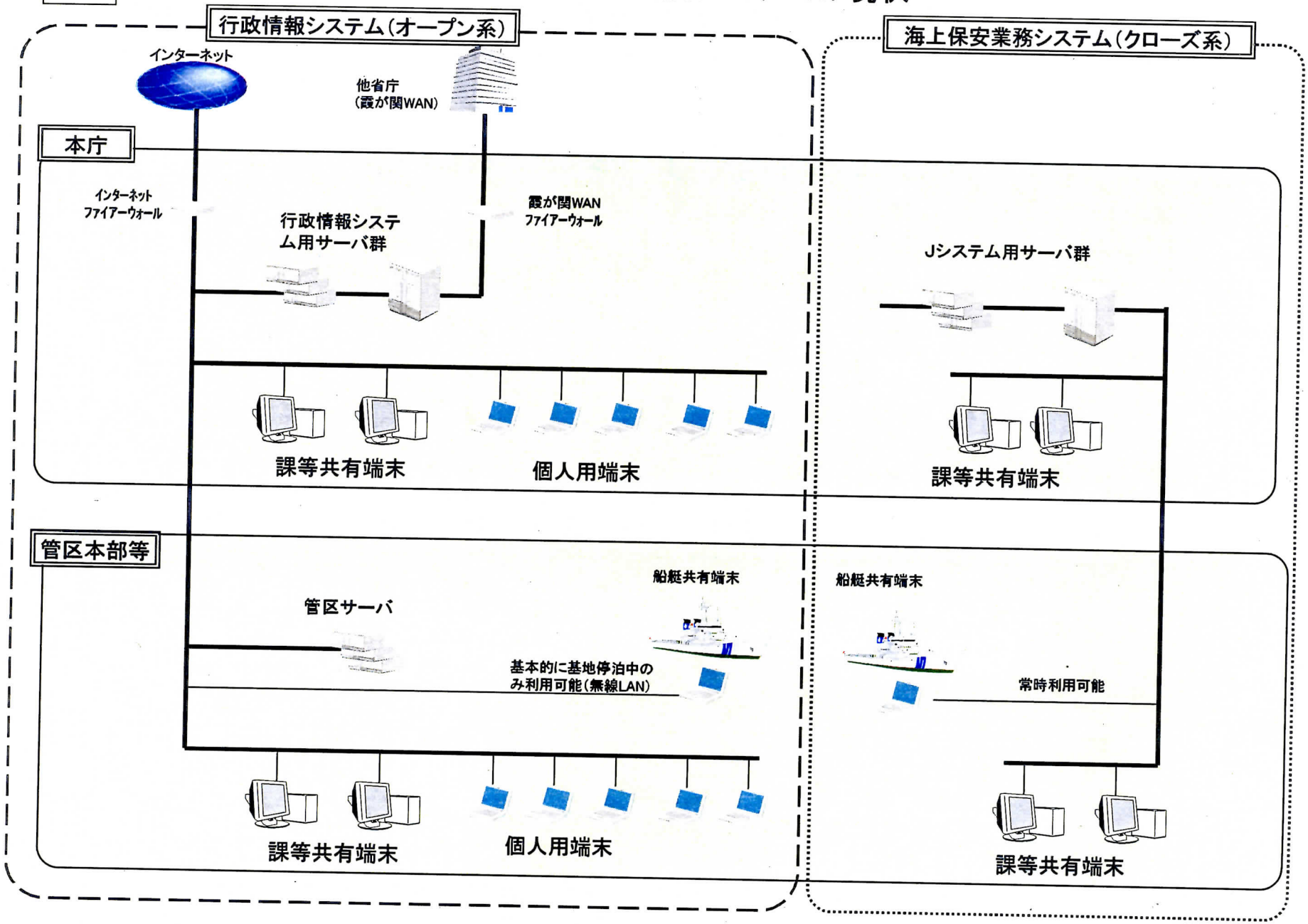
（3） 同年10月31日、衝突事件映像を流出させた職員は、当該行政情報端末機から衝突事件映像を私有USBメモリに保存し、部外に持ち出したもの。

2. システムの現状

別添のとおり。

別添

海上保安庁における主要システムの現状



平成23年２月４日
警　　察　　庁

警察における情報保全に関する取組みについて

１　経緯

平成22年12月16日（木）、警備局に情報保全に関するプロジェクト・チーム（以下「ＰＴ」という。）を設置。

ＰＴでは、警備部門における情報保全に関し、その実態について調査するとともに、今後の在り方を検討。

２　実地調査

(1)　調査の内容

警備部門における情報保全の実態について、全ての都道府県警察に対して実地調査を実施（平成22年11月16日～12月21日）。

(2)　調査の結果

外部記録媒体の使用履歴の証跡管理その他の管理が不十分と思われるコンピュータが一部存在することが判明。

(3)　改善措置の指導

調査の結果を踏まえ、取り急ぎ講ずるべき改善措置について、各都道府県警察に対し、個別の指導を実施。

【指導事項】

○　外部記録媒体を使用する機会の低減
○　データ保存時の暗号化措置の徹底　　等

３　全国警備関係庶務担当課長・情報管理課長会議の開催

(1)　日時

平成23年１月31日（月）

(2)　指示事項

情報保全に関する今後の在り方の検討結果等を踏まえ、情報保全の徹底・強化方策を全国警察に指示。

【主な指示事項】

○　情報の持ち出しを物理的に困難にする情報システムの確立
○　運用管理の徹底
○　情報保全の重要性を真に理解した人材の養成
○　警備部門と情報管理課及び情報通信部との緊密な連携

警察情報セキュリティポリシーにおける対策①

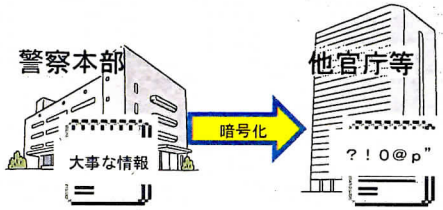
基本事項

ファイル共有ソフトの禁止

私有機器・媒体の公務使用禁止

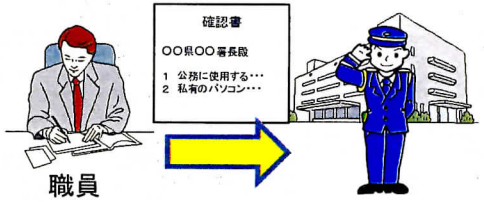
警察情報の無断持ち出し禁止

警察情報の適正な管理
異動期の情報管理の徹底



情報の持ち出し時の暗号化

意識向上対策



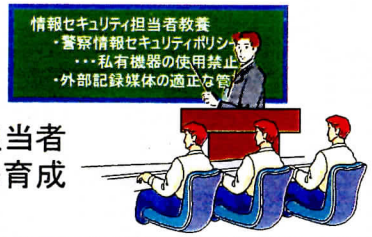
確認書の提出

小グループ検討会

監査・指導、教育

公用パソコンにおける
未登録外部記録媒体使用の点検

監査・業務指導



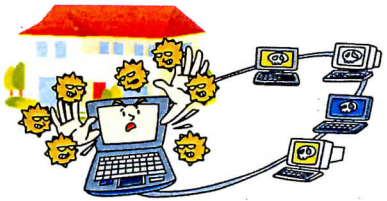
情報セキュリティ担当者
の育成

私有機器等に関する対策

私有パソコン等の自己点検

自己点検の検証

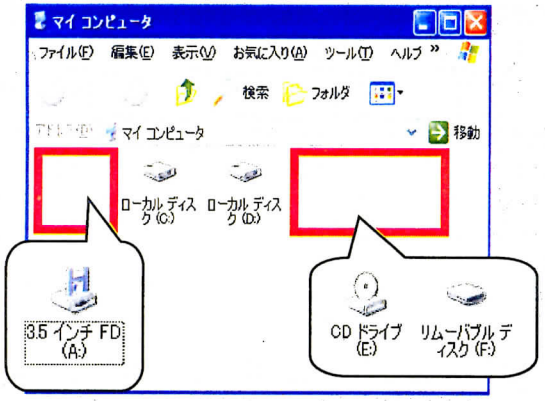
家族等に対する協力要請



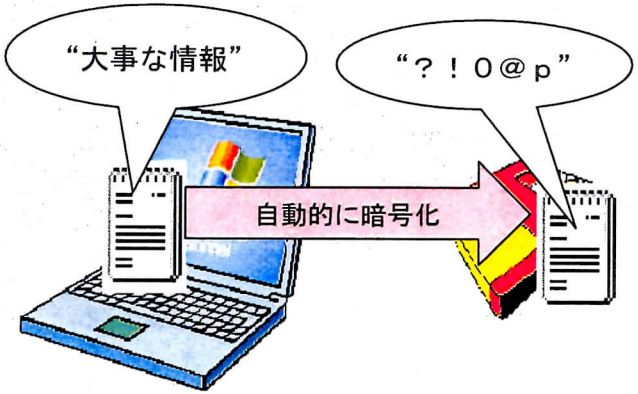
私有機器における
情報セキュリティ対策の教養

警察情報セキュリティポリシーにおける対策②

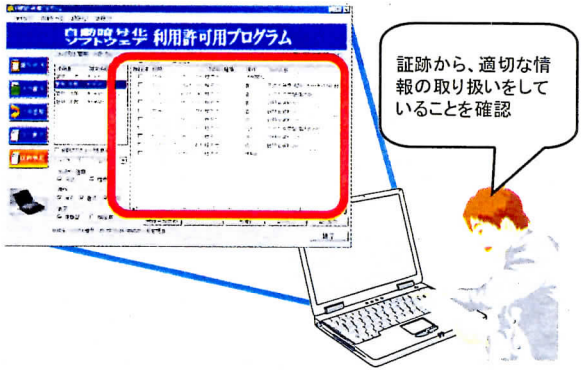
外部記録媒体等の情報セキュリティ対策の強化



メディアドライブの利用制限



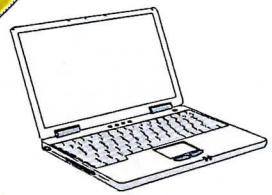
外部記録媒体への出力情報の暗号化



外部記録媒体の利用状況の検証

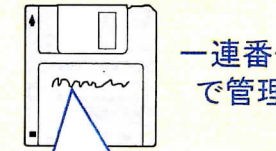
内蔵ハードディスクの自動暗号化

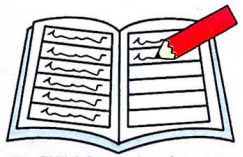
登録キーが書き込まれている媒体



端末

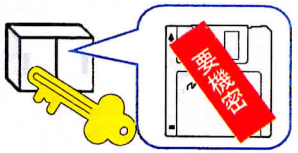
登録キーが書き込まれていない媒体





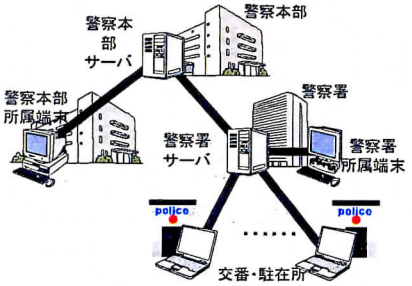
使用開始、廃棄、持ち出し等の使用状況を簿冊で管理

定期的に所在確認を行い、簿冊で管理



鍵のかかる保管庫で保管

外部記録媒体の管理



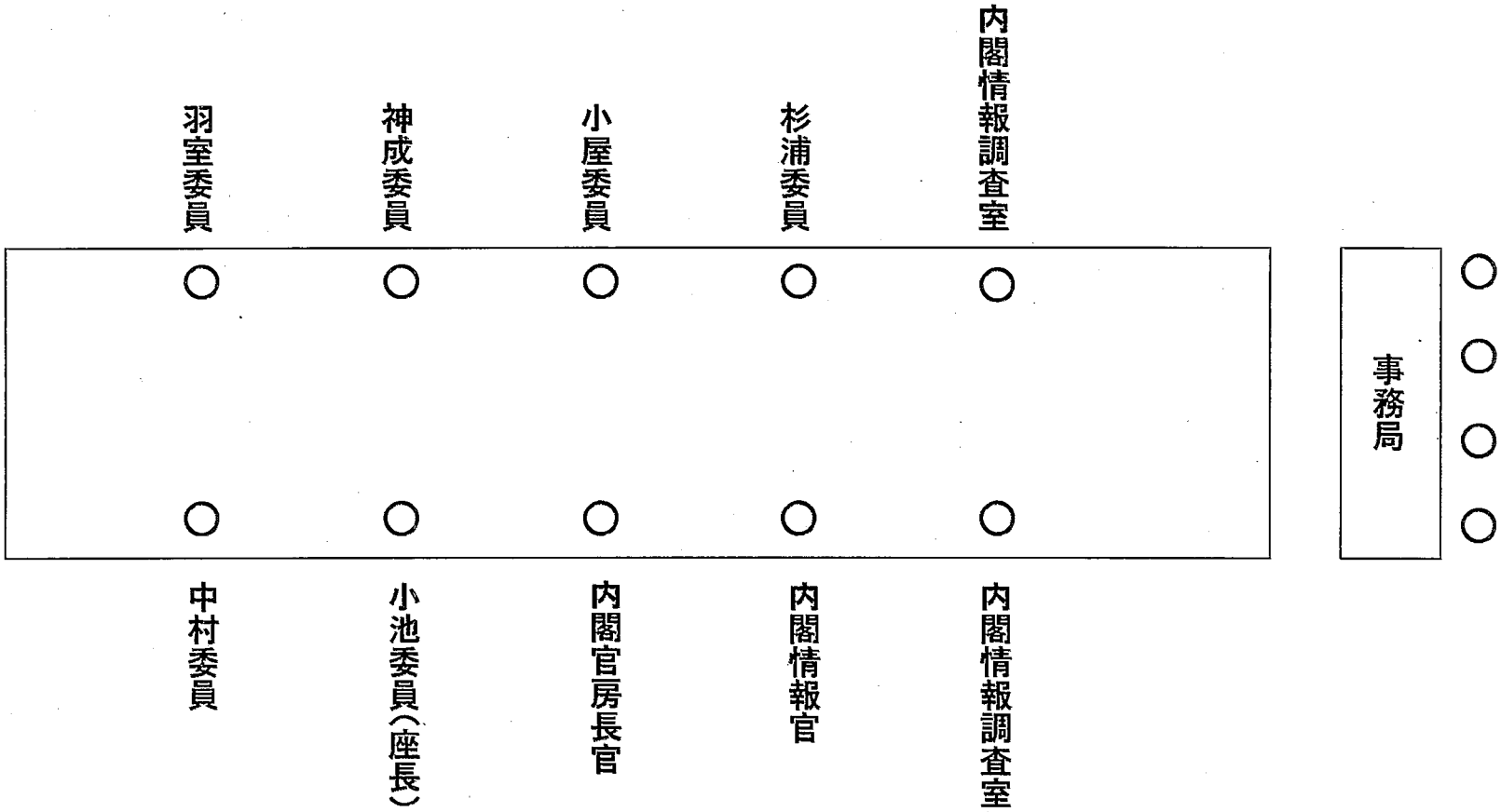
ファイルサーバの整備の促進

未登録外部記録媒体の利用制限

第3回情報保全システムに関する有識者会議　座席表

平成23年3月9日（水）午前9時30分～午前11時30分（概ね2時間）　於：官邸4階大会議室

（出入口）



配付資料

資料１　特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状について（追加調査）【席上回収】

資料２　想定される脅威及び対策ポイント【席上回収】

資料３　情報保全システム【席上回収】

資料４　考えられる対応策（案）【席上回収】

資料５　将来想定される脅威等に関する各委員の御説明資料

- 今後想定される脅威・対策等【羽室委員】
- 各府省庁等における機密性の高い情報を扱うシステムにおいて将来情報漏洩リスクとなり得るセキュリティ問題とその事前対策について【中村委員】
- 情報保全に関する脅威考察【小屋委員】
- この先５年の情報漏洩リスクの予測【杉浦委員】
- 先端技術の活用可能性【神成委員】

【機密性2情報】席上回収

配付資料1

特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状について（追加調査）

番号	項目		現状
1	システム構築、納入、保守等業者に対して提供する情報の管理	保護すべき情報を指定しているか。	[redacted]
		業者における保護すべき情報を取り扱う者を指定しているか。	
		業者における保護すべき情報の取り扱い手法を定めているか	
		再委託（孫請け）を行う際に、事前承認制とするなど、制限をしているか	
2	印刷物の破棄方法		
3	事後対策（事態の把握、被害拡大防止、広報等の対外対応等）に関し、マニュアルや対応要領を定めているか。		
4	ログの改ざん・消去への対策		

【機密性2情報】席上回収

配付資料2

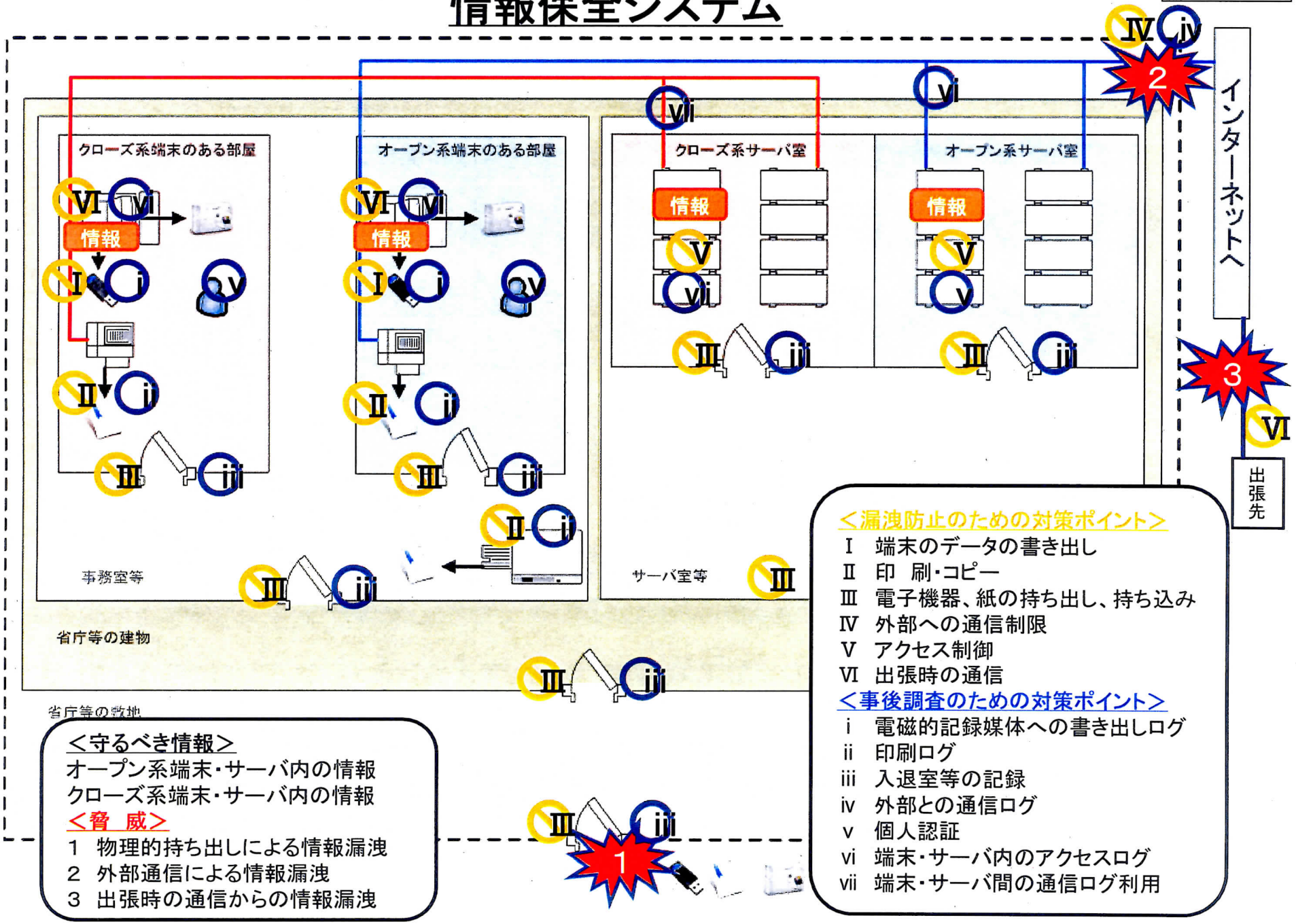
想定される脅威及び対策ポイント

脅威の概要	守るべき情報	具体的な脅威	対策ポイント	
			漏洩防止	事後調査
物理的持ち出しによる情報漏洩	オープン系 クローズ系	サーバ内データを電磁的記録媒体に書き出し、持ち出し	Ⅰ、Ⅲ、Ⅴ	i 、iii 、v vi 、vii
	オープン系 クローズ系	端末内データを電磁的記録媒体に書き出し、持ち出し	Ⅰ、Ⅲ、Ⅴ	i 、iii 、v vi 、vii
	オープン系 クローズ系	サーバ内データを印刷し、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii 、iii 、v vi 、vii
	オープン系 クローズ系	端末内データを印刷し、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii 、iii 、v vi 、vii
	オープン系 クローズ系	印刷したデータをコピーし、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii 、iii 、v vi 、vii
	オープン系 クローズ系	ディスプレイに表示されている情報を撮影し、持ち出し	Ⅲ	iii
外部通信による情報漏洩	オープン系	サーバ内データを外部との通信により漏洩	Ⅳ、Ⅴ	iv 、v 、vi 、 vii
	オープン系	端末内データを外部との通信により漏洩	Ⅳ、Ⅴ	iv 、v 、vi 、 vii
	クローズ系	サーバ内データを電磁的記録媒体に書き出し、オープン系にデータを移し、外部との通信により漏洩	Ⅰ、Ⅲ、Ⅳ Ⅴ	i 、iii 、iv 、 v 、vi 、vii
	クローズ系	端末内データを電磁的記録媒体に書き出し、オープン系にデータを移し、外部との通信により漏洩	Ⅰ、Ⅲ、Ⅳ Ⅴ	i 、iii 、iv 、 v 、vi 、vii
出張時の通信からの情報漏洩	モバイル端末	出張時の通信について通信経路上で情報を窃取される	Ⅵ	–

【機密性2情報】席上回収

配付資料3

情報保全システム



＜守るべき情報＞
オープン系端末・サーバ内の情報
クローズ系端末・サーバ内の情報

＜脅　威＞
1　物理的持ち出しによる情報漏洩
2　外部通信による情報漏洩
3　出張時の通信からの情報漏洩

＜漏洩防止のための対策ポイント＞
Ⅰ　端末のデータの書き出し
Ⅱ　印　刷・コピー
Ⅲ　電子機器、紙の持ち出し、持ち込み
Ⅳ　外部への通信制限
Ⅴ　アクセス制御
Ⅵ　出張時の通信

＜事後調査のための対策ポイント＞
i　電磁的記録媒体への書き出しログ
ii　印刷ログ
iii　入退室等の記録
iv　外部との通信ログ
v　個人認証
vi　端末・サーバ内のアクセスログ
vii　端末・サーバ間の通信ログ利用

【機密性2情報】席上回収

考えられる対応策（案）　1／6

配付資料4

端末のデータの書き出し

- 漏洩防止のための対策　（Ⅰ）
  - a システム的に強制力のある制限（以下のa-1又はa-2のいずれかの対策を取る）
    - a-1　許可がなければ書き出しを禁止、例外措置を講ずる場合の許可手順
    - a-2　特別な手段がないと復号できない方法により強制的に暗号化、例外措置を講ずる場合の許可手順
  - b 私用電磁的記録媒体の使用制限（以下のb-1又はb-2のいずれかの対策を取る）
    - b-1　個体識別が可能な電磁的記録媒体について、登録済のもの（公用電磁的記録媒体等）以外の電磁的記録媒体を接続した場合に使用不可能とする
    - b-2　私用・公用にかかわらず書き出しても自動暗号化され特別な手段がない限り復号不可能とする
    - インターフェースの形状の特殊化
  - c 暗号化による書き出しデータの保護
    - 電磁的記録媒体への書き出し時に自動暗号化され特別な手段がない限り復号不可能とする

- 事後調査のための対策　（ｉ）
  - a システム的に強制力のある制限の例外措置を講ずる場合の記録及びその監査
  - b 電磁的記録媒体への書き出し時にログを保存
  - c 電磁的記録媒体への書き出し時のログの監査
  - d 公用電磁的記録媒体の適切な保管（原則として集中保管）　※
  - e 公用電磁的記録媒体の定期的な所在確認　※
  - [redacted]

凡例
赤字：オープン系・クローズ系ともにとるべき対策
橙字：クローズ系においてとるべき対策
緑字：必要に応じてとるべき対策
※　：システム上の対策が困難なため、システム以外の対策となっているもの

【機密性2情報】席上回収

考えられる対応策(案)　2／6

凡例
赤字:オープン系・クローズ系ともにとるべき対策
橙字:クローズ系においてとるべき対策
緑字:必要に応じてとるべき対策
※　:システム上の対策が困難なため、システム以外の対策となっているもの

印　刷・コピー

－　漏洩防止のための対策　（Ⅱ）

a　印刷時のプリンタ認証
b　決められたプリンタでのみの印刷を許可
c　特に機密性の高い情報の印刷時の管理者の許可(必要に応じ保全担当者の立会い)　※
d　課・室外への印刷出力の禁止
e　印刷物への取扱い区分の明示　※
f　特に機密性の高い情報の印刷時の複製防止用紙の使用　※
g　特に機密性の高い情報の印刷物への持ち出し防止タグの取付け
h　印刷物への日付、印刷者名(アカウント情報)等の刷り込み
i　指定された出力元以外からの印刷防止(プリンタのパラレル、USB各ポート及びSDカードスロット、無線LANポート等の物理的(論理的)閉鎖)
j　コピー機のメモリ情報の管理
k　コピー機(特に複合機)のセキュリティ機能の活用(認証機能とアクセス制限機能、情報漏洩防止機能及びネットワークセキュリティ機能等)
l　コピー保守業者のコピー機設定情報の確認と設定の認証　※
m　複合機のプリンター機能、FAX機能、スキャナー機能の使用許可(制限)と機能設定

－　事後調査のための対策　（ⅱ）

a　プリンタの印刷ログの取得
b　印刷者名(アカウント情報)の確実な管理
c　プリンタ・コピー機周辺に取り忘れ、紛失防止のための監視カメラの設置
d　特に機密性の高い情報の印刷時の管理者の許可の履歴の監査(保全担当者の立会いの履歴の監査)　※

[redacted]

【機密性2情報】席上回収

考えられる対応策(案)　3／6

電子機器(PC、携帯電話、カメラ、電磁的記録媒体等)、紙の持ち出し、持ち込み

– 漏洩防止のための対策 (Ⅲ)

a 執務室(サーバ室含む。)への許可された電子機器以外の持ち込み禁止・制限 ※
b 執務室(サーバ室含む。)への出入りに際し、電子機器の持ち込み状況の確認のため、抜き打ち検査の実施 ※
c 執務室(サーバ室含む。)における執務中の電子機器の持ち込み状況の確認のため、抜き打ち検査の実施 ※
d 保守業者に対するクリアランスの確認 (P)
e 保守業者のサーバ室出入りの確認、作業の立会い及び監督 ※
f 保守用電子機器持ち込み時の確認と申請等手続きの確立。履歴の記録と持ち出し時の確認 ※
g 電磁的記録媒体の修理・交換時の確実な消去の確認 ※
h 特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に関する持ち出し防止タグを用いた検出機能
i 職員のIDカード等による入退館管理(特に機密性の高い情報を扱う執務室(サーバ室含む。)では生体認証も併用)

– 事後調査のための対策 (ⅲ)

a 保守業者に対するクリアランスの確認資料の保存 (P)
b 保守業者のサーバ室出入りの記録 ※
c 保守用電子機器持ち込み時の記録 ※
d 特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に関する持ち出し防止タグ検出機能のログの保存
e IDカード等による入退館の記録及び生体認証の記録
f 特に機密性の高い情報を扱う執務室(サーバ室含む。)の入退室映像の保存
[redacted]

凡例
赤字:オープン系・クローズ系ともにとるべき対策
橙字:クローズ系においてとるべき対策
緑字:必要に応じてとるべき対策
※　:システム上の対策が困難なため、システム以外の対策となっているもの
(P) :具体的な方法について別途検討を要する

【機密性2情報】席上回収

考えられる対応策(案)　4／6

外部への通信制限

- 漏洩防止のための対策 （Ⅳ）
  - a ホワイトリストによる通信の制限
    業務に必要な通信のみを許可
  - b ブラックリストによる通信の制限
    業務に不必要な通信を制限
    - 民間が運営しているフリーのWebメールの使用禁止
    - 掲示板サイトへの通信制限(アクセスを禁止、書き込みを禁止)
    - 市販のWebフィルタリングソフトウエアを導入し、カテゴリ別で通信を制限

- 事後調査のための対策 （ⅳ）
  - a 許可している通信を考慮に入れたログの取得
  - b 取得したログの定期的な監査
  - [redacted]

凡例
青字：オープン系においてとるべき対策

【機密性2情報】席上回収

考えられる対応策（案）　5／6

アクセス制御

- 漏洩防止のための対策 （V）
  - a 個人認証
    登録された本人のみがログインできる仕組み（生体認証方式の採用等）
  - b 確実なアクセス制御の実施
    ファイル・フォルダごとのアクセス制限の実施
    ファイルを作成する際にアクセス制限を強制的にかけるような仕組みの導入

- 事後調査のための対策 （v 、vi 、vii）
  - a 個人認証ログの取得
  - b 端末ーサーバ間の通信ログの取得
  - c 端末・サーバ内それぞれのファイルアクセスログの取得
  - d 取得したログの定期的な監査
  - [redacted]

凡例
赤字：オープン系・クローズ系ともにとるべき対策
橙字：クローズ系においてとるべき対策
緑字：必要に応じてとるべき対策

考えられる対応策(案)　6／6

出張時の通信

- 漏洩防止のための対策 (Ⅵ)
  - a 出張先において電子機器により特に機密性の高い情報に関し通信をやむを得ず行う場合には、クローズ系専用回線と同等の暗号化を講じた回線(衛星回線、VPN)を用いる
  - b 上記回線に接続する出張用端末については、紛失時に備えて、ハードディスク上における必要な暗号化措置等を講ずる

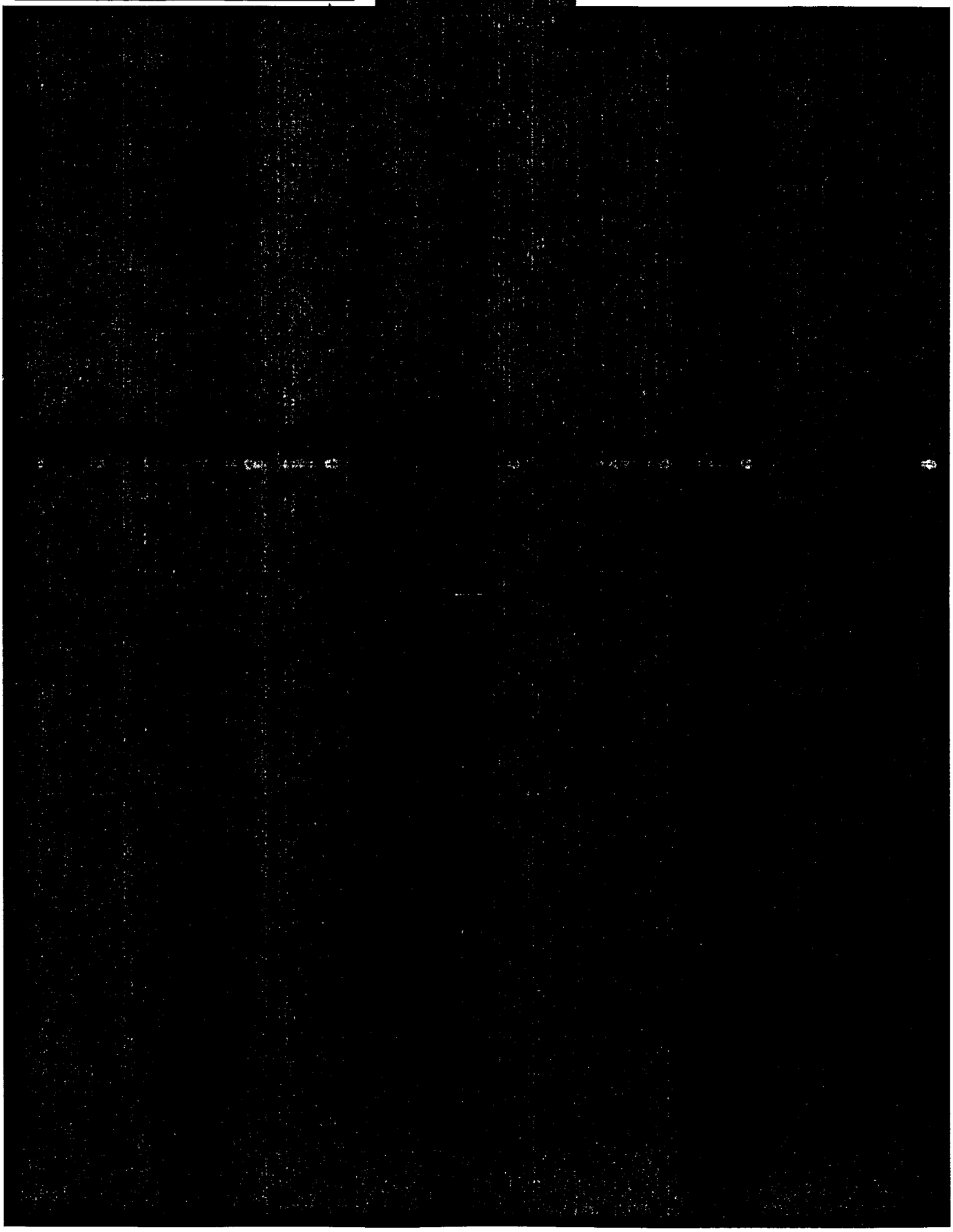
機密性２情報

配付資料５

将来予想される脅威等に関する各委員の御説明資料

今後想定される脅威・対策等

non-paper　羽室　英太郎



【機密性２情報】

各府省庁等における機密性の高い情報を扱うシステムにおいて将来情報漏洩リスクとなり得るセキュリティ問題とその事前対策について

防衛大学校　中村康弘

[redacted]

【機密性２情報】

[redacted]

【機密性２情報】

[redacted]

【機密性２情報】

[redacted]

【機密性２情報】

情報保全に関する脅威考察

トレンドマイクロ株式会社
小屋　晋吾

[redacted]

【機密性２情報】

[redacted]

【機密性２情報】

この先５年の情報漏洩リスクの予測

2011/3/1

ネットエージェント株式会社
杉浦　隆幸

[redacted]

【機密性２情報】

[redacted]

【機密性２情報】

[redacted]

【機密性2情報】

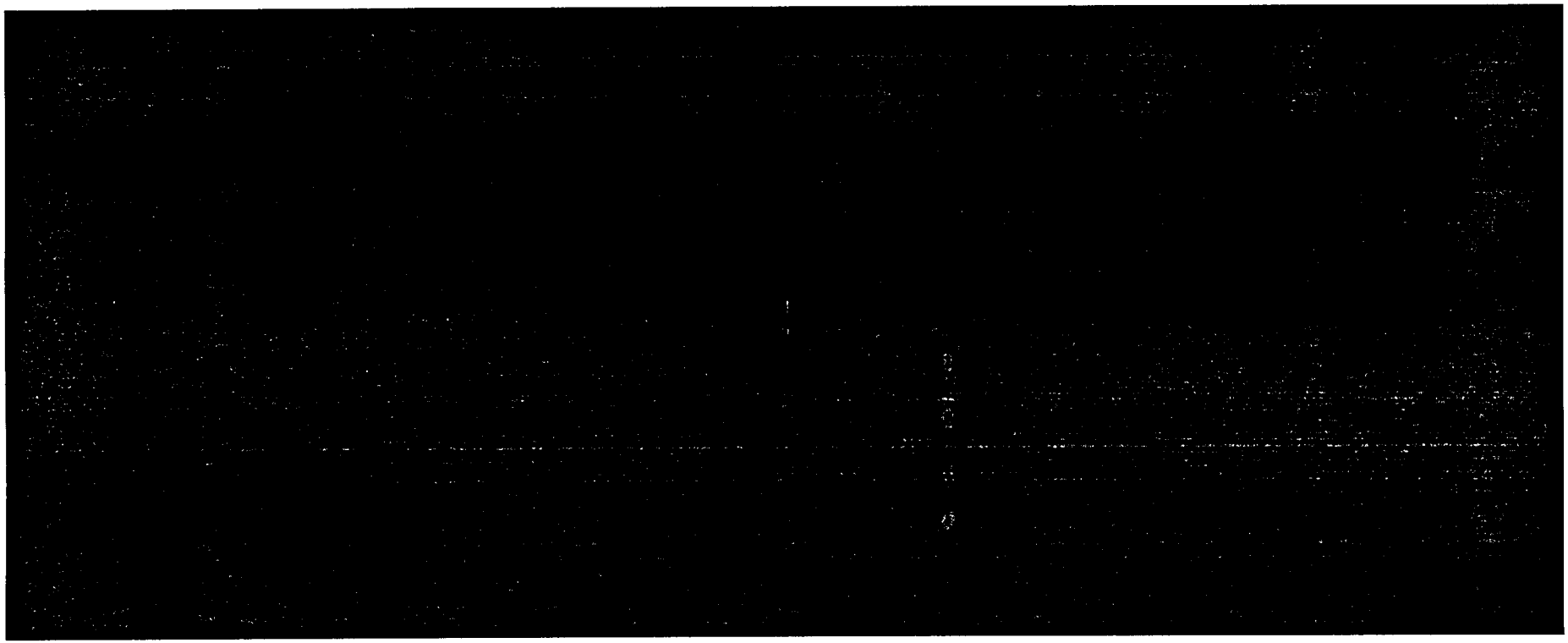
先端技術の活用可能性

2011年3月9日

慶應義塾大学
神成　淳司

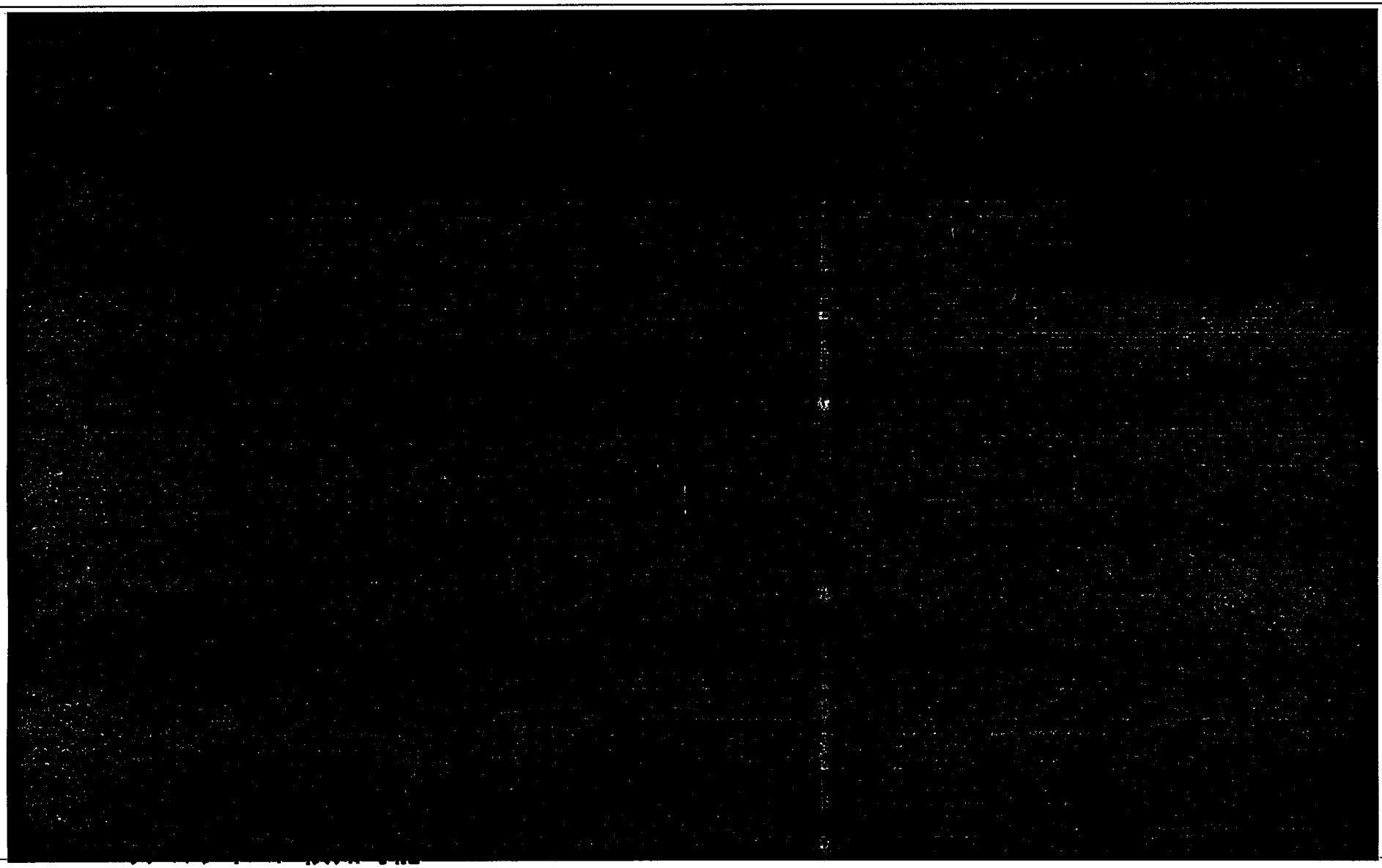
【機密性2情報】

[redacted]

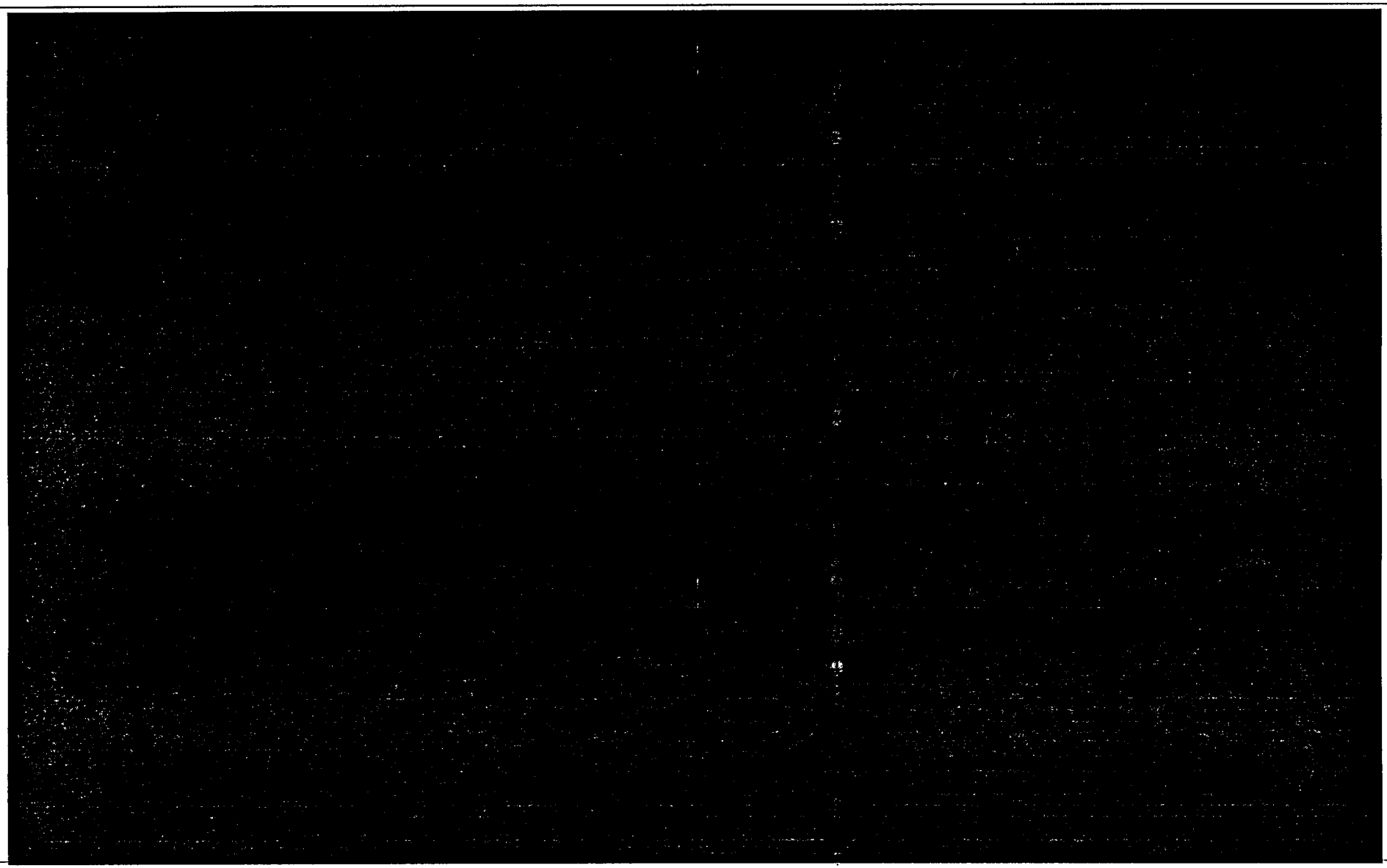


【機密性2情報】

[redacted]

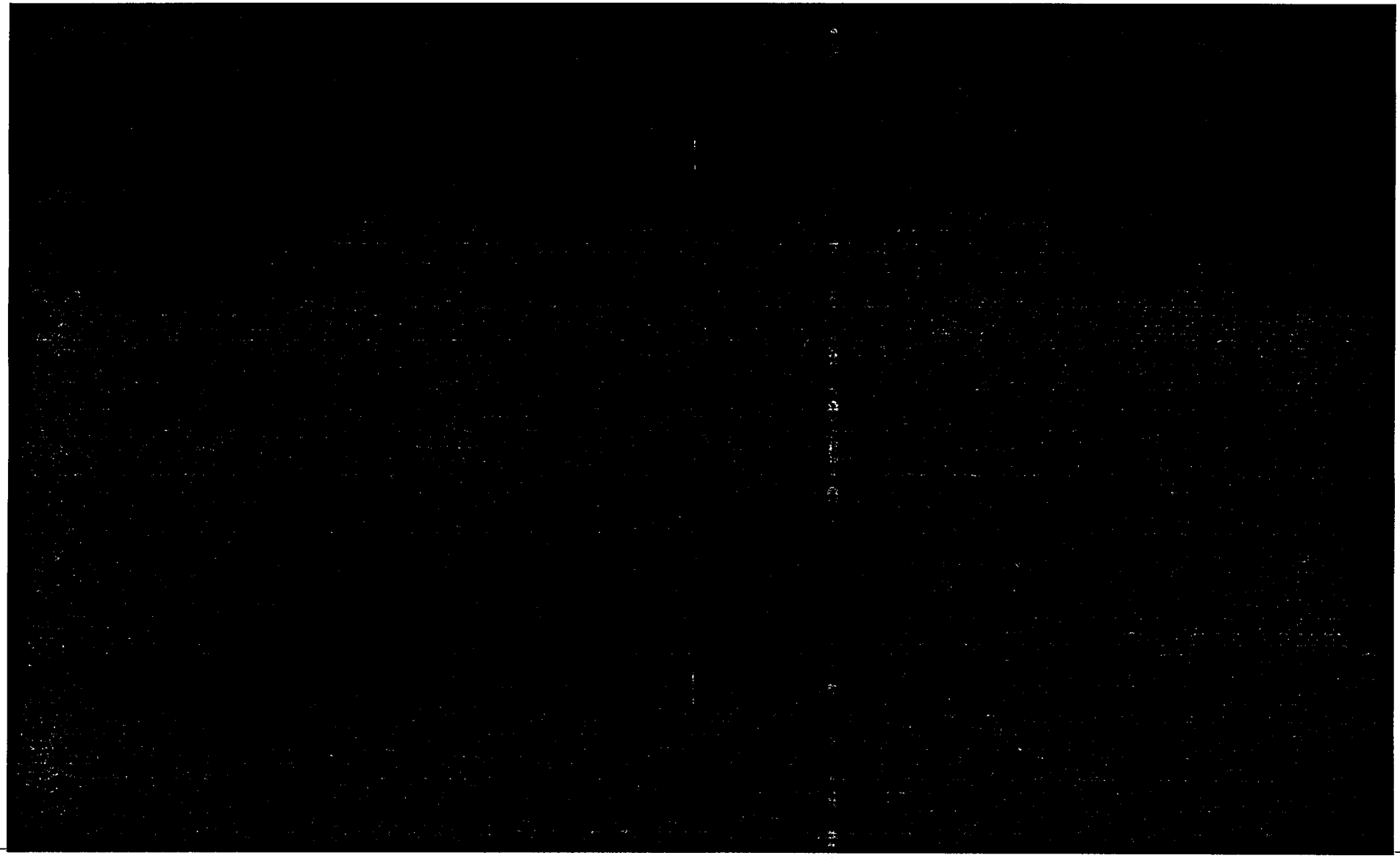


【機密性2情報】 [redacted]



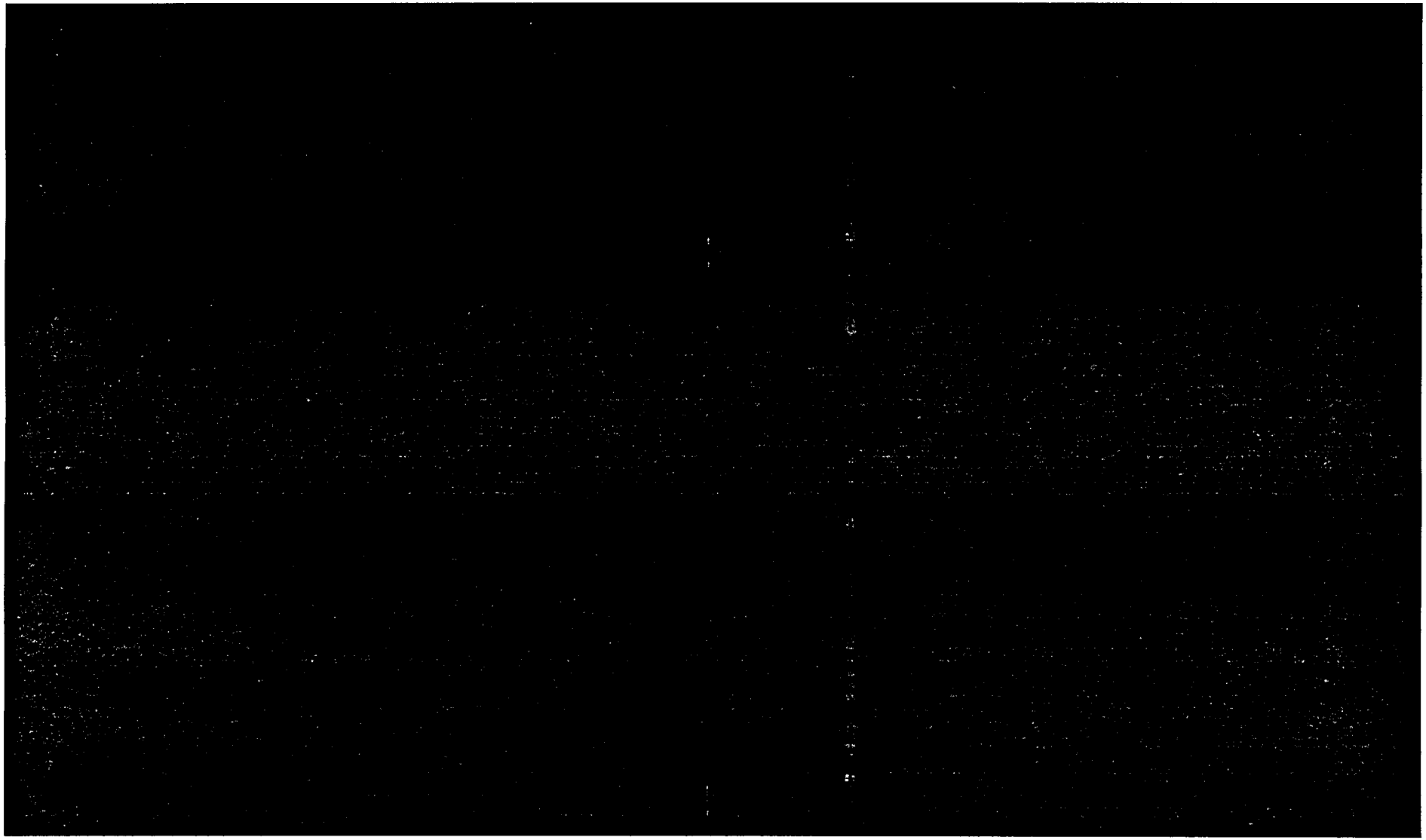
【機密性2情報】

[redacted]



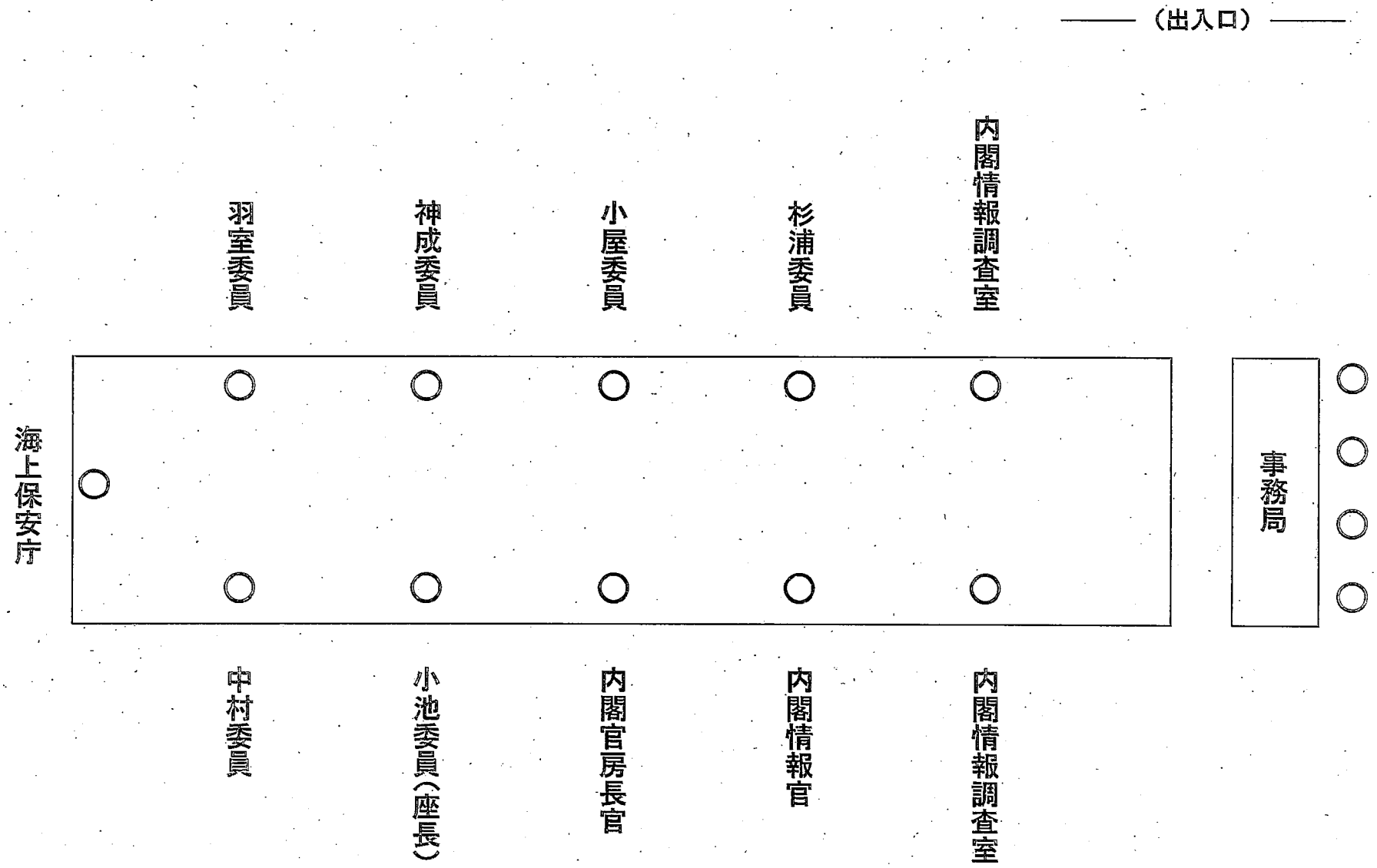
【機密性2情報】

[redacted]



第4回情報保全システムに関する有識者会議　座席表

平成23年5月20日（金）午後1時30分～午後3時30分　於：官邸4階大会議室



機密性２情報（関係者限り）

配布資料

特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について

（報告書）

（案）

平成２３年５月　日

情報保全システムに関する有識者会議

機密性２情報（関係者限り）

はじめに

当会議は、昨年１２月、政府における情報保全に関する検討委員会から、特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について意見を示すよう要請を受け、以後数次にわたる会合において議論を重ねてきた。本報告書は、これらの議論を踏まえ、特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し特に留意すべき事項について、当会議としての意見を取りまとめたものである。

Ⅰ　総論

ＩＴ技術やネットワーク社会の進展が著しい現在、情報が一旦ネットワーク上に流出するや極めて短期間に世界規模で広がり、もはや取り返しのつかない事態に陥ってしまう。こうした環境の中で、我が国政府における情報保全の万全をいかに図るかが極めて重要な課題になっている。

情報保全を図る上で、情報を取り扱う職員に対する教育など、人的な面での対策の強化が不可欠であることは論をまたないが、同時に、職員による故意の情報漏洩のリスクが常に存在することも念頭に置き、万一職員が情報漏洩を企図しても物理的に困難、もしくは後日判明するという心理的抑止力のためその証拠が保全されるように、システム上必要な対策が講じられていなければならない。

当会議では、特別管理秘密等の特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状や、過去発生した情報漏洩事案及び事後強化した対策等を踏まえた上で、守るべき情報、対象となるシステム及び想定される脅威について整理し、情報漏洩防止等のために必要と考えられる措置について取りまとめた。

情報漏洩を防止する観点からは、情報の取扱いについてあらかじめ厳しい制限を加えることとしがちであるが、それだけでは、運用面に過大な負担を与える場合があることから、業務に支障のないように、実情を踏まえバランスの取れた対策を実施することが求められる。

また、情報漏洩のリスクを完全にゼロにすることは不可能であるため、事前予防だけでなく、万が一漏洩事案が発生した際には迅速に状況を把握して適切な事後対応を可能とするための対策にも力を入れることが肝要である。

ＩＴ技術の急速な発展を踏まえると、情報保全システムに対する脅威も逐次変化することが想定される。当会議では、将来想定される脅威についても議論を行ったところ、特に機密性の高い情報を取り扱う政府機関においては、技術の動向やこれらを悪用した脅威について常に情報収集を行い、途切れることなく適時適切に対策をとっていく必要がある。

第１　守るべき情報及び対象となるシステム

当会議では、守るべき情報として、特別管理秘密をはじめとした特に機密性の高い情報を念頭に置き、議論を行った。特に機密性の高い情報を取り扱う政府機関においては、これらの情報をインターネットと接続されていないクローズ系のシステムで取り扱っている。また、クローズ系のシステムとは別に、インターネットに接続されたオープン系のシステムがあり、外部との連絡等に使っている。情報漏洩防止のため、機密性の高い情報を含む文書の作成や保存は、原則としてクローズ系のシステムで行い、オープン系のシステムではできないものとしている。

以上を踏まえれば、特に機密性の高い情報の漏洩防止のためのシステム上の対策としては、基本的にクローズ系のシステムのサーバ及び端末内の情報が同システムの外部に流出することがないように必要な措置を講じれば足りるように思われる。

しかしながら、実務上は、外部との連絡のためクローズ系のシステムから機密性の低い情報を電磁的記録媒体へ書き出し、オープン系のシステムに読み込む必要がある場合がある。この際、不正プログラム等により、本来クローズ系にあるべき機密性の高い情報が全く意図せずに電磁的記録媒体に書き込まれる可能性があり、オープン系で当該電磁的記録媒体を読み込んだ際に、機密性の高い情報がオープン系に移され、さらにインターネットを通じて外部に流出するおそれは否定できない。

以上から、オープン系のシステムについても、特に機密性の高い情報の流出経路となるおそれがあるという観点から、所要の措置を講じる必要がある。

一方、スタンドアロン端末については、現状では、出張時の記録に使用するなど特段機密性の高い情報を取り扱わないものと、クローズ系以上に機密性の高い情報を取り扱うためにネットワークを構成していないものがある。一般にスタンドアロン端末は管理が十分に行き届かない傾向にあると言われることから、スタンドアロン端末についてはその必要性について検討し、運用するに当たっては、厳格な管理を徹底する必要がある。

第２　想定される脅威

情報漏洩の脅威として、①物理的持ち出しによる情報漏洩、②外部通信による情報漏洩、③出張時の通信からの情報漏洩を想定している。（別添１参照）

物理的持ち出しによる情報漏洩とは、管理区域内の執務室等に設置された情報システムから、管理区域外に通信以外の方法でデータが持ち出されることであり、例としては、情報システムから電磁的記録媒体にデータを書き出し、当該電磁的記録媒体を物理的に管理区域外に持ち出すことが挙げられる。

次に、外部通信による情報漏洩とは、管理区域内の執務室等に設置された情報システムから、管理区域外に通信によってデータが送出されることであり、例としては、オープン系システムの端末からインターネットに情報が送信されることが挙げられる。

また、出張時の通信からの情報漏洩とは、出張先から本府省庁に通信を行う場合に通信経路上で情報を窃取されることである。出張時には、出張者と本府省庁間で機密性の高い情報の送受信が発生しうるところ、当該送受信を可能な限り安全に行うための基準についても例外的な措置として設けることとした。

第３　対策ポイント

守るべき情報及び対象となるシステム、そして想定される脅威について整理した上で、必要と考えられる措置を６項目にまとめ、各項目ごとに漏洩防止のための対策ポイント及び事後調査のための対策ポイントを設定した（下表及び別添２参照）。漏洩防止のための対策ポイントは、データの電磁的記録媒体への書き出しや紙への出力等についてシステム上で強制力を持って制限するこ

とにより、直接的に情報漏洩を防ぐための対策のポイントである。一方、事後調査のための対策ポイントは、データに対して行われた操作等を記録し、事後的に確認することを可能としておくことにより、事案発生時に漏洩の範囲等被害状況を迅速に把握し、適切な事後対応を行うための対策のポイントである。

情報保全システムに必要と考えられる措置は多岐に渡るところ、現時点で最も優先されるべき喫緊の対策は、電磁的記録媒体へのデータの書き出し制限及びログの保存である。インターネットを介した情報漏洩対策について以前から取り組まれているのに比べ、電磁的記録媒体を介した情報漏洩については、昨今の情報漏洩事案の経路になるなど対策が遅れている上、電磁的記録媒体の記憶容量が大きいことから情報漏洩が発生した場合の被害が大きくなるおそれが高い。以上から、電磁的記録媒体へのデータの書き出しを的確に制限することが求められる。ログの保存については、情報漏洩のリスクを完全にゼロにすることが不可能であり、特に情報を管理する立場の者による故意の漏洩に対してはログの検証による事後的追及以外に対策がないため、必須である。また、ログが残ること自体が不正行為に対する抑止力となることも期待される。

＜必要と考えられる措置及び対策ポイント＞（下線は喫緊の課題）

必要と考えられる措置		漏洩防止のための対策ポイント	事後調査のための対策ポイント
1	端末のデータの書き出し対策	電磁的記録媒体への書き出し制限（Ⅰ）	電磁的記録媒体への書き出しログ（ⅰ）
2	印刷・コピー対策	印刷・コピーの制限（Ⅱ）	印刷ログ（ⅱ）
3	電子機器及び紙の持ち出し及び持ち込み対策	電子機器及び紙の持ち出し及び持ち込みの制限（Ⅲ）	入退館等の記録（ⅲ）
4	外部への通信制御	外部への通信制限（Ⅳ）	外部との通信ログ（ⅳ）
5	アクセス制御	アクセス制限（Ⅴ）	個人認証（ⅴ） 端末・サーバ内のアクセスログ（ⅵ） 端末・サーバ間の通信ログ（ⅶ）
6	出張時の通信対策	出張時に使用する端末及び通信回線の制限（Ⅵ）	－

Ⅱ　各論

第１　必要と考えられる措置

個別の措置については別添３参照。

なお、必要と考えられる措置には、システム上の措置だけではなく、システム上の対策が困難なためシステム以外の対策となっているものも含まれている。

１　端末のデータの書き出し対策

総論でも触れたとおり、クローズ系のシステムで管理している機密性の高い情報がその外部に出る契機となるのは、クローズ系の端末から電磁的記録媒体へのデータの書き出しであるから、これについて適切に管理することが極めて重要である。

一方、本来機密性の高い情報を取り扱わないこととしているオープン系のシステムについても、電磁的記録媒体を介して機密性の高い情報が移されるおそれがあり、そうした場合には、オープン系がインターネットを通じた外部への情報流出の経路となる可能性のみならず、オープン系端末から当該情報が更に別の電磁的記録媒体に書き出されてしまう可能性も否定できない。このため、端末から電磁的記録媒体へのデータの書き出しについては、オープン系においてもクローズ系に準じた措置が必要であると考えられる。

端末からのデータの書き出しについては、単に規則で制限し、職員にその遵守を求めるに留まらず、システム上強制力のある制限を行うことが必要である。具体的には、端末から電磁的記録媒体へ書き出す際に自動的に暗号化を行い、

当該媒体のデータは組織外の端末では復号できないようにするなどの措置が想定される。組織外の端末で利用できる形で書き出すことが必要な場合には、管理者の許可を得てこれを行うこととする。

次に、私用の電磁的記録媒体を持ち込み、これにデータを書き出すことも大きなリスクであることから、これについても規則で禁止するだけではなく、システム上であらかじめ登録されていない電磁的記録媒体を検知して使用不可とする措置や、仮に私用の電磁的記録媒体にデータを書き込んだとしても、組織外の端末では利用できないことにする措置などが必要である。

また、日常的に発生する電磁的記録媒体への書き出しが適切に行われていることを事後的に確認可能とするため、電磁的記録媒体へのデータの書き出しに関するログや許可の記録を必要十分な期間保存し、定期的に監査を行うことが求められる。公用の電磁的記録媒体の持ち出しを防止するため、原則として集中保管し、定期的に所在確認を行うことなども必要である。

さらに、書き出したデータのトレーサビリティを確保するため、必要に応じ、電子データに電子透かしを導入すること等について検討することが望ましい。

２　印刷・コピー対策

守るべき情報がクローズ系のシステムの外へ出ていく経路としては、プリンタにより印刷した文書や、それをさらにコピー機により複製した文書が物理的に持ち出されることも挙げられる。印刷物等は、電磁的記録媒体と比較すればその情報量に限りがあるが、プリンタやコピー機は一般に複数の職員が共用しているため、印刷した者が不明確となったり、印刷物の取り忘れが起こるおそ

れがあり、ひいては情報の不要な拡散へとつながる可能性がある。

これらを踏まえ、印刷やコピーについても組織的な管理により、必要な者が必要なだけ行うことを担保することが必要である。システム上は、コピー機やプリンタ等に備えられた認証機能等のセキュリティ機能を活用するほか、印刷に関するログや許可の記録を必要十分な期間保存し、定期的に監査を行うことが求められる。

また、必要に応じ、監視カメラの設置や複製防止用紙の利用、持ち出し防止タグの取付け等についても導入を検討することが望ましい。

３　電子機器（ＰＣ、携帯電話、カメラ、電磁的記録媒体等）及び紙の持ち出し及び持ち込み対策

守るべき情報が外部に流出する場合の経路として、外部との通信のほか、当該情報が記録された電子機器や紙が物理的に管理区域外に持ち出されることが考えられる。これを防止するためには、電子機器及び紙の持ち出し及び持ち込みを制限する必要がある。

職員については、あらかじめ許可された電子機器以外は持ち込み禁止とし、抜き打ち検査等によって抑止力を持たせるほか、ＩＤカード等による入退館、入退室の管理を適切に行う必要がある。また、電子機器及び紙の持ち出しについては、必要に応じ、特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に持ち出し防止タグを貼付し、庁舎の出入り口等において検知する機能を備えることについて検討することが望ましい。

一方、保守業者等がサーバ室等に立ち入り、保守等の作業を行うことが避け

られないところ、保守業者等のサーバ室等への出入りや電子機器の持ち込みについても管理する必要がある。

さらに、電子機器の持ち込み、入退館及び入退室の記録やログを必要十分な期間保存し、定期的に監査を行うことが求められる。

４　外部への通信制御

総論でも触れたとおり、インターネットと接続されているオープン系システムについては、外部との通信によって職員の意図と関係なくデータが不正に送出されるおそれがある。このため、業務に必要な通信のみを許可し、不必要な通信を制限することとともに、通信のログを必要十分な期間保存し、定期的に監査を行うことにより情報漏洩を防止する必要がある。

５　アクセス制御

情報保全においては、「Need to Know」の原則の徹底が不可欠であるところ、システム上はアクセス制御がその基盤となるものである。

個人認証については、データに対する操作を行った本人を事後的に特定できることを担保する必要があり、あらかじめ登録された本人のみがログインできる生体認証方式の採用等が求められる。また、ユーザーがファイルを作成する際にアクセス制限を自動的にかける仕組みを導入するなど、アクセス制限を確実に実施する必要がある。

また、個人認証ログ、端末・サーバ内のアクセスログ、端末とサーバ間の通信ログ等を必要十分な期間保存し、定期的に監査を行うことが求められる。

６　出張時の通信対策

出張者と本府省庁間で特に機密性の高い情報の送受信を業務上やむを得ず行う場合には、出張者が使用する端末においては常時暗号化を講じた通信回線を使用すること及び当該端末については紛失等に備え、ハードディスクの暗号化等を行っておくことが必要である。

７　その他

上記１から６の中には整理していないが、定期的な監査等を行うための体制整備や訓練の実施、委託先における情報の取扱いの管理や、印刷物の廃棄方法、ログの改ざんへの対策など、これまでに述べた諸対策の実効性を高めるための対策は多岐に渡っている。これらについても必要に応じて実施すべきことは言うまでもない。

また、無線ＬＡＮについては、暗号を破る技術が年々進化しているため、専門家の意見を聞きながらセキュリティ対策の更新を随時行わなければ、安全性を確保することは難しい。また、無線ＬＡＮを導入するに当たっては、無線ＬＡＮが使用不可能となった場合を想定して、有線通信等を用いた代替手段を備えておく必要がある。

第２　将来想定される脅威

情報保全に関わる電子機器や技術は多岐に渡り、これらに関連する将来の脅威として多様なものが想定されうるところ、最近社会的に利用が拡大し、近い

将来、特に機密性の高い情報の漏洩防止等の観点から対応を検討する必要性が高いものとして、以下のものが挙げられる。さらに、技術的進歩の速度を踏まえると、今後新たな技術を悪用した脅威に晒されるおそれは十分にあることから、特に機密性の高い情報を取り扱う政府機関においては、常に関連する情報の収集及び分析を行い、途切れることなく適時適切に対策をとっていく必要がある。

○　スマートフォン

現在普及が進んでいるスマートフォンについては、ユーザーによるソフトウェアのインストールを制限することが困難であるなどの問題がある。機密性の高い情報を取り扱う場合は、こうしたスマートフォンの機能や脆弱性などを踏まえ、使用を制限する又はその安全性を十分に確保するための特段の措置をとるなどの対応を検討する必要がある。

○　クラウドコンピューティング

クラウドコンピューティングには、海外サーバを利用する場合の情報保全上のリスク、大量の演算を安価に行うことができるようになることにより暗号解読の可能性が高まるリスク、特定の業者を使い続けないと業務が継続できなくなるリスクなども指摘されており、その安全性が十分に確保されるまでは、機密性の高い情報の取り扱いに関し、使用を制限するなどの対応を検討する必要がある。

おわりに

特に機密性の高い情報を取り扱う政府機関の情報保全システムの確立は、我が国を取り巻く現下の厳しい情勢にかんがみれば、まさに喫緊の課題である。

当会議としては、政府において、本報告書の内容を十分踏まえつつ、①守るべき情報が確実に保護されるシステムとすること、②運用面に過度の負担を与えることのないシステムとすること、③万一情報漏洩等の事案が発生した際は、迅速かつ適切な事後対応が可能なシステムとすることの３点を基本とし、国家と国民の発展に資する情報保全システムに必要と考えられる対策が速やかに進められること、及びその進捗状況が適切にフォローアップされることを強く期待するものである。

別添1

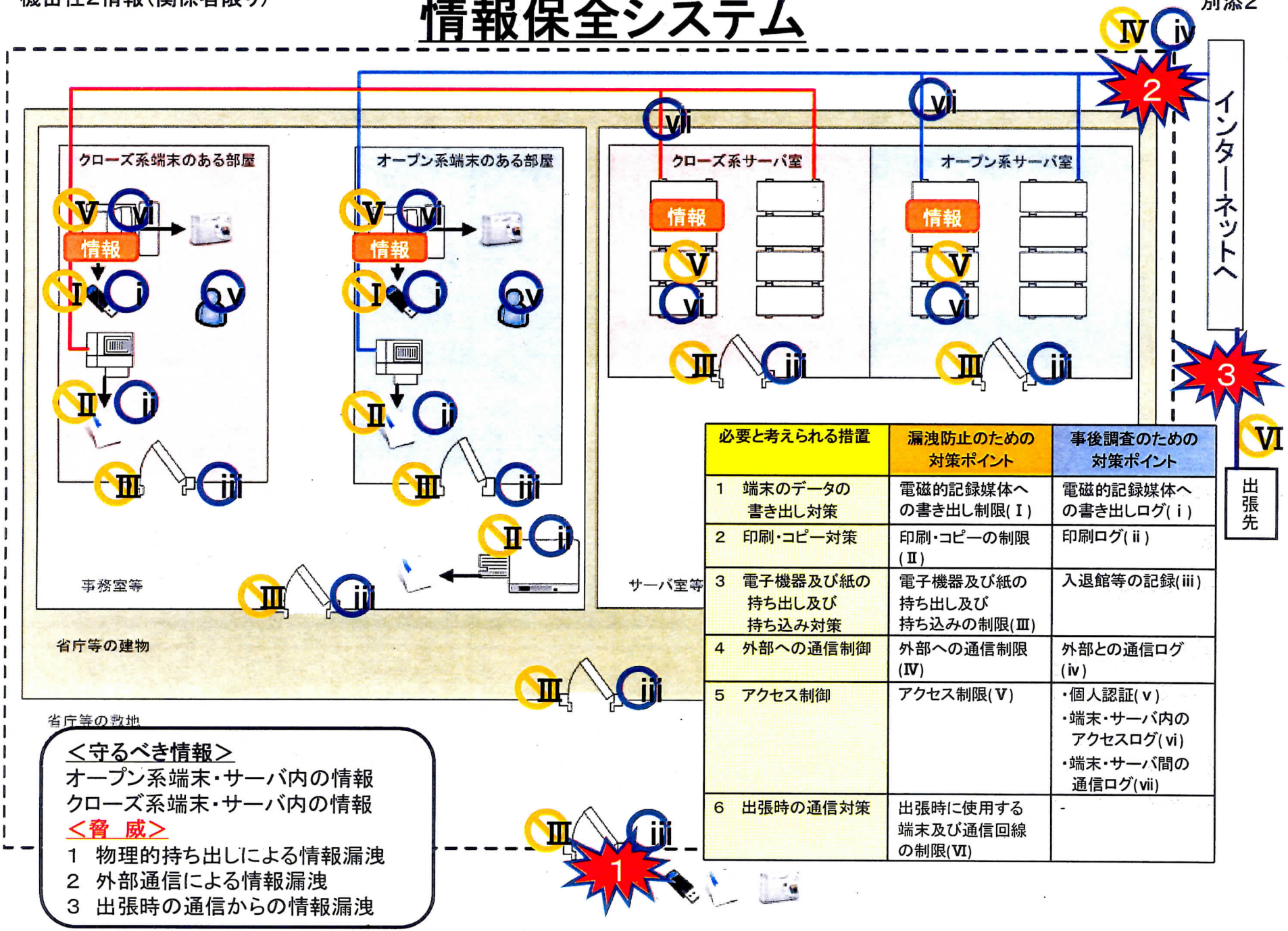
想定される脅威及び対策ポイント

脅威の概要	対象となるシステム	具体的な脅威	対策ポイント	
			漏洩防止	事後調査
物理的持ち出しによる情報漏洩	オープン系 クローズ系	サーバ内データを電磁的記録媒体に書き出し、持ち出し	Ⅰ、Ⅲ、Ⅴ	i、iii、v vi、vii
	オープン系 クローズ系	端末内データを電磁的記録媒体に書き出し、持ち出し	Ⅰ、Ⅲ、Ⅴ	i、iii、v vi、vii
	オープン系 クローズ系	サーバ内データを印刷し、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii、iii、v vi、vii
	オープン系 クローズ系	端末内データを印刷し、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii、iii、v vi、vii
	オープン系 クローズ系	印刷したデータをコピーし、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii、iii、v vi、vii
	オープン系 クローズ系	ディスプレイに表示されている情報を撮影し、持ち出し	Ⅲ	iii
外部通信による情報漏洩	オープン系	サーバ内データを外部との通信により漏洩	Ⅳ、Ⅴ	iv、v、vi、vii
	オープン系	端末内データを外部との通信により漏洩	Ⅳ、Ⅴ	iv、v、vi、vii
	クローズ系	サーバ内データを電磁的記録媒体に書き出し、オープン系にデータを移し、外部との通信により漏洩	Ⅰ、Ⅲ、Ⅳ Ⅴ	i、iii、iv、 v、vi、vii
	クローズ系	端末内データを電磁的記録媒体に書き出し、オープン系にデータを移し、外部との通信により漏洩	Ⅰ、Ⅲ、Ⅳ Ⅴ	i、iii、iv、 v、vi、vii
出張時の通信からの情報漏洩	出張時の端末及び通信回線	出張時の通信について通信経路上で情報を窃取される	Ⅵ	－

機密性2情報（関係者限り）

別添2

情報保全システム



必要と考えられる措置	漏洩防止のための対策ポイント	事後調査のための対策ポイント
1　端末のデータの書き出し対策	電磁的記録媒体への書き出し制限(Ⅰ)	電磁的記録媒体への書き出しログ(ⅰ)
2　印刷・コピー対策	印刷・コピーの制限(Ⅱ)	印刷ログ(ⅱ)
3　電子機器及び紙の持ち出し及び持ち込み対策	電子機器及び紙の持ち出し及び持ち込みの制限(Ⅲ)	入退館等の記録(ⅲ)
4　外部への通信制御	外部への通信制限(Ⅳ)	外部との通信ログ(ⅳ)
5　アクセス制御	アクセス制限(Ⅴ)	・個人認証(ⅴ) ・端末・サーバ内のアクセスログ(ⅵ) ・端末・サーバ間の通信ログ(ⅶ)
6　出張時の通信対策	出張時に使用する端末及び通信回線の制限(Ⅵ)	-

