

法案の問題点 質問のポイント

論点	質問	質問の意図
現行警察法について	1) 警察法第19条で警察庁に警備局、生活安全局、刑事局などの内部部局をおくとしているが、その法的根拠は何か。条文では警察法のどこにあたるか。 2) 警察法第36条で都道府県警察は第二条（犯罪の予防、鎮圧及び捜査、被疑者の逮捕など）の責務に任ずるとされている。犯罪捜査などは都道府県警察だけができることとされ、警察庁には捜査権限はない。この理由を説明してほしい。 3) 警察庁の所掌事務は第十七条で、第五条第4項各号（26号ある）に掲げる事務をつかさどるとされているが、これ以外に所掌事務はあるか。	
下位の法令との関係	下記はどのように変更されるのか。 1) 警察庁組織令 2) 警察法施行令	
サイバー警察局の位置づけ	サイバー警察局がサイバー事案について都道府県警察に対して指揮監督権限をもてるということか。	改正案では、サイバー警察局を設置し、所掌事務として「サイバー事案に関する警察に関すること」をつかさどるとされている。
警察庁内・都道府県警察のリソースの一元化 他部局との連携はどうやるのか	他部局との連携はどうやるのか	警察庁のサイバーセキュリティ政策会議の令和3年度報告書では、サイバー警察局とサイバー特別捜査隊を設置し、サイバー犯罪対策のために警察庁内のリソースを一元化して効果的な対処体制を構築する必要性を述べている。 「刑事部門、生活安全部門、交通部門、警備部門など既存の警察部門と連携し、警察組織全体でサイバー空間・実空間の両者にわたり隙間なく脅威に対処」（報告書21頁）とは、具体的にどのように行うのか。

	サイバー警察局が一元化するシステムは、市民生活のすべてを監視する大量監視システムにならないか。	「警察庁デジタル・ガバメント中長期計画」では、警察庁が共通基盤を整備し、他のシステムとの連携も含めた警察情報管理システム全体の合理化・高度化に取り組むとしていた。 共通基盤システム上では警察庁及び各都道府県警察のデータは区別して管理するが、「全国共有が可能なデータや警察庁への送受信が必要なデータについては、警察庁が管理するデータとして一元的に集約を行う」と予定とされている。 この共通基盤システムは、サイバー対策のために一元化されるリソースの中に含まれるか。含まれるとすると、サイバー警察局が一元化するシステムは、市民生活のすべてを監視すべき公共空間とする大量監視システムにならないか。
	国家機関である警察庁のサイバー局に捜査権限を付与しようとしているが、他の生活安全局などの機関に拡大されていく危険性はないのか。	
警察庁の情報通信組織	警察庁の情報通信組織はどのように改訂されるのか	下記での説明と組織図はどのように変更されるのか https://www.npa.go.jp/joutuu/001.htm
警察の組織全体との関係	組織の概要について 下記のウェブに掲載されている「警察のしくみ国と都道府県の警察組織のあらまし」のなかの組織図はどのようになるのか	https://www.npa.go.jp/about/overview/sikumi.html
	国の機構図はどのように変更されるのか	https://www.npa.go.jp/about/overview/img/R3_kuni_kikouzu.pdf
	地方の機構図はどのように変更されるのか 刑事局とサイバー警察局との関係を説明せよ。例：通信傍受捜査の実施体制 はどのように変更されるのか。	https://www.npa.go.jp/about/overview/img/R3_ken_kikouzu.pdf
	刑事局とサイバー警察局との関係を説明せよ。例：通信傍受捜査の実施体制はどのように変更されるのか。	
	警備局とサイバー警察局との関係を説明せよ。例：法	

