「治安基盤」の抜本的強化に関する提言
～日本が誇る安全・安心を未来世代に引き継ぐために～
【治安・テロ・サイバー犯罪対策調査会　提言】

令和８年５月２１日
自由民主党政務調査会

昨今、「世界一安全」と言われてきた日本の治安が、量・質共に揺らいでおり、懸念される状況である。例えば、刑法犯認知件数の総数は、令和３年から４年連続で前年を上回った。さらに、匿名・流動型犯罪グループによる犯罪やサイバー事案のように、治安事象そのものが複雑化・広域化している。

こうした情勢の中では、治安を支える基盤を維持・強化することが急務であるが、隘路が存在している。具体的には、警察官の採用情勢は、採用試験の受験者数及び競争倍率が15年間で約３分の１にまで落ち込んでいるなど厳しさが増しており、治安を守るという警察官としての「誇りと使命感」を強く打ち出しても、「警察官のなり手」が増えていないのが現状である。また、複雑化・広域化する治安事象に現在の体制では必ずしも対処し切れていない。さらに、警備業界をはじめとする警察の治安基盤を補完する民間セクターの育成も必要不可欠である。

本調査会では、治安を支える現場に精通した有識者からのヒアリングや、治安基盤を強化するための取組についての議論を踏まえ、正に今直面している治安課題と今後十数年先の社会構造の双方を見据えて、着実に進めるべき取組について、この度、総括的な提言を取りまとめた。政府においては、本提言を踏まえ、日本社会を支える重要インフラである「治安」を未来世代に引き継ぐために、取組の抜本的強化を図っていただきたい。

１　警察力の充実・強化
（１）優秀な警察官の確保に向けた取組の推進
ア　将来を見据えた優秀な警察官の確保

「誇りと使命感」だけで受験者が確保できる時代では最早ない。このため、警察庁が本年４月に策定した「将来を見据えた優秀な警察官の確保に向けた緊急対策プラン」も踏まえつつ、以下の取組を強力に推進すべきである。

(ｱ)　「過剰に厳しい」という警察学校のイメージの払拭～警察学校の運営の改善～

新人警察官の教育訓練や生活の場となる警察学校については、生活上のルール等が「過剰に厳しい」と認識されていることや、施設が老

朽化していることなどが警察官志望者に不安を与えていると考えられる。

こうした警察学校のネガティブイメージを払拭するため、時代に即した学校運営の見直しを推進するとともに、広域連携を要する分野における合同授業・訓練の導入による教育訓練の高度化や、適正規模を考慮した施設の集約等を通じて、老朽化した学校施設の建替えや既存の良好な施設の活用を進め、生活環境の改善を早急に進めるべきである。

(イ) 処遇と職場環境の改善

警察官の職務の特殊性を踏まえ、手当の整備・拡充を含めた処遇面の更なる改善を進めるとともに、有事即応体制の確保のための待機宿舎の整備、職員の健康や安全を確保するための被服や装備品の充実を含めた、警察官の職務を取り巻く環境の更なる改善に向けた取組も推進すべきである。

そのほか、若い世代に対する訴求力の高い媒体等による発信力強化や、試験制度の不断の見直しによる採用の間口拡大についてもあわせて推進するべきである。

イ サイバー人材の確保・育成

(ア) 高度人材の育成と捜査員全体のサイバー対処能力の底上げ

我が国の安全保障にとって重大な脅威となる懸念国からのサイバー攻撃への対処に関しては、アクセス・無害化措置に関する規定が本年秋から施行されることも踏まえ、高度な人材の確保・育成が急務である。また、サイバー空間の匿名性を悪用した犯罪に対処するため、捜査員のサイバー技能の底上げも喫緊の課題である。

(イ) 最新の機器を導入した演習環境の整備

サイバー分野において職員の対処能力を強化するためには、座学による研修のみならず、安全な仮想空間の下、最新の手口や技術を踏まえた実践的な訓練を継続的に行う必要があることは自明である。こうした観点から、警察のサイバー人材育成のために必要不可欠なインフラとして、サイバーレンジ[1]や教材等の演習環境の整備を確実に推進する必要がある。また、サイバー分野においては、技術や手口が急速に変化・高度化し続けていることから、対処能力を陳腐化させないためには、演習環境も最新のものを導入し、これを高度化し続ける必要がある。

[1] サイバー事案に対する実践的な訓練を行うためのサイバー演習環境

これらの取組に加えて、高度なサイバー人材の確保のため、サイバー部門独自の採用も含め、既存の枠組みにとらわれない採用を推進すべきである。

（２）警察庁の調整機能の強化による広域・国際犯罪対処の効率化等

サイバー事案、匿名・流動型犯罪グループやローン・オフェンダー（ＬＯ）による犯罪、対日有害活動等は、手口がより専門化・高度化するとともに、県境や国境を越えて広域化・国際化している。また、例えばサイバー空間では、捜査によって国家の関与の疑いが判明する事案も継続的に発生しており、国家安全保障領域での警察の役割も複雑化・重要化している。

かかる状況の下、警察庁は、全国的・国際的見地から都道府県警察をより強力に調整し、サイバー事案、匿名・流動型犯罪グループ、ＬＯ等に係る情報の集約・融合・分析等に一層積極的に取り組むべきである。また、国際刑事警察機構（ＩＣＰＯ）や国連薬物犯罪事務所（ＵＮＯＤＣ）等の国際機関との連携を一層強化すべきである。

さらに、広域犯罪等への対処の中で重要な役割を果たしている警察用ヘリコプターの安定的な運航を確保するため、複数の府県警察から成るブロック内で複数のヘリコプターを計画的・効率的に運用するなど、都道府県警察の枠を越えた広域的な連携を強化すべきである。

（３）警察の装備資機材の充実等

ＡＩやドローン等の先端技術について、ＳＢＩＲ[2]、ＢＲＩＤＧＥ[3]、経済安全保障重要技術育成プログラムといった省庁横断的な研究開発支援の枠組みも必要に応じて活用し、積極的に警察業務に導入することにより、様々な警察活動を総合的に高度化すべきである。

また、犯罪の検挙に不可欠なスマートフォン等の解析やマネー・ローンダリングに用いられた暗号資産追跡の強化のため、解析資機材等を充実させるほか、情報通信技術を用いて高度な解析を遠隔支援するなど、解析態勢を全国的に強化すべきである。さらに、高度な科学技術を用いた鑑識・鑑定資

---

[2] スタートアップ等による研究開発を促進し、その成果を円滑に社会実装し、それによって我が国のイノベーション創出を促進するための制度。同時に、革新的な技術を社会実装していくことで我が国が直面する様々な社会課題を解決に導くことも目的の１つとする。

[3] 科学技術・イノベーション政策の方針に基づき、総合科学技術・イノベーション会議の司令塔機能を生かし各省庁の研究開発等の施策のイノベーション化を推進するプログラム。「重点課題」（例：事業環境整備、スタートアップ創出、人材育成等）を設定し、研究開発だけでなく社会課題解決等に向けた取組を推進する。

機材、ＣＢＲＮＥテロに対応する部隊等の装備資機材、高性能なドローン対処資機材、証拠保全等に資するウェアラブルカメラ等の警察の装備資機材を充実させるほか、警察活動を支える通信インフラを高度化すべきである。

（４）警察における情報力・カウンターインテリジェンス機能の強化

政府全体でインテリジェンス機能の強化に取り組む中、インテリジェンスