ネット監視・先制サイバー攻撃法案と警察

関東学院大学名誉教授　足立　昌勝

１　能動的サイバー防御法案審議の現状

四月八日、警察の権限を拡大し、自衛隊による先制サイバー攻撃を容認する能動的サイバー防御法案は、衆議院本会議で圧倒的多数で可決され、参議院に送付された。反対したのは、共産党とれいわ新選組のみであった。四月十八日、参議院本会議で審議が始められ、では、に送付した。この法案は、重要電子計算機に対する不正な行為による被害の防止に関する法律案」（以下、「新法」）及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律案」（以下、「整備法」）の二本からなっている。

これらの法案のもととなったのは、二十二年十二月十六日に閣議決定された国家安全保障戦略である。そこでは、今後の検討課題として、①官民連携の強化、②通信情報の利用、③攻撃者のサーバ等への侵入・無害化、④内閣サイバーセキュリティセンター（ＮＩＳＣ）の発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置等が挙げられていた。

２　法案の概要

サイバー対処能力強化法案及び整備法案の全体像

サイバー対処能力強化法案	Ⅰ官民連携の強化 ・基幹インフラ事業者（注）に対する一定の電子計算機の届出義務、インシデント報告義務（第２章） ・情報共有・対策のための協議会の設置（第９章：第 45 条） ・脆弱性対応の強化（第 42 条） Ⅱ通信情報の利用 ・基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章） ・（同意によらない）通信情報の取得（第４章、第６章） ・自動的な方法による機械的情報の選別の実施（第５章、第７章） ・関係行政機関の分析への協力（第 27 条） ・取得した通信情報の厳格な取扱い（第 23 条） ・サイバー通信情報監理委員会による事前審査・継続的検査等（第 10 章） （ⅠとⅡによる） ・分析情報・脆弱性情報の提供等（第８章）
整備法案	Ⅲアクセス・無害化措置 ・重大な危害を防止するための警察による措置 ・サイバー通信情報監理委員会の事前承認、警察庁長官の指揮 等 （以上、警職法改正） ・内閣総理大臣の命令による自衛隊の通信防護措置 ・自衛隊、日本に所在する米軍が使用するコンピュータ等の警護 等 （以上、自衛隊法改正）

	Ⅳ組織・体制整備等 ・サイバーセキュリティ戦略本部の改組、機能強化 等 （以上、サイバーセキュリティ基本法改正） ・内閣サイバー官（内閣法改正）

「能動的サイバー防御の導入 ― サイバー対処能力強化法案及び整備法案の概要と主な論点―」柿沼重志（内閣委員会調査室）・立法と調査４７４号より

まず新法では、①基幹インフラ事業者による導入された一定の電子計算機の届出やインシデントの報告を求め、情報共有・対策のための協議会を設置し、脆弱性対応を強化することについての官民連携を図り、②基幹インフラ事業者等と協定（同意）に基づく通信情報の取得、同意なき通信情報の取得、自動的な方法による機械による情報の選別の実施、関係行政機関の分析への協力、取得した通信情報の厳格な取扱い、独立機関による事前審査・継続的検査の実施等という通信情報の利用が定められた。これにより、分析情報・脆弱性情報の提供等が可能となるという。

これらのうち、特に「同意なき通信情報の取得」には注意する必要がある。政府が作成した説明文書（十頁、新法②［通信情報の利用］）によれば、それには、外外通信の分析と外内通信または内外通信の分析があり、前者は「国外の攻撃インフラ等の実態把握のため必要があると認める」時に行なわれ、後者は、「国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要がある」時に行なわれるという。これらは、憲法が保障する通信の秘密を侵害することは明白であり、「制度設計にあたっては、『通信の秘密』に十分に配慮」するとしているが、無同意での通信情報の取得は、通信の秘密を侵害していることに間違いはない。どのような制度設計をしようが、憲法違反であることは明白である。

整備法では、警察官職務執行法の改正により、重大な危害を防止するための警察による無害化措置の実施を認め、そのためには、独立機関の事前承認を求め、警察庁長官等による指揮に基づくこととされ、自衛隊法改正により、内閣総理大臣の命令による自衛隊の通信防護措置、自衛隊・在日米軍が使用するコンピュータ等の警護がその内容となり、サーバへのアクセス・無害化措置を認めている。

さらに、整備法では、サイバーセキュリティ戦略本部の改組・機能強化、内閣サイバー官の新設が盛られている。

３　警察による能動的サイバー防御の実施

能動的サイバー防御を実施するために、整備法は警察官職務執行法を改正し、新たに六条の二「サイバー危害防止措置執行官による措置」を設け、また、自衛隊法を改正し、八十一条の三「重要電子計算機に対する通信防護措置」を設けている。

サイバー攻撃は、攻撃サーバが電子計算器内にある情報を窃取したり、そこにあるソフト等の機能を停止させることによって成り立っている。その攻撃対象は、政府自治体等、基幹インフラ、経済情報保有事業者等に及んでおり、その機能が停止してしまえば、その影響は甚大であることを理由に、能動的サイバー防御を実施する根拠があるという。

能動的サイバー防衛は、警察庁長官により指名されたサイバー危害防止措置執行官により実施される。

実施するための要件は、①サイバーセキュリティを害する等の情報技術を用いた不正な行為に用いられまたはその疑いのある電気通信の認知、②そのまま放置すれば、人の生命、身体または財産に重大な危害が発生するおそれがあるため緊急の必要があるときであり、その実施の内容は、①通信の送信元であるサーバ等の管理者等に対する「危害防止のために通常必要と認められる措置であって電気通信回線を介して行う加害関係電子計算機の動作に係るものをとること」を命令し、②攻撃関係サーバ等への措置（インストールされている攻撃のためのプログラムの停止・削除など）を自ら実施することである（サイバー危害防止措置)。

その電子計算機が、「国内に設置されていると認める相当な理由がない場合」には、事前に外務大臣と協議しなければならず、その実施については、独立機関であるサイバー通信情報管理委員会の承認を得なければならず、加害の通信がすでに送信されている場合など、承認を得るいとまがないと認める特段の事由がある場合には、速やかな事後通知で足りるとしている。

サイバー危害防止措置執行官による措置の実施については、警察庁長官等の指揮を受けなければならない。

法案に規定されている警察による能動的サイバー防御措置の概要は、以上のとおりであるが、ここには、非常に大きな問題が含まれている。

攻撃の通信をしてきたサーバの管理者に対しする措置命令を認めているが、その法的根拠については何も明らかにされていない。法的根拠を有しない命令は無効であることは明白である。送信元が従わないことを前提とし、自らが行なうことを自明のこととしているので、その法的根拠を無視しているのであろうか。それは。非常に荒っぽい議論である。人々が警察の命令に従わざるを得ないのは、その命令が法的根拠を以て発信されているからである。こんな法的根拠を持たない命令には、従う義務は存在しない。

さらに、送信元が命令に従わなかった場合、警察自らがその措置をとるという。それは、相手方電子計算機に侵入し、プログラム等を破壊し、無害化することを示している。このような措置をとることに、令状主義は必要ないのであろうか。警察が強制処分を行う場合には、令状が必要なことは憲法三十五条が認めていることだ。それを無視することができる根拠はどこにあるのか。そんな根拠はどこにもない。

また、整備法では、国内に設置されていない電子計算機についても、同様な措置をとることが認められている。これは、警察権限の発動は国内に限定されなければならないという大原則を完全に無視している。

外国にあるサーバに侵入し、そこにあるソフト等を破壊する行為を警察が行なうことを許容する根拠はどこにあるのか。サイバー社会には国境がないことを良しとし、外に出ていこうというのか。本来は、現実の社会と同様に、自らの財産は自らの力で守るべきであり、放置されていてはならない。現実の社会には国境があり、国を守るために、防空措置を講じている。サイバー社会でも、その論理は変わるところがない。攻撃対象となる電子計算機が外国に存在している事実については、警察は把握しているのだ。その外国に存在する電子計算機への攻撃は、その正当化根拠を明示し、法的根拠を明らかにすべきである。

４　自衛隊による能動的サイバー防御の実施

整備法は、自衛隊にもサイバー防御を実施する権限を与えている。

内閣総理大臣が次の場合に通信防護措置を命じた上で、自衛隊の部隊等が措置を実施することとなる。①重要電子計算機に対する特定不正行為があり、②本邦外にある者による特に高度に組織的かつ計画的な行為と認められるものが行なわれ、③次の各号のいずれにも該当することにより、自衛隊が対処を行なう特別な理由があると認めるときである。

一　当該不正行為により重要電子計算機に特定重大支障（重要電子計算機の機能の停止または低下であって、当該機能の停止または低下が生じた場合に、当該電子計算機に係る事務または事業の安定的な遂行に容易に回復することができない支障が生じ、これによって国家及び国民の安全を著しく損なう事態が生ずるものをいう。）が生ずる恐れが大きいと認めること。

二　特定重大支障の発生を防止するために自衛隊が有する特別な技術または情報が必要不可欠であること。

三　国家公安委員会からの要請またはその同意があること。

それに対する措置は、「部隊等に当該特定不正行為による当該電子計算機への被害を防止するための必要な電子計算機の動作に係る措置であって電気通信回線を介して行うものをとる」ことであり、この措置をとるときは、「警察庁又は都道府県警察と共同して」実施するとされている。

警察が行なう能動的サイバー防御は「サイバー危害防止措置」であり、自衛隊が行なうものは、「通信防護措置」である。これらの措置は全く異なっている。にもかかわらず、自衛隊が行う通信防護措置については、警察が共同して行なうという。警察は、国内に設置されていることについての相当な理由がない場合のみ、例外的にサイバー危害防止措置を実施することが許されているにすぎない。通信防護措置の実施についての権限を持たない警察が、自衛隊が行なう通信防護措置の実施に参加できるのかについての合理的根拠は示されていない。これでは、国外での警察権力の実施が、当然のように許されることになってしまうだろう。この通信防護措置がサイバー戦争行為の一環であると捉えた場合には、その戦争行為に警察が参加することを意味し、整備法に規定されているような形での自衛隊と警察の共同作業を簡単に認めるわけにはいかない。

ここでも、憲法九条を忘れてはならない。能動的サイバー防御関連法案について、マスコミは様々な視点から報道しているが、一番欠落しているのが、憲法九条の視点が欠け、この法案が戦争推進法であることである。マスコミは、冷静な視点を持ち、的確な批判を行なう責務があると思うが、いかがかな。

さらに、自衛隊及び日本に所在する米軍が使用する電子計算機をサイバー攻撃から職務上警護する自衛官が、緊急の必要があるときに無害化措置を実施するとし、措置を実施する場面・措置の内容は、警察と同様である。また、国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議が必要であり、措置に際しての手続は、独立機関の承認（承認を得るいとまがないと認める特段の事由がある場合：事後通知）がなければならず、防衛大臣の指揮も必要である。

この要件の一つである「本邦外にある者による特に高度に組織的かつ計画的な行為と認められるものが行なわれ」ということについては、政府が作成した説明文書では、「外国政府を背景とする主体による高度な攻撃と認められるもの」とされている（一六頁「整備法①［アクセス・無害化］」。どのように理解すれば、政府の説明になるのかは全く理解できない。「本邦外にある者」を「外国政府を背景とする主体」と理解しようとしたいのは、政府が自らの中で仮想敵国を設け、それによるサイバー攻撃が行われることを想定しているのではないだろうか。それはもう戦争行為そのものである。

外国からのサイバー攻撃を受け、それに対処するために行われる防御であっても、それは反撃であり、

それを戦争とみるかどうかは別として、もう戦争行為の一環でなされている。

本来、サイバー社会は無防備なものであり、セキュリティの確立は、その程度を問わず、それぞれの所有者の判断に任されている。技術は毎日のように進歩するのだから、それに対応した形で、セキュリティも進歩しなければならない。その際に絶対に行ってはいけないことは、セキュリティが破られたからということを理由とした相手方電気計算機への反撃である。もしこれを許してしまえば、復讐の連鎖であり、留まるところを知らなくなってしまう。

サイバー攻撃は、対象となる電子計算機が保有する秘密情報を窃取し、機能停止させることを目的として行なわれると思われる。

自衛隊による通信防護措置が行われる要件の一つに、「重要電子計算機に対する特定不正行為」の存在が挙げられている。「重要電子計算機」とは、新法二条二項に規定されており、内閣に置かれる機関、内閣の所管の下に置かれる機関等、地方公共団体、独立行政法人等が使用する電子計算機のうち、そのサイバーセキュリティが害された場合において、当該者における重要情報の管理または重要な情報システムの運用に関する事務の実施に重大な支障が生ずる恐れがあるものとされている。

さらに、三号で、重要情報を保有する事業者が使用する電子計算機のうち、そのサイバーセキュリティが害された場合において、当該事業者における重要情報の管理に関する業務の実施に重大な支障が生ずる恐れがあるものについては、次のものに限定されている。

①ＭＳＡ秘密保護法の特別防衛秘密である情報

②特定秘密保護法 3 条 1 項に規定する特定秘密（防衛大臣が保有させ、又は八条一項の規定により防衛大臣が提供したものに限る。）である情報

③防衛省調達装備品基盤強化法に規定される装備品等秘密である情報

④重要経済安保法三条一項に規定する重要経済安保情報である情報

これらから判断できることは、通信防護措置は、広義での秘密保護法の秘密性を強化するものであり、国民から遠ざけるものでしかないということである。

柿沼は、次のように、説明している。

警察によるサイバー事案への対処に関しては、従来は、各都道府県警察が捜査権限を執行し、警察庁は必要な指示や調整等を実施していた。しかし、サイバー空間には国境がないことから、外国捜査機関等との連携が不可欠であり、都道府県警察の捜査のみを前提とする仕組みでは、その対処に支障が生じていた。こうした事態を受け、令和４年４月に警察法が改正され、警察庁にサイバー警察局が設置されるとともに、重大サイバー事案における捜査権限の執行を行うサイバー特別捜査隊が設置された。その後、令和６年４月に、同特別捜査隊は、サイバー特別捜査部に昇格している。

また、防衛省・自衛隊による対処としては、令和４年３月、陸海空自衛隊の共同の部隊として、自衛隊サイバー防衛隊（防衛大臣の直轄部隊）が新編され、サイバー攻撃などへの対処等を実施している。また、同年 12 月 16 日に国家安全保障会議が決定し、閣議決定もされた「防衛力整備計画（令和９年度までの計画）」においては、令和６年度末現在で 2,410 人のサイバー専門部隊を約 4,000 人に拡充すること等が盛り込まれた。

参考

（サイバー危害防止措置執行官による措置）

第六条の二 警察庁長官は、警察庁又は都道府県警察の警察官のうちから、次項の規定による処置を適正にとるために必要な知識及び能力を有すると認められる警察官をサイバー危害防止措置執行官として指名するものとする。

２ サイバー危害防止措置執行官は、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を害することその他情報技術を用いた不正な行為（以下この項において「情報 技術利用不正行為」という。）に用いられる電気通信若しくはその疑いがある電気通信（以下この項及び第四項ただし書において「加害関係電気通信」という。）又は情報技術利用不正行為に用いられる電磁的記録（電子的方式、磁気的方式その他人の知覚によつては認識することができない方式で作られる記録であつて、電子計算機による情報処理の用に供されるものをいう。以下この項において同じ。）若しくはその疑いがある電磁的記録（以下この項において「加害関係電磁的記録」という。）を認めた場合であつて、そのまま放置すれば人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、加害関係電気通信の送信元若しくは送信先である電子計算機又は加害関係電磁的記録が記録された電子計算機（以下この条において「加害関係電子計算機」と総称する。）の管理者その他関係者に対し、加害関係電子計算機に記録されている加害関係電磁的記録の消去その他の危害防止のため通常必要と認められる措置であつて電気通信回線を介して行う加害関係電子計算機の動作に係るもの（適切に危害防止を図るために通常必要と認められる限度において、電気通信回線を介して当該加害関係電子計算機に接続して当該加害関係電子計算機に記録されたその動作に係る電磁的記録を確認することを含む。）をとることを命じ、又は自らその措置をとることができる。