	改正後では、東京オリンピックのようなメガイベントの場合、どのような組織の連携をとるのか。	
	生活安全局とサイバー警察局との関係を説明せよ。 例：薬物の取り締まりのような事案の場合、生活安全局とどのような連携をとるのか。	
あいまいな用語の事例	以下の用語の定義を示せ。 1) 重要な情報 2) 重要な情報システム 3) 国民生活、経済活動の基盤 4) 国民生活、経済活動の基盤に影響を及ぼす「おそれ」とは、どのような場合か 5) 十六の「重大サイバー事案に係る犯罪の捜査その他」の「その他」とは何を想定しているのか。「その他」は不要ではないか。 6) 第二十一条二十六「情報の管理に関する企画」とはどのような「企画」か。「技術的研究」とはどのような研究か。 7) 二十七「情報システムの整備」「管理」とは何か	
関東管区警察局について	なぜ関東管区警察局を「全国を管轄区域」としたのか。こうした改正がなぜ必要なのか。この条文のよって都道府県警察および関東以外の管区警察局の機能はどのように変更されるのか。変更案を示せ。	
六十一条の三の3以降の新設条項	なぜ「警察庁又は関係都道府県警察」「警察庁及び関係都道府県警察」のようにあえて「警察庁」を加える必要があるのか。	
(重大)サイバー事案の概念	サイバー事案、重大サイバー事案という規定が設けられるが、サイバー犯罪とかサイバー攻撃という言葉はよく聞くが、そうではなく、なぜ、サイバー事案としたのか。 1) サイバーセキュリティとは何か、それが害されることとは具体敵な事例をいくつかあげてほしい。	改正案では、新設される第4条6項ハで、サイバー事案はサイバーセキュリティ(サイバーセキュリ

	<p>2) 情報技術を用いた不正な行為により、個人の生命、身体、財産並びに公共安全と秩序を害するという具体的事例をいくつかあげてほしい。</p> <p>3) 「害される恐れのある事案とは」の意味と、具体的事例をあげてほしい。</p>	<p>ティ基本法第二条に規定) が害されること、そのほか 情報技術を用いた不正な行為により、個人の生命、身体、財産並びに公共安全と秩序を害し、または害される恐れのある事案とされているが、この規定はあまりにも無限定的で拡大解釈され、乱用されかねない危険をはらんでいる。それぞれについて説明してほしい。</p>
	<p>(重大)サイバー事案に関連する用語があまりにもあいまいである。以下について説明してほしい。</p> <p>1) 重大サイバー事案、サイバー事案のそれぞれの定義を具体的にしてほしい。それぞれ具体的にどのような行為を想定しているのか。</p> <p>2) サイバー事案かどうかの決定手続。誰に決定権があるのか。決定に至る意思決定の仕組みはどのようなものか。</p> <p>3) サイバー警察局ではサイバー事案に関する情報収集、分析、対策等を一元的により効果的に進めるとあるが、</p> <p>4) 情報収集とはなにか。</p> <p>5) 情報収集の対象にメールや SNS など含まれるのか。</p> <p>6) 常時監視にならないか。</p> <p>7) 「重大な支障」とあるが重大のレベルをどのように規定しているのか。規定しているならレベルを段階的に示してほしい。</p> <p>8) 「サイバー事案」「重大サイバー事案」が発生したときに、サイバー空間の何(SNS等?)をどのように捜査対象にするのか。具体的に例示してほしい。</p>	
	<p>対処に高度な技術を要する事案とは何を指すのか</p>	<p>サイバー警察局の設置等により今後行おうとしている「高度な技術を要する事案」とはどういうものか。 他国で行っているようなパソコンやスマートフォンに監視ソフトをインストールしたり、諸外国が連携して Emotet で行ったような犯罪者のインフラ</p>

		を破壊する攻撃的なサイバー対策も含まれるか。
サイバー攻撃との関係	1) サイバー攻撃を受けた時、攻撃元を突き止めるために、中継サーバーの通信記録（ログ）を解析する必要があるが、憲法 21 条（通信の秘密）を侵害することにならないか。 2) サイバー攻撃とサイバー事案はどのように違うのか 3) 自衛隊の活動との関係はどうなるのか。現状はどうなっているのか。法改正後はどうなるのか	
国家安全保障と人権、 プライバシー	警察庁のサイバーセキュリティの観点は「サイバーセキュリティ戦略 2021」の観点を共有しているのか。	警察庁のサイバーセキュリティ政策会議の令和 3 年度報告書では、「国際共同オペレーションを、法の支配、自由、民主主義といった価値観を共有する国家や国際機関と連携して幅広く進めていくことが重要」(23 頁)とし、「令和 4 年度以降、サイバー隊が、国の捜査機関として前面に立ち、戦略的に国際捜査を推進する」(30 頁)としているが、これはサイバーセキュリティ戦略 2021 が中国・ロシア・北朝鮮を脅威と名指しし同盟国・同志国と連携して対応するとしているのと同じ考えか。
	NSA など他国諜報機関との連携は、現状がどうなっており、今後はどのようになるのか。	NSA（アメリカ国家安全保障局）のスノーデン元職員が暴露したアメリカ政府機関による同盟国も含む世界的な通信傍受のような事案も、重大サイバー事案に該当するか。該当する場合、「法の支配、自由、民主主義といった価値観を共有する国家や国際機関と連携」とは、どこでの連携を指すのか。
	諜報活動（インテリジェンス）と犯罪捜査との関係はどのようなものか。	警察庁サイバーセキュリティ政策会議では委員から、インテリジェンスの部分が法執行の部分にどう重なってくるのか、あるいは重なってこないのか、その区分けをどう説明していくかが課題と指摘されていた（第 1 回 8-9 頁）。 警察庁は、指摘のような懸念が存在することは認め丁寧な説明が必要と応じているが、その区分けを説明せよ。

	セキュリティ対策の取り組みとはなにか、具体的な技術の仕組みを示してほしい。	セキュリティ対策の取り組みとはなにか、具体的な技術の仕組みを示してほしい。サイバー警察局とサイバー特別捜査の新設はデジタル社会におけるサイバー空間と実空間の安心・安全の確保を目的にサイバーセキュリティ対策の取り組みを抜本的に強化するためと説明しているが、セキュリティ対策の取り組みとはなにか、具体的な技術の仕組みを示してほしい。 安心・安全の確保は技術的なセキュリティ対策を構築することで、警察が行なうことではないと考えるが、警察が行なわなければならない理由を明確にしてほしい。
個人情報の保護	警察庁内部の個人情報の扱いがどのようになるのか。	共通基盤システムにより一元的に個人情報が利用されると、本来それぞれの目的の範囲内で利用されるべき刑事部門の捜査情報、生活安全部門の相談情報、交通部門の運転免許等の情報、警備部門の治安情報などが目的外利用・提供されることになるが、その個人情報保護のための措置を明らかにされたい。
	個人情報保護委員会はチェック機能を果せるのか。	2021年5月の個人情報保護法改正により、捜査機関が保有する捜査情報に含まれる個人情報の取扱いも個人情報保護委員会の監視対象になっている。警察の個人情報の扱いについてはこれまでブラックボックス化されてきた。サイバー警察局の新設や警視庁の共通基盤システム構築を踏まえ、委員会として今後どのような監視を行っていくのか。個人情報保護委員会がチェック機能を果たすことができるのか。
	マイナンバー制度の利用拡大があるのか。	マイナンバーカードを運転免許証として利用しようとしているなかで、サイバー事案についてマイナンバー制度の利用拡大があるのか。
生体認証やAIなどの技術利用	生体認証やAIなどの技術利用への歯止めがないのか。 1) 警察による生体認証やAIなどの技術利用の歯止めを	

	<p>どのように考えているのか</p> <p>2) 生体認証や AI 技術の開発、利用を管轄するのはサイバー警察局か</p>	
憲法と人権	<p>憲法および電気通信事業法の通信の秘密を遵守する制度的、技術的な歯止めがどこにあるのか。</p>	
	<p>サイバー空間は公共空間であり、さいばー警察局は個人の思想信条の自由の侵害をまねくのではないか。憲法で保障されている言論・表現の自由や思想信条の自由を侵害する危険性への歯止めがどこにあるのか。</p>	
網羅的監視の危険性	<p>捜査の歯止めは担保されるのか(網羅的監視の危険性)</p> <p>1) 現状ではサイバー空間での捜査には歯止めがないのではないのか。</p> <p>2) サイバー空間の捜査は、裁判所の令状に基づくものなのか。</p> <p>3) 警察はサイバー攻撃を防ぐとして、狙いを付けた個人・団体に対してサイバー空間で常時監視を行うのではないのか。</p> <p>4) サイバー事案・重大サイバー事案の発生および、その捜査については国会に報告はするのか。</p>	
「苦情申立て」	<p>1) 苦情対象が警察庁の警察官なのか都道府県の警察官なのかを見分ける方法は、どのように制度化されるのか。文書による苦情申立て後の苦情処理の手続が定められていないので、この苦情申立ては事実上意味をなさないのではないのか。</p> <p>2) 苦情があれば国家公安委員会に苦情を申し出ることができるとしているが、警察と一体となっている公安委員会への「苦情申出制度」は形骸化しており、苦情の解決機関としては不適切であり、別の機関をつくるべきではないのか。</p> <p>3) また、繰り返されている警察による冤罪などがおきないように、第三者機関を設置することが必要ではないか。</p>	

2022/2/22 作成

2.6 実行委 <https://www.jca.apc.org/no-cyberpolice/>

問い合わせ先

メール no-cyberpolice.techcenter@aleeas.com

電話 070-5553-5495 (小倉利丸)