＜守るべき情報＞
オープン系端末・サーバ内の情報
クローズ系端末・サーバ内の情報

＜脅　威＞
1　物理的持ち出しによる情報漏洩
2　外部通信による情報漏洩
3　出張時の通信からの情報漏洩

必要と考えられる措置

1　端末のデータの書き出し対策

－　漏洩防止のための対策　（Ｉ）

a　システム上で強制力のある制限（次のa-1又はa-2のいずれかの対策をとる）

a-1　許可がなければ書き出しを禁止、例外措置を講ずる場合の許可手順

a-2　特別な手段がないと復号できない方法により強制的に暗号化、例外措置を講ずる場合の許可手順

b　私用電磁的記録媒体の使用制限（次のb-1又はb-2のいずれかの対策をとる）

b-1　個体識別が可能な電磁的記録媒体について、登録済のもの（公用電磁的記録媒体等）以外の電磁的記録媒体を接続した場合に使用不可能とする

b-2　私用・公用にかかわらず書き出しても自動暗号化され特別な手段がない限り復号不可能とする

インターフェースの形状の特殊化

c　暗号化による書き出しデータの保護

電磁的記録媒体への書き出し時に自動暗号化され特別な手段がない限り復号不可能とする

－　事後調査のための対策　（ｉ）

a　システム上で強制力のある制限の例外措置を講ずる場合の記録及びその監査

b　電磁的記録媒体への書き出し時にログを保存

c　電磁的記録媒体への書き出し時のログの監査

d　公用電磁的記録媒体の適切な保管（原則として集中保管）　※

e　公用電磁的記録媒体の定期的な所在確認　※

[redacted]

g 電磁的記録媒体への書き出し時に電子透かしを入れる

凡例
赤字：オープン系・クローズ系ともにとるべき対策
緑字：必要に応じてとるべき対策
※　：システム上の対策が困難なため、システム以外の対策となっているもの

必要と考えられる措置

凡例
赤字：オープン系・クローズ系ともにとるべき対策
橙字：クローズ系においてとるべき対策
緑字：必要に応じてとるべき対策
※　：システム上の対策が困難なため、システム以外の対策となっているもの

2　印　刷・コピー対策

－　漏洩防止のための対策　（Ⅱ）

a　印刷時のプリンタ認証
b　決められたプリンタでのみの印刷を許可
c　特に機密性の高い情報の印刷時の管理者の許可（必要に応じ保全担当者の立会い）　※
d　課・室外への印刷出力の禁止
e　印刷物への取扱い区分の明示　※
f　特に機密性の高い情報の印刷時の複製防止用紙の使用　※
g　特に機密性の高い情報の印刷物への持ち出し防止タグの取付け
h　印刷物への日付、印刷者名（アカウント情報）等の刷り込み
i　指定された出力元以外からの印刷防止（プリンタのパラレル、USB各ポート及びSDカードスロット、無線LANポート等の物理的（論理的）閉鎖）
j　コピー機のメモリ情報の管理
k　コピー機（特に複合機）のセキュリティ機能の活用（認証機能とアクセス制限機能、情報漏洩防止機能及びネットワークセキュリティ機能等）
l　コピー保守業者のコピー機設定情報の確認と設定の認証　※
m　複合機のプリンター機能、FAX機能、スキャナー機能の使用許可（制限）と機能設定

－　事後調査のための対策　（ⅱ）

a　プリンタの印刷ログの取得
b　印刷者名（アカウント情報）の確実な管理
c　プリンタ・コピー機周辺に取り忘れ、紛失防止のための監視カメラの設置
d　特に機密性の高い情報の印刷時の管理者の許可の履歴の監査（保全担当者の立会いの履歴の監査）　※
[redacted]

必要と考えられる措置

3　電子機器(PC、携帯電話、カメラ、電磁的記録媒体等)及び紙の持ち出し及び持ち込み対策

－　漏洩防止のための対策　（Ⅲ）

a　執務室（サーバ室含む。）への許可された電子機器以外の持ち込み禁止・制限　※
b　執務室（サーバ室含む。）への出入りに際し、電子機器の持ち込み状況の確認のため、抜き打ち検査の実施　※
c　執務室（サーバ室含む。）における執務中の電子機器の持ち込み状況の確認のため、抜き打ち検査の実施　※
d　保守業者に対するクリアランスの確認　※
e　保守業者のサーバ室出入りの確認、作業の立会い及び監督　※
f　保守用電子機器持ち込み時の確認と申請等手続きの確立。履歴の記録と持ち出し時の確認　※
g　電磁的記録媒体の修理・交換時の確実な消去の確認　※
h　特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に関する持ち出し防止タグを用いた検出機能
i　職員のIDカード等による入退館管理（特に機密性の高い情報を扱う執務室（サーバ室含む。）では生体認証も併用）

－　事後調査のための対策　（ⅲ）

a　保守業者に対するクリアランスの確認資料の保存　※
b　保守業者のサーバ室出入りの記録　※
c　保守用電子機器持ち込み時の記録　※
d　特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に関する持ち出し防止タグ検出機能のログの保存
e　IDカード等による入退館の記録及び特に機密性の高い情報を扱う執務室（サーバ室含む。）に係る生体認証の記録
f　特に機密性の高い情報を扱う執務室（サーバ室含む。）の入退室映像の保存
[redacted]

凡例
赤字：オープン系・クローズ系ともにとるべき対策
橙字：クローズ系においてとるべき対策
緑字：必要に応じてとるべき対策
※　：システム上の対策が困難なため、システム以外の対策となっているもの

必要と考えられる措置

4 外部への通信制御

- 漏洩防止のための対策 （Ⅳ）
  - a ホワイトリストによる通信の制限
    業務に必要な通信のみを許可
  - b ブラックリストによる通信の制限
    業務に不必要な通信を制限
    - 民間が運営しているフリーのWebメールの使用禁止
    - 掲示板サイトへの通信制限（アクセスを禁止、書き込みを禁止）
    - 市販のWebフィルタリングソフトウエアを導入し、カテゴリ別で通信を制限

- 事後調査のための対策 （ⅳ）
  - a 許可している通信を考慮に入れたログの取得
  - b 取得したログの定期的な監査
  - [redacted]

凡例
青字：オープン系においてとるべき対策

必要と考えられる措置

5　アクセス制御

- 漏洩防止のための対策　（Ⅴ）
  - a　個人認証
    登録された本人のみがログインできる仕組み（生体認証方式の採用等）
  - b　確実なアクセス制御の実施
    ファイル・フォルダごとのアクセス制限の実施
    ファイルを作成する際にアクセス制限を強制的にかけるような仕組みの導入

- 事後調査のための対策　（ⅴ、ⅵ、ⅶ）
  - a　個人認証ログの取得
  - b　端末－サーバ間の通信ログの取得
  - c　端末・サーバ内それぞれのファイルアクセスログの取得
  - d　取得したログの定期的な監査
  - [redacted]

凡例
赤字：オープン系・クローズ系ともにとるべき対策

6　出張時の通信対策

- 漏洩防止のための対策　（Ⅵ）
  - a　出張先において電子機器により特に機密性の高い情報に関し通信をやむを得ず行う場合には、クローズ系専用回線と同等の暗号化を講じた回線（衛星回線、VPN）を用いる
  - b　上記回線に接続する出張用端末については、紛失時に備えて、ハードディスク上における必要な暗号化措置等を講ずる

機密性２情報　　会議後回収

平成２３年５月㉙㉚日
海　上　保　安　庁

情報流出再発防止対策検討委員会中間報告書（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、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　情報流出再発防止のために必要な改善策

（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

３　委員会報告の実施とフォローアップ

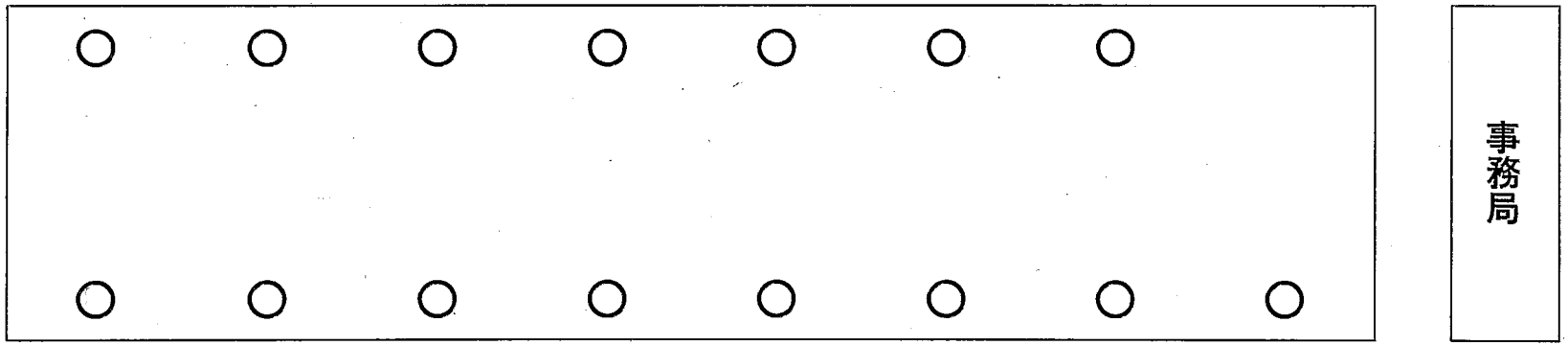
（１）本報告書で提言された改善策を可能な限り、速やかに実施

（２）「政府における情報保全に関する検討委員会」の検討結果を踏まえ、必要に応じて追加的提言を行い、最終取りまとめを実施

第2回政府における情報保全に関する検討委員会　座席表

平成23年7月1日（金）午後4時30分～午後5時　於：官邸4階大会議室

（出入口）



配付資料一覧

資料１　情報保全システムに関する有識者会議における検討状況

資料２　情報保全システムに関する有識者会議　報告書の骨子

資料３　情報保全システムに関する有識者会議　報告書
「特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について」

資料４　情報保全システムに関する有識者会議　報告書公表版

資料５　特に機密性の高い情報を取り扱う政府機関の情報保全システムの強化に向けた取組の推進について（案）

機密性３情報

配付資料３

特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について

（報告書）

平成２３年７月１日

情報保全システムに関する有識者会議

機密性３情報

目次

機密性３情報

はじめに

当会議は、昨年１２月、政府における情報保全に関する検討委員会から、特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し必要と考えられる措置について意見を示すよう要請を受け、以後数次にわたる会合において議論を重ねてきた。本報告書は、これらの議論を踏まえ、特に機密性の高い情報を取り扱う政府機関の情報保全システムに関し特に留意すべき事項について、当会議としての意見を取りまとめたものである。

Ⅰ　総論

ＩＴ技術やネットワーク社会の進展が著しい現在、情報が一旦ネットワーク上に流出するや極めて短期間に世界規模で広がり、もはや取り返しのつかない事態に陥ってしまう。こうした環境の中で、我が国政府における情報保全の万全をいかに図るかが極めて重要な課題になっている。

情報保全を図る上で、情報を取り扱う職員に対する教育など、人的な面での対策の強化が不可欠であることは論をまたないが、同時に、職員による故意の情報漏洩のリスクが常に存在することも念頭に置き、万一職員が情報漏洩を企図しても物理的に困難、もしくは後日判明するという心理的抑止力のためその証拠が保全されるように、システム上必要な対策が講じられていなければならない。情報漏洩を防止する観点からは、情報の取扱いについてあらかじめ厳しい制限を加えることとしがちであるが、それだけでは、運用面に過大な負担を与える場合があることから、業務に支障のないように、実情を踏まえバランスの取れた対策を実施することが求められる。

また、情報漏洩のリスクを完全にゼロにすることは不可能であるため、事前予防だけでなく、万が一漏洩事案が発生した際には迅速に状況を把握して適切な事後対応を可能とするための対策にも力を入れることが肝要である。

当会議では、以上のような認識の下、特別管理秘密等の特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状や、過去発生した情報漏洩事案及び事後強化した対策等を踏まえた上で、守るべき情報、対象となるシステム及び想定される脅威について整理し、情報漏洩防止等のために必要と考えられる措置について取りまとめた。

特に機密性の高い情報を取り扱う政府機関においては、その取り扱う情報の性質にかんがみ、すべての政府機関に適用される情報セキュリティ対策の基準を定めた「政府機関の情報セキュリティ対策のための統一基準群」を遵守するほか、当会議が取りまとめた「必要と考えられる措置」を確実に実施することが求められる。

ＩＴ技術の急速な発展を踏まえると、情報保全システムに対する脅威も逐次変化することが想定される。当会議では、今後顕在化が想定される脅威についても議論を行ったところ、特に機密性の高い情報を取り扱う政府機関においては、技術の動向やこれらを悪用した脅威について常に情報収集を行い、途切れることなく適時適切に対策をとっていく必要がある。

第１　守るべき情報及び対象となるシステム

当会議では、守るべき情報として、特別管理秘密をはじめとした特に機密性の高い情報を念頭に置き、議論を行った。特に機密性の高い情報を取り扱う政

府機関においては、これらの情報をインターネットと接続されていないクローズ系のシステムで取り扱っている。また、クローズ系のシステムとは別に、インターネットに接続されたオープン系のシステムがあり、外部との連絡等に使っている。情報漏洩防止のため、機密性の高い情報を含む文書の作成や保存は、原則としてクローズ系のシステムで行い、オープン系のシステムではできないものとしている。

以上を踏まえれば、特に機密性の高い情報の漏洩防止のためのシステム上の対策としては、基本的にクローズ系のシステムのサーバ及び端末内の情報が同システムの外部に流出することがないように必要な措置を講じれば足りるように思われる。

しかしながら、実務上は、外部との連絡のためクローズ系のシステムから機密性の低い情報を電磁的記録媒体へ書き出し、オープン系のシステムに読み込む必要がある場合がある。この際、不正プログラム等により、本来クローズ系にあるべき機密性の高い情報が全く意図せずに電磁的記録媒体に書き込まれる可能性があり、オープン系で当該電磁的記録媒体を読み込んだ際に、機密性の高い情報がオープン系に移され、さらにインターネットを通じて外部に流出するおそれは否定できない。

以上から、クローズ系のシステムから電磁的記録媒体へのデータの書き出しについては、その要否及び内容について管理者が確認するなど、組織的に管理し、クローズ系から機密性の高い情報が不正に書き出されることのないように対策を実施する必要があるが、同時に、オープン系のシステムについても、特に機密性の高い情報の流出経路となるおそれがあるという観点から、所要の措

置を講じる必要がある。

一方、スタンドアロン端末については、現状では、出張時の記録に使用するなど特段機密性の高い情報を取り扱わないものと、クローズ系以上に機密性の高い情報を取り扱うためにネットワークを構成していないものがある。一般にスタンドアロン端末は管理が十分に行き届かない傾向にあると言われることから、スタンドアロン端末についてはその必要性について検討し、運用するに当たっては、厳格な管理を徹底する必要がある。

第２　想定される脅威

情報漏洩の脅威として、①物理的持ち出しによる情報漏洩、②外部通信による情報漏洩、③出張時の通信からの情報漏洩を想定している。（別添１参照）

物理的持ち出しによる情報漏洩とは、管理区域内の執務室等に設置された情報システムから、管理区域外に通信以外の方法でデータが持ち出されることであり、例としては、情報システムから電磁的記録媒体にデータを書き出し、当該電磁的記録媒体を物理的に管理区域外に持ち出すことが挙げられる。

次に、外部通信による情報漏洩とは、管理区域内の執務室等に設置された情報システムから、管理区域外に通信によってデータが送出されることであり、例としては、オープン系システムの端末からインターネットに情報が送信されることが挙げられる。

また、出張時の通信からの情報漏洩とは、出張先から本府省庁に通信を行う場合に通信経路上で情報を窃取されることである。出張時には、出張者と本府省庁間で機密性の高い情報の送受信が発生しうるところ、当該送受信を可能な限り安全に行うための基準についても例外的な措置として設けることとした。

第３　対策ポイント

守るべき情報及び対象となるシステム、そして想定される脅威について整理した上で、必要と考えられる措置を６項目にまとめ、各項目ごとに漏洩防止のための対策ポイント及び事後調査のための対策ポイントを設定した（下表及び別添２参照）。漏洩防止のための対策ポイントは、データの電磁的記録媒体への書き出しや紙への出力等についてシステム上で強制力を持って制限することにより、直接的に情報漏洩を防ぐための対策のポイントである。一方、事後調査のための対策ポイントは、データに対して行われた操作等を記録し、事後的に確認することを可能としておくことにより、事案発生時に漏洩の範囲等被害状況を迅速に把握し、適切な事後対応を行うための対策のポイントである。

情報保全システムに必要と考えられる措置は多岐にわたるところ、現時点で最も優先されるべき喫緊の対策は、電磁的記録媒体へのデータの書き出し制限及びログの保存である。インターネットを介した情報漏洩対策について以前から取り組まれているのに比べ、電磁的記録媒体を介した情報漏洩については、昨今の情報漏洩事案の経路になるなど対策が遅れている上、電磁的記録媒体の記憶容量が大きいことから情報漏洩が発生した場合の被害が大きくなるおそれが高い。以上から、電磁的記録媒体へのデータの書き出しを的確に制限することが求められる。ログの保存については、情報漏洩のリスクを完全にゼロにすることが不可能であり、特に情報を管理する立場の者による故意の漏洩に対してはログの検証による事後的追及以外に対策がないため、必須である。また、ログが残ること自体が不正行為に対する抑止力となることも期待される。