３ 加害関係電子計算機が国内に設置されていると認める相当な理由がない場合における当該加害関係電子計算機の動作に係る前項の規定による処置は、警察庁の警察官であるサイバー危害防止措置執行官に限り、とることができるものとする。この場合において、当該サイバー危害防止措置執行官は、あらかじめ、警察庁長官を通じて、外務大臣に協議しなければならない。

４ サイバー危害防止措置執行官は、第二項の規定による処置をとる場合には、あらかじめ、サイバー通信情報監理委員会の承認を得なければならない。ただし、当該加害 関係電子計算機から重要電子計算機（重要電子計算機に対する不正な行為による被害の防止に関する法律（令和七年法律第▼▼▼号）第二条第二項に規定する重要電子計算機をいう。）に対してその機能に重大な障害を生じさせ、又は生じさせるおそれのある加害関係電気通信が現に送信されている場合その他の当該危害防止のためにはサイバー通信情報監理委員会の承認を得るいとまがないと認める特段の事由がある場合は、この限りでない。

５ 第三項に規定する場合における前項の承認の求めは、第三項の規定による協議の結果を添えて行わなければならない。

６ サイバー通信情報監理委員会は、第四項の承認の求めがあつた場合において、当該求めが第二項及び第三項の規定に照らして適切であると認めるときは、当該承認をするものとする。

７ サイバー危害防止措置執行官は、第二項の規定による処置をとるに際しては、みだりに関係者の正当な業務を妨害してはならない。

８ サイバー危害防止措置執行官は、第二項の規定による処置をとつたときは、当該加害関係電子計算機の管理者に同項に規定する措置をとることを命じた場合を除き、国家公安委員会規則で定めるところにより、遅滞なく、その旨を当該管理者に通知するものとする。ただし、当該加害関係電子計算機に関係する危害の防止に支障がある場合及び当該管理者の所在が不明である場合は、この限りでない。
９ サイバー危害防止措置執行官は、第四項ただし書の規定によりサイバー通信情報監理委員会の承認を得ないで第二項の規定による処置をとつたときは、速やかに、当該処置についてサイバー通信情報監理委員会に通知しなければならない。
10 前項の規定による通知を受けたサイバー通信情報監理委員会は、当該通知に係る処置が第二項、第三項及び第四項ただし書の規定に照らして適切に行われたかどうかを確認し、第二項の規定による処置に係る事務の適正な実施を確保するため必要があると認めるときは、当該確認の結果に基づき、当該通知を行つたサイバー危害防止措置 執行官が所属する警察庁又は都道府県警察の警察庁長官又は警視総監若しくは道府県警察本部長（次項において「警察庁長官等」という。）に対し、必要な措置をとるべきことを勧告するものとする。
11 サイバー危害防止措置執行官は、この条の規定による措置の実施について、警察庁長官等（第三項に規定する場合にあつては、警察庁長官）の指揮を受けなければならない。

（重要電子計算機に対する通信防護措置）
第八十一条の三 内閣総理大臣は、重要電子計算機に対する特定不正行為（重要電子計算機に対する不正な行為による被害の防止に関する法律（令和七年法律第▼▼▼号）第二条第四項に規定する特定不正行為をいい、電気通信回線を介して行われるものに限る。以下この項及び第四項第一号において同じ。）であつて、本邦外にある者による特に高度に組織的かつ計画的な行為と認められるものが行われた場合において、次の各号のいずれにも該当することにより自衛隊が対処を行う特別の必要があると認めるときは、部隊等に当該特定不正行為（当該特定不正行為を行つた者による同種の特定不正行為を含む。第一号において同じ。）による当該重要電子計算機への被害を防止するために必要な電子計算機の動作に係る措置であつて電気通信回線を介して行うもの（以下この条及び第九十一条の三において「通信防護措置」という。）をとるべき旨を命ずることができる。
一 当該特定不正行為により重要電子計算機に特定重大支障（重要電子計算機の機能の停止又は低下であつて、当該機能の停止又は低下が生じた場合に、当該重要電子計算機に係る事務又は事業の安定的な遂行に容易に回復することができない支障が生じ、これによつて国家及び国民の安全を著しく損なう事態が生ずるものをいう。次号において同じ。）が生ずるおそれが大きいと認めること。
二 特定重大支障の発生を防止するために自衛隊が有する特別の技術又は情報が必要不可欠であること。
三 国家公安委員会からの要請又はその同意があること。
２ 前項の「重要電子計算機」とは、重要電子計算機に対する不正な行為による被害の防止に関する法律第二条第二項に規定する重要電子計算機（同項第三号に該当するものにあつては、防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律（令和五年法律第五十四号）第二十七条第一項に規定する契約事業者である者が次に掲げる情報を取り扱うために使用するものに限る。）をいう。
一 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である情報

二 特定秘密の保護に関する法律（平成二十五年法律第百八号）第三条第一項に規定する特定秘密（同法第五条第四項の規定により防衛大臣が保有させ、又は同法第八条第一項の規定により防衛大臣が提供したものに限る。）である情報
三 防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律第二十七条第一項に規定する装備品等秘密である情報
四 重要経済安保情報の保護及び活用に関する法律（令和六年法律第二十七号）第三条第一項に規定する重要経済安保情報（同法第十条第一項の規定により防衛大臣が提供し、又は同条第二項の規定により防衛大臣が保有させたものに限る。）である情報
３ 第一項の規定により通信防護措置をとるべき旨を命ぜられた部隊等は、警察庁又は都道府県警察（次項第四号において「警察庁等」という。）と共同して当該通信防護措置を実施するものとする。
４ 内閣総理大臣は、第一項の規定により部隊等に通信防護措置をとるべき旨を命ずる場合には、あらかじめ、防衛大臣と国家公安委員会との間で協議をさせた上で、次に 掲げる事項を指定しなければならない。
一 通信防護措置により対処を行う特定不正行為及び防護の対象となる第二項に規定する重要電子計算機
二 通信防護措置として実施すべき措置に関する事項
三 通信防護措置の期間
四 警察庁等と共同して通信防護措置を実施する要領その他の警察庁等との連携に関する事項
五 その他必要な事項
５ 内閣総理大臣は、前項第三号の期間内であつても、通信防護措置の必要がなくなつたと認める場合には、速やかに、部隊等に通信防護措置の終了を命じなければならない。

（重要電子計算機に対する通信防護措置の際の権限）
第九十一条の三 警察官職務執行法第六条の二第二項から第十一項までの規定は、第八十一条の三第一項の規定により通信防護措置をとるべき旨を命ぜられた部隊等の自衛官の職務の執行について準用する。この場合において、同法第六条の二第二項中「サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を害することその他情報技術を用いた不正な行為（以下この項において「情報技術利用不正行為」という。）」とあるのは「重要電子計算機（自衛隊法（昭和二十九年法律第百六十五号）第八十一条の三第二項に規定する重要電子計算機をいう。第四項において同じ。）に対する特定不正行為（同条第一項に規定する特定不正行為をいう。以下この項において同じ。）」と、 「情報技術利用不正行為に」とあるのは「当該特定不正行為に」と、同条第三項中 「処置は、警察庁の警察官であるサイバー危害防止措置執行官に限り、とることができるものとする。この場合において、当該」とあるのは「処置をとる」と、「警察 長官」とあるのは「防衛大臣」と、同条第四項中「あらかじめ」とあるのは「あら じめ、防衛大臣を通じて」と、同項ただし書中「重要電子計算機（重要電子計算機 対する不正な行為による被害の防止に関する法律（令和七年法律第▼▼▼号）第二条第二項に規定する重要電子計算機をいう。）」とあるのは「重要電子計算機」と、同条第八項中「国家公安委員会規則」とあるのは「防衛省令」と、「その旨を」とあるのは「その旨を部隊等の長を通じて」と、同条第九項中「サイバー通信情報監理委員会に」とあるのは「防衛大臣を通じて

サイバー通信情報監理委員会に」と、同条第十項中「当該通知を行つたサイバー危害防止措置執行官が所属する警察庁又は都道府県警察の警察庁長官又は警視総監若しくは道府県警察本部長（次項において「警察庁長官等」という。）」とあり、及び同条第十一項中「警察庁長官等（第三項に規定する場合にあつては、警察庁長官）」とあるのは「防衛大臣」と読み替えるものとする。 第九十二条第二項中「及び第九十条第一項」を「（第六条の二を除く。）及び第九十条第一項」に、「規定は、」を「規定は」に、「海上保安庁法第十六条」を「同法第六条の二第二項から第十一項までの規定は当該自衛官のうちこの項において準用する同条第二項の規定による処置を適正にとるために必要な能力を有する部隊等として防衛大臣が指定する部隊等に属するものが前項の規定により公共の秩序の維持のため行う職務の執行について、海上保安庁法第十六条」に、「準用する。」を「、それぞれ準用する。」に改め、「者」と」の下に「、同法第六条の二第三項中「処置は、警察庁の警察官であるサイバー危害防止措置執行官に限り、とることができるものとする。この場合において、当該」とあるのは「処置をとる」と、「警察庁長官」とあるのは「防衛大臣」と、同条第四項中「あらかじめ」とあるのは「あらかじめ、防衛大臣を通じて」と同条第八項中「国家公安委員会規則」とあるのは「防衛省令」と、「その旨を」とあるのは「その旨を部隊等の長を通じて」と、同条第九項中「サイバー通信情報監理委員会に」とあるのは「防衛大臣を通じてサイバー通信情報監理委員会に」と、同条第十項中「当該通知を行つたサイバー危害防止措置執行官が所属する警察庁又は都道府県警察の警察庁長官又は警視総監若しくは道府県警察本部長（次項において「警察庁長官等」という。）」とあり、及び同条第十一項中「警察庁長官等（第三項に規定する場合にあつては、警察庁長官）」とあるのは「防衛大臣」と」を加え、「この項において準用する 警察官職務執行法第七条及びこの法律」を「自衛隊法（昭和二十九年法律第百六十五号）第九十二条第二項において準用する警察官職務執行法第七条及び自衛隊法」に、「この項において準用する海上保安庁法」を「同法第九十二条第二項において準用す る」に改め、「、「海上保安官又は海上保安官補の職務」とあるのは「第七十六条第一項（第一号に係る部分に限る。）の規定により出動を命ぜられた自衛隊の自衛官が公共の秩序の維持のため行う職務」と」を削る。

（自衛隊等が使用する特定電子計算機の警護のための権限）

第九十五条の四 警察官職務執行法第六条の二第二項から第十一項までの規定は、次に掲げる特定電子計算機（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）第二条第一項に規定する特定電子計算機をいう。）をサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を害することその他情報技術を用いた不正な行為から職務上警護する自衛官の職務の執行について準用する。この場合において、警察官職務執行法第六条の二第二項中「、サイバーセキュリティ」とあるのは「、自衛隊法（昭和二十九年法律第百六十五号）第九十五条の四第一項各号に掲げる特定電子計算機（第四項ただし書において「特定電子計算機」という。）に対するサイバーセキュリティ」と、「情報技術利用不正行為に」とあるのは「当該情報技術利用不正行為に」と、同条第三項中「処置は、警察庁の警察官であるサイバー危害防止措置執行官に限り、とることができるものとする。この場合において、当該」とあるのは「処置をとる」と、「警察庁長官」とあるのは「防衛大臣」と、同条第四項中「あらかじめ」とあるのは「あらかじめ、防衛大臣を通じて」と、同項ただし書中「に対し」とあるのは「である特定電子計算機に対し」と、同条第八項中「国家公安委員会規則」とあるのは「防衛省令」と、「その旨を」とあるのは「その旨を部隊等の長を通じて」と、同条第九項中「サイバー通信情報監理委員会に」とあるのは「防衛大臣を通じてサイバー

通信情報監理委員会に」と、同条第十項中「当該通知を行つたサイバー危害防止措置執行官が所属する警察庁又は都道府県警察の警察庁長官又は警視総監若しくは道府県警察本部長（次項において「警察庁長官等」という。）」とあり、及び同条第十一項中「警察庁長官等（第三項に規定する場合にあつては、警察庁長官）」とあるのは「防衛大臣」と読み替えるものとする。

一　自衛隊が使用する特定電子計算機

二　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軍隊が使用する特定電子計算機

２　前項第二号に掲げる特定電子計算機に対する同項の警護は、アメリカ合衆国の軍隊から要請があつた場合であつて、防衛大臣が必要と認めるときに限り、自衛官が行うものとする。