機密性３情報

＜必要と考えられる措置及び対策ポイント＞（下線は喫緊の課題）

必要と考えられる措置		漏洩防止のための対策ポイント	事後調査のための対策ポイント
1	端末のデータの書き出し対策	電磁的記録媒体への書き出し制限（Ⅰ）	電磁的記録媒体への書き出しログ（ⅰ）
2	印刷・コピー対策	印刷・コピーの制限（Ⅱ）	印刷ログ（ⅱ）
3	電子機器及び紙の持ち出し及び持ち込み対策	電子機器及び紙の持ち出し及び持ち込みの制限（Ⅲ）	入退館等のログ（ⅲ）
4	外部への通信制御	外部への通信制限（Ⅳ）	外部との通信ログ（ⅳ）
5	アクセス制御	アクセス制限（Ⅴ）	個人認証ログ（ⅴ） 端末・サーバ内のアクセスログ（ⅵ） 端末・サーバ間の通信ログ（ⅶ）
6	出張時の通信対策	出張時に使用する端末及び通信回線の制限（Ⅵ）	－

Ⅱ　各論

第１　必要と考えられる措置

個別の措置については別添３参照。

なお、必要と考えられる措置には、システム上の措置だけではなくシステム上の対策が困難なためシステム以外の対策となっているものも含まれている。

１　端末のデータの書き出し対策

総論でも触れたとおり、クローズ系のシステムで管理している機密性の高い情報がその外部に出る契機となるのは、クローズ系の端末から電磁的記録媒体へのデータの書き出しであるから、これについて適切に管理することが極めて重要である。

一方、クローズ系において機密性の高い情報が電磁的記録媒体へ不正に書き出されないよう対策を実施していても、職員の故意又は検知されない不正プログラムにより、本来機密性の高い情報を取り扱わないこととしているオープン系のシステムへ電磁的記録媒体を介して機密性の高い情報が移される可能性がないとは言えない。そうした場合には、オープン系がインターネットを通じた外部への情報流出の経路となる可能性のみならず、オープン系端末から当該情報が更に別の電磁的記録媒体に書き出されてしまう可能性も否定できない。このため、端末から電磁的記録媒体へのデータの書き出しについては、オープン系においてもクローズ系に準じた措置が必要であると考えられる。

端末からのデータの書き出しについては、単に規則で制限し、職員にその遵守を求めるに留まらず、システム上強制力のある制限を行うことが必要である。

具体的には、端末から電磁的記録媒体へ書き出す際に自動的に暗号化を行い、当該媒体のデータは組織外の端末では復号できないようにするなどの措置が想定される。組織外の端末で利用できる形で書き出すことが必要な場合には、管理者の許可を得てこれを行うこととする。

次に、私用の電磁的記録媒体を持ち込み、これにデータを書き出すことも大きなリスクであることから、これについても規則で禁止するだけではなく、システム上であらかじめ登録されていない電磁的記録媒体を検知して使用不可とする措置や、仮に私用の電磁的記録媒体にデータを書き込んだとしても、組織外の端末では利用できないことにする措置などが必要である。

また、日常的に発生する電磁的記録媒体への書き出しが適切に行われていることを事後的に確認可能とするため、電磁的記録媒体へのデータの書き出しに関するログや許可の記録を必要十分な期間保存し、定期的に監査を行うことが求められる。公用の電磁的記録媒体の持ち出しを防止するため、原則として集中保管し、定期的に所在確認を行うことなども必要である。

さらに、書き出したデータのトレーサビリティを確保するため、必要に応じ電子データに電子透かしや電子署名を施すこと等について検討することが望ましい。

2　印刷・コピー対策

守るべき情報がクローズ系のシステムの外へ出ていく経路としては、プリンタにより印刷した文書や、それをさらにコピー機により複製した文書が物理的に持ち出されることも挙げられる。印刷物等は、電磁的記録媒体と比較すれば

その情報量に限りがあるが、プリンタやコピー機は一般に複数の職員が共用しているため、印刷した者が不明確となったり、印刷物の取り忘れが起こるおそれがあり、ひいては情報の不要な拡散へとつながる可能性がある。

これらを踏まえ、印刷やコピーについても組織的な管理により、必要な者が必要なだけ行うことを担保することが必要である。システム上は、コピー機やプリンタ等に備えられた認証機能等のセキュリティ機能を活用するほか、印刷に関するログや許可の記録を必要十分な期間保存し、定期的に監査を行うことが求められる。

また、必要に応じ監視カメラの設置や複製防止用紙の利用、持ち出し防止タグの取付け等についても検討することが望ましい。

３　電子機器（ＰＣ、携帯電話、カメラ、電磁的記録媒体等）及び紙の持ち出し及び持ち込み対策

守るべき情報が外部に流出する場合の経路として、外部との通信のほか、当該情報が記録された電子機器や紙が物理的に管理区域外に持ち出されることが考えられる。これを防止するためには、電子機器及び紙の持ち出し及び持ち込みを制限する必要がある。

職員については、あらかじめ許可された電子機器以外は持ち込み禁止とし、抜き打ち検査等によって抑止力を持たせるほか、ＩＤカード等による入退館、入退室の管理を適切に行う必要がある。また、電子機器及び紙の持ち出しについては、必要に応じ特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に持ち出し防止タグを貼付し、庁舎の出入り口等において検知する機能を備

えることについて検討することが望ましい。

一方、保守業者等がサーバ室等に立ち入り、保守等の作業を行うことが避けられないところ、保守業者等のサーバ室等への出入りや電子機器の持ち込みについても管理する必要がある。

さらに、電子機器の持ち込み、入退館及び入退室の記録やログを必要十分な期間保存し、定期的に監査を行うことが求められる。

４　外部への通信制御

総論でも触れたとおり、インターネットと接続されているオープン系システムについては、外部との通信によって職員の意図と関係なくデータが不正に送出されるおそれがある。このため、業務に必要な通信のみを許可し、不必要な通信を制限することとともに、通信のログを必要十分な期間保存し、定期的に監査を行うことにより情報漏洩を防止する必要がある。

また、ウイルス対策ソフトで検知されない不正プログラムを用いた標的型攻撃が散見されていることを踏まえ、必要に応じ標的型攻撃を検知する機能を備えることについて検討することが望ましい。

５　アクセス制御

情報保全においては、「Need to Know」の原則の徹底が不可欠であるところ、システム上はアクセス制御がその基盤となるものである。

個人認証については、データに対する操作を行った本人を事後的に特定できることを担保する必要があり、あらかじめ登録された本人のみがログイン

できる生体認証方式の採用等が求められる。また、ユーザーがファイルを作成する際にアクセス制限を自動的にかける仕組みを導入するなど、アクセス制限を確実に実施する必要がある。

また、個人認証ログ、端末・サーバ内のアクセスログ、端末とサーバ間の通信ログ等を必要十分な期間保存し、定期的に監査を行うことが求められる。

６　出張時の通信対策

出張者と本府省庁間で特に機密性の高い情報の送受信を業務上やむを得ず行う場合には、出張者が使用する端末においては常時暗号化を講じた通信回線を使用すること及び当該端末については紛失等に備え、ハードディスクの暗号化等を行っておくことが必要である。

７　その他

上記１から６の中には整理していないが、定期的な監査等を行うための基準及び体制の整備や訓練の実施、委託先における情報の取扱いの管理や、印刷物の廃棄方法、ログの改ざんへの対策など、これまでに述べた諸対策の実効性を高めるための対策は多岐にわたっている。これらについても必要に応じて実施すべきことは言うまでもない。

また、無線ＬＡＮについては、暗号を破る技術が年々進化しているため、専門家の意見を聞きながらセキュリティ対策の更新を随時行わなければ、安全性を確保することは難しい。

第２　今後顕在化が想定される脅威

情報保全に関わる電子機器や技術は多岐にわたり、これらに関連する将来の脅威として多様なものが想定されうるところ、最近社会的に利用が拡大し、今後関連する脅威の顕在化が想定されるため、特に機密性の高い情報の漏洩防止等の観点から対応を検討する必要性が高いものとして、以下のものが挙げられる。さらに、技術的進歩の速度を踏まえると、今後新たな技術を悪用した脅威に晒されるおそれは十分にあることから、特に機密性の高い情報を取り扱う政府機関においては、常に関連する情報の収集及び分析を行い、途切れることなく適時適切に対策をとっていく必要がある。

○　スマートフォン

現在普及が進んでいるスマートフォンについては、ユーザーによるソフトウェアのインストールを制限することが困難であるなどの問題がある。機密性の高い情報を取り扱う場合は、こうしたスマートフォンの機能や脆弱性などを踏まえ、使用を制限する又はその安全性を十分に確保するための特段の措置をとるなどの対応を検討する必要がある。

○　クラウドコンピューティング

クラウドコンピューティングには、海外サーバを利用する場合の情報保全上のリスク、特定の業者を使い続けないと業務が継続できなくなるリスクなども指摘されており、その安全性が十分に確保されるまでは、機密性の高い情報の取り扱いに関し、使用を制限するなどの対応を検討する必要がある。

おわりに

特に機密性の高い情報を取り扱う政府機関の情報保全システムの確立は、我が国を取り巻く現下の厳しい情勢にかんがみれば、まさに喫緊の課題である。

当会議としては、政府において、本報告書の内容を十分踏まえつつ、①守るべき情報が確実に運用・保護されるシステムとすること、②運用面に過度の負担を与えることのないシステムとすること、③万一情報漏洩等の事案が発生した際は、迅速かつ適切な事後対応が可能なシステムとすることの３点を基本とし、国家と国民の発展に資する情報保全システムに必要と考えられる対策が速やかに進められること、及びその進捗状況が適切にフォローアップされることを強く期待するものである。

なお、当会議の検討期間中の平成２３年３月１１日、東日本大震災が発生した。これを契機として、当会議において大規模災害への対応についても議論を行ったところ、重要な情報については、記録の断絶が生じないようバックアップデータの保管場所、方法等について、各府省庁において今一度チェックする必要があるといった指摘や、非常時のデータの保護や復旧を迅速に行うことができるよう、緊急時の手続きをあらかじめ定めておく必要があるといった指摘がなされた。これらの指摘が、今後政府が大規模災害の発生に備えた対応について検討を進める上での一助になれば幸いである。

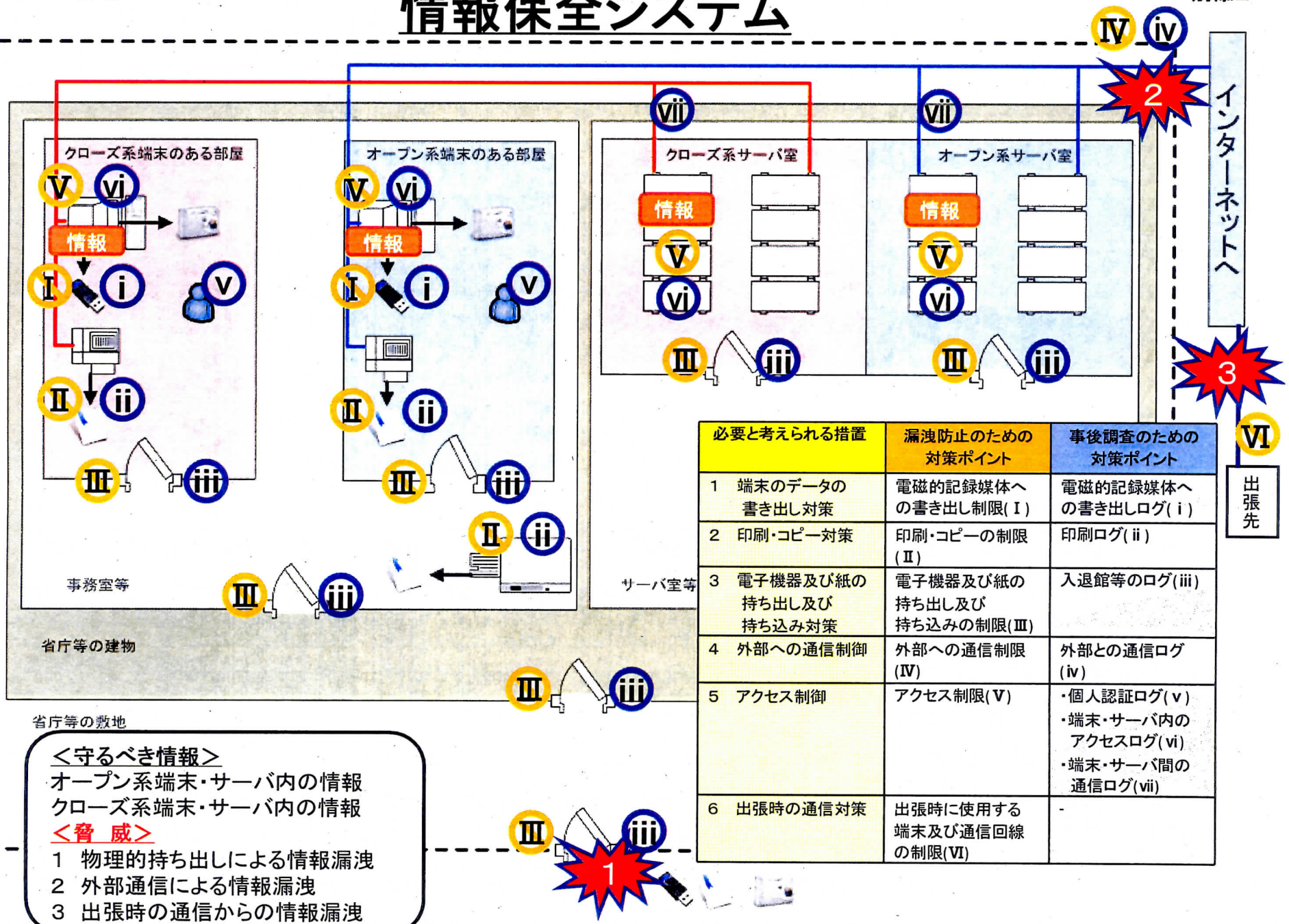
別添1

想定される脅威及び対策ポイント

脅威の概要	対象となるシステム	具体的な脅威	対策ポイント	
			漏洩防止	事後調査
物理的持ち出しによる情報漏洩	オープン系 クローズ系	サーバ内データを電磁的記録媒体に書き出し、持ち出し	Ⅰ、Ⅲ、Ⅴ	i 、iii 、v vi 、vii
	オープン系 クローズ系	端末内データを電磁的記録媒体に書き出し、持ち出し	Ⅰ、Ⅲ、Ⅴ	i 、iii 、v vi
	オープン系 クローズ系	サーバ内データを印刷し、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii 、iii 、v vi 、vii
	オープン系 クローズ系	端末内データを印刷し、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii 、iii 、v vi
	オープン系 クローズ系	印刷したデータをコピーし、持ち出し	Ⅱ、Ⅲ、Ⅴ	ii 、iii 、v vi 、vii
	オープン系 クローズ系	ディスプレイに表示されている情報を撮影し、持ち出し	Ⅲ	iii
外部通信による情報漏洩	オープン系	サーバ内データを外部との通信により漏洩	Ⅳ、Ⅴ	iv 、v 、vi 、 vii
	オープン系	端末内データを外部との通信により漏洩	Ⅳ、Ⅴ	iv 、v 、vi
	クローズ系	サーバ内データを電磁的記録媒体に書き出し、オープン系にデータを移し、外部との通信により漏洩	Ⅰ、Ⅲ、Ⅳ Ⅴ	i 、iii 、iv 、 v 、vi 、vii
	クローズ系	端末内データを電磁的記録媒体に書き出し、オープン系にデータを移し、外部との通信により漏洩	Ⅰ、Ⅲ、Ⅳ Ⅴ	i 、iii 、iv 、 v 、vi
出張時の通信からの情報漏洩	出張時の端末及び通信回線	出張時の通信について通信経路上で情報を窃取される	Ⅵ	-

別添2

情報保全システム



必要と考えられる措置	漏洩防止のための対策ポイント	事後調査のための対策ポイント
1 端末のデータの書き出し対策	電磁的記録媒体への書き出し制限(Ⅰ)	電磁的記録媒体への書き出しログ(ⅰ)
2 印刷・コピー対策	印刷・コピーの制限(Ⅱ)	印刷ログ(ⅱ)
3 電子機器及び紙の持ち出し及び持ち込み対策	電子機器及び紙の持ち出し及び持ち込みの制限(Ⅲ)	入退館等のログ(ⅲ)
4 外部への通信制御	外部への通信制限(Ⅳ)	外部との通信ログ(ⅳ)
5 アクセス制御	アクセス制限(Ⅴ)	・個人認証ログ(ⅴ) ・端末・サーバ内のアクセスログ(ⅵ) ・端末・サーバ間の通信ログ(ⅶ)
6 出張時の通信対策	出張時に使用する端末及び通信回線の制限(Ⅵ)	-

＜守るべき情報＞
オープン系端末・サーバ内の情報
クローズ系端末・サーバ内の情報

＜脅　威＞
1　物理的持ち出しによる情報漏洩
2　外部通信による情報漏洩
3　出張時の通信からの情報漏洩

必要と考えられる措置

1　端末のデータの書き出し対策

－　漏洩防止のための対策　（Ⅰ）

a　システム上で強制力のある制限（次のa-1又はa-2のいずれかの対策をとる）

a-1　許可がなければ書き出しを禁止、例外措置を講ずる場合の許可手順

a-2　特別な手段がないと復号できない方法により強制的に暗号化、例外措置を講ずる場合の許可手順

b　私用電磁的記録媒体の使用制限（次のb-1又はb-2のいずれかの対策をとる）

b-1　個体識別が可能な電磁的記録媒体について、登録済のもの（公用電磁的記録媒体等）以外の電磁的記録媒体を接続した場合に使用不可能とする

b-2　私用・公用にかかわらず書き出しても自動暗号化され特別な手段がない限り復号不可能とする

公用電磁的記録媒体のインターフェースの形状の特殊化

c　暗号化による書き出しデータの保護

電磁的記録媒体への書き出し時に自動暗号化され特別な手段がない限り復号不可能とする

－　事後調査のための対策　（ｉ）

a　システム上で強制力のある制限の例外措置を講ずる場合の記録及びその定期的な監査

b　電磁的記録媒体への書き出し時のログの保存及び定期的な監査

c　公用電磁的記録媒体の適切な保管（原則として集中保管）　※

d　公用電磁的記録媒体の定期的な所在確認　※

e　電磁的記録媒体への書き出し時に電子透かしや電子署名を施す

[redacted]

凡例
赤字：オープン系・クローズ系ともにとるべき対策
緑字：必要に応じてとるべき対策
※　：システム上の対策が困難なため、システム以外の対策となっているもの

必要と考えられる措置

凡例
赤字：オープン系・クローズ系ともにとるべき対策
橙字：クローズ系においてとるべき対策
緑字：必要に応じてとるべき対策
※　：システム上の対策が困難なため、システム以外の対策となっているもの

2 印 刷・コピー対策

– 漏洩防止のための対策 （Ⅱ）

a 印刷時のプリンタ認証
b 決められたプリンタでのみの印刷を許可
c 特に機密性の高い情報の印刷時の管理者の許可（必要に応じ保全担当者の立会い） ※
d 課・室外への印刷出力の禁止
e 印刷物への取扱い区分の明示 ※
f 特に機密性の高い情報の印刷時の複製防止用紙の使用 ※
g 特に機密性の高い情報の印刷物への持ち出し防止タグの取付け
h 印刷物への日付、印刷者名（アカウント情報）等の刷り込み
i 指定された出力元以外からの印刷防止（プリンタのパラレル、USB各ポート及びSDカードスロット、無線LANポート等の物理的（論理的）閉鎖）
j コピー機のメモリ情報の管理
k コピー機（特に複合機）のセキュリティ機能の活用（認証機能とアクセス制限機能、情報漏洩防止機能及びネットワークセキュリティ機能等）
l コピー保守業者のコピー機設定情報の確認と設定の認証 ※
m 複合機のプリンター機能、FAX機能、スキャナー機能の使用許可（制限）と機能設定

– 事後調査のための対策 （ⅱ）

a プリンタの印刷ログの保存及び定期的な監査
b 印刷者名（アカウント情報）の確実な管理
c プリンタ・コピー機周辺に取り忘れ、紛失防止のための監視カメラの設置
d 特に機密性の高い情報の印刷時の管理者の許可の履歴の定期的な監査（保全担当者の立会いの履歴の定期的な監査） ※

[redacted]

必要と考えられる措置

3　電子機器(PC、携帯電話、カメラ、電磁的記録媒体等)及び紙の持ち出し及び持ち込み対策

－　漏洩防止のための対策　（Ⅲ）

a　執務室（サーバ室含む。）への許可された電子機器以外の持ち込み禁止・制限　※
b　執務室（サーバ室含む。）への出入りに際し、電子機器の持ち込み状況の確認のため、抜き打ち検査の実施　※
c　執務室（サーバ室含む。）における執務中の電子機器の持ち込み状況の確認のため、抜き打ち検査の実施　※
d　保守業者に対するクリアランスの確認　※
e　保守業者のサーバ室出入りの確認、作業の立会い及び監督　※
f　保守用電子機器持ち込み時の確認と申請等手続きの確立。履歴の記録と持ち出し時の確認　※
g　電磁的記録媒体の修理・交換時の確実な消去の確認　※
h　特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に関する持ち出し防止タグを用いた検知機能
i　職員のIDカード等による入退館管理（特に機密性の高い情報を扱う執務室（サーバ室含む。）では生体認証も併用）

－　事後調査のための対策　（iii）

a　保守業者に対するクリアランスの確認資料の保存及び定期的な監査　※
b　保守業者のサーバ室出入りの記録の保存及び定期的な監査　※
c　保守用電子機器持ち込み時の記録の保存及び定期的な監査　※
d　特に機密性の高い情報を記録した電磁的記録媒体及び印刷物に関する持ち出し防止タグ検知機能のログの保存
e　IDカード等による入退館のログ及び特に機密性の高い情報を扱う執務室（サーバ室含む。）に係る生体認証のログの保存及び定期的な監査
f　特に機密性の高い情報を扱う執務室（サーバ室含む。）の入退室映像の保存

[redacted]

凡例
赤字：オープン系・クローズ系ともにとるべき対策
橙字：クローズ系においてとるべき対策
緑字：必要に応じてとるべき対策
※　：システム上の対策が困難なため、システム以外の対策となっているもの

必要と考えられる措置

4 外部への通信制御

– 漏洩防止のための対策 （Ⅳ）

a ホワイトリストによる通信の制限

業務に必要な通信のみを許可

b ブラックリストによる通信の制限

業務に不必要な通信を制限

- 民間が運営しているフリーのWebメールの使用禁止
- 掲示板サイトへの通信制限（アクセスを禁止、書き込みを禁止）
- 市販のWebフィルタリングソフトウエアを導入し、カテゴリ別で通信を制限

c 標的型攻撃の検知機能

– 事後調査のための対策 （ⅳ）

a 許可している通信を考慮に入れたログの保存及び定期的な監査

[redacted]

凡例
青字：オープン系においてとるべき対策
緑字：必要に応じてとるべき対策

必要と考えられる措置

5　アクセス制御

– 漏洩防止のための対策 （Ⅴ）

a 個人認証
登録された本人のみがログインできる仕組み（生体認証方式の採用等）

b 確実なアクセス制御の実施
ファイル・フォルダごとのアクセス制限の実施
ファイルを作成する際にアクセス制限を強制的にかけるような仕組みの導入

– 事後調査のための対策 （ⅴ、ⅵ、ⅶ）

a 個人認証ログの保存及び定期的な監査

b 端末ーサーバ間の通信ログの保存及び定期的な監査

c 端末・サーバ内それぞれのファイルアクセスログの保存及び定期的な監査

[redacted]

凡例
赤字：オープン系・クローズ系ともにとるべき対策

6　出張時の通信対策

– 漏洩防止のための対策 （Ⅵ）

a 出張先において電子機器により特に機密性の高い情報に関し通信をやむを得ず行う場合には、クローズ系専用回線と同等の暗号化を講じた回線（衛星回線、VPN）を用いる

b 上記回線に接続する出張用端末については、紛失時に備えて、ハードディスク上における必要な暗号化措置等を講ずる

別添４

本有識者会議の開催経緯・開催経過等

○ 情報保全システムに関する有識者会議委員名簿

○ 情報保全システムに関する有識者会議開催状況

○ 政府における情報保全に関する検討委員会の開催について

○ 情報保全システムに関する有識者会議の開催について

機密性３情報

情報保全システムに関する有識者会議
委員名簿

（五十音順　／　○：座長）

○	小池　英樹（こいけ　ひでき）	電気通信大学大学院情報システム学研究科　教授
	小屋　晋吾（こや　しんご）	トレンドマイクロ㈱　戦略企画室統合政策担当部長
	神成　淳司（しんじょう　あつし）	慶應義塾大学環境情報学部　准教授
	杉浦　隆幸（すぎうら　たかゆき）	ネットエージェント㈱　代表取締役社長
	中村　康弘（なかむら　やすひろ）	防衛大学校電気情報学群情報工学科　教授
	羽室　英太郎（はむろ　えいたろう）	警察大学校附属警察情報通信学校　情報管理教養部長

機密性３情報

情報保全システムに関する有識者会議
開催状況

第１回　平成２２年１２月１７日
（１）有識者会議の設置の経緯と位置付けについて
（２）情報保全システムに関する有識者会議の運営について
（３）情報保全システムの検討スケジュールについて
（４）脅威に関する現状認識について

第２回　平成２３年２月４日
（１）近年の情報流出事案について
（２）特に機密性の高い情報を取り扱う政府機関の情報保全システムの現状について
（３）民間の情報保全システムの現状について

第３回　平成２３年３月９日
（１）考えられる対応策（案）について
（２）将来想定される脅威について

第４回　平成２３年５月２０日
報告書（案）について

機密性３情報

政府における情報保全に関する検討委員会の開催について

［平成22年12月7日
内閣総理大臣決裁］

1　政府における情報保全に関し、秘密保全に関する法制の在り方及び特に機密性の高い情報を取り扱う政府機関の情報保全システムにおいて必要と考えられる措置について検討するため、政府における情報保全に関する検討委員会（以下「委員会」という。）を開催する。

2　委員会の構成は、次のとおりとする。ただし、委員長は、必要があると認めるときは、委員を追加し、又は関係者に出席を求めることができる。

委員長　内閣官房長官
副委員長　内閣官房副長官
委員　内閣危機管理監
内閣官房副長官補（内政担当）
内閣官房副長官補（外政担当）
内閣官房副長官補（安全保障・危機管理担当）
内閣情報官
警察庁警備局長
公安調査庁次長
外務省国際情報統括官
海上保安庁警備救難監
防衛省防衛政策局長

3　委員会は、必要に応じ、関係行政機関の職員による検討部会を開催することができる。検討部会の構成員は、委員長が指名する。

4　委員会は、必要に応じ、有識者会議を開催することができる。有識者会議の出席者は、委員長が参集を求める。

5　委員会の庶務は、関係行政機関の協力を得て、内閣官房において処理する。

6　前各項に定めるもののほか、委員会の運営に関する事項その他必要な事項は、委員長が定める。

機密性３情報

情報保全システムに関する有識者会議の開催について

［平成２２年１２月１６日
政府における情報保全に
関する検討委員会委員長決定］

１　開催の趣旨

政府における情報保全に関する検討委員会（平成２２年１２月７日内閣総理大臣決裁。以下「委員会」という。）における検討に資するため、各界の有識者から御意見をいただくことを目的として、情報保全システムに関する有識者会議（以下「会議」という。）を開催する。

２　構成

（１）会議は、別紙に掲げる者により構成し、委員会の委員長が開催する。
（２）委員長は、別紙に掲げる委員の中から、会議の座長を依頼する。
（３）座長は、必要に応じ、関係者の出席を求めることができる。

３　その他

会議の庶務は、関係行政機関の協力を得て、内閣官房において処理する。

別紙

情報保全システムに関する有識者会議の構成員

小池　英樹	電気通信大学大学院情報システム学研究科　教授
小屋　晋吾	トレンドマイクロ㈱　戦略企画室統合政策担当部長
神成　淳司	慶應義塾大学環境情報学部　准教授
杉浦　隆幸	ネットエージェント㈱　代表取締役社長
中村　康弘	防衛大学校電気情報学群情報工学科　准教授
羽室　英太郎	警察大学校附属警察情報通信学校　情報管理教養部長

五十音順

（注）役職は決定当時のもの

平成23年 8 月 29 日

行政文書の開示の実施方法等申出書

内閣情報官　植松 信一 殿

氏名又は名称

住所又は居所

連絡先電話番号

[redacted]

行政機関の保有する情報の公開に関する法律第14条第２項の規定に基づき、下記のとおり申出をします。

記

1　行政文書開示決定通知書の番号等

＊ 日　　付　平成２３年８月１８日
　 文書番号　閣　情　　第３１７号

2　求める開示の実施の方法

下表から実施の方法を選択し、該当するものに○印を付してください。

＊ 行政文書の名称	種類・量	実施の方法	
（1）第１回秘密保全のための法制の在り方に関する有識者会議（平成２３年１月１５日）配付資料	A４判文書 ２４枚 （内訳） 白黒 １８枚 カラー ６枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（2）第２回秘密保全のための法制の在り方に関する有識者会議（平成２３年２月１８日）配付資料	A４判文書 ９枚 （内訳） 白黒 ２枚 カラー ７枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（3）第３回秘密保全のための法制の在り方に関する有識者会議（平成２３年４月８日）配付資料	A４判文書 １６枚 （内訳） 白黒 ２枚 カラー １４枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）

すべてスキャナにより電子化された
ものの写しを希望

（４）第４回秘密保全のための法制の在り方に関する有識者会議（平成２３年４月２２日）配付資料	A４判文書 ４７枚 （内訳） 白黒 １５枚 カラー ３２枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（５）第５回秘密保全のための法制の在り方に関する有識者会議（平成２３年５月１３日）配付資料	A４判文書 １７枚 （内訳） 白黒 １３枚 カラー ４枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（６）第６回秘密保全のための法制の在り方に関する有識者会議（平成２３年６月１０日）秘密保全のための法制の在り方について（報告書案）	A４判文書 ８４枚 （内訳） 白黒 ６３枚 カラー ２１枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（７）第１回情報保全システムに関する有識者会議（平成２２年１２月１７日）配付資料	A４判文書 ７枚 （内訳） 白黒 ７枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（８）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料	A４判文書 ６枚 （内訳） 白黒 ６枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（９）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料「中国漁船衝突事件映像情報流出事案の概要について」	A４判文書 ２枚 （内訳） 白黒 １枚 カラー １枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（１０）第２回情報保全システムに関する有識者会議（平成２３年２月４日）配付資料「警察における情報保全に関する取組みについて」	A４判文書 ３枚 （内訳） 白黒 １枚 カラー ２枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）

（１１）第３回情報保全システムに関する有識者会議（平成２３年３月９日）配付資料	Ａ４判文書 １１枚 （内訳） 白黒 ４枚 カラー ７枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（１２）第３回情報保全システムに関する有識者会議（平成２３年３月９日）配付資料５「将来予想される脅威等に関する各委員の御説明資料」	Ａ４判文書 １７枚 （内訳） 白黒 １７枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（１３）第４回情報保全システムに関する有識者会議（平成２３年５月２０日）配付資料「報告書（案）」	Ａ４判文書 ２３枚 （内訳） 白黒 １６枚 カラー ７枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（１４）第４回情報保全システムに関する有識者会議（平成２３年５月２０日）配付資料「情報流出再発防止対策検討委員会中間報告書（概要）」	Ａ４判文書 ２枚 （内訳） 白黒 ２枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）
（１５）第２回情報保全に関する検討委員会（平成２３年５月２０日）　配付資料　「情報保全システムに関する有識者会議報告書(案)」	Ａ４判文書 ３０枚 （内訳） 白黒 ２３枚 カラー ７枚	1　閲覧	①全部 ②一部（　　）
		2　写しの交付	①全部 ②一部（　　）
		3　写しの送付	①全部 ②一部（　　）

4　「写しの送付」の希望の有無　［有／無　：同封する郵便切手の額 200 円］

開示実施手数料 2,780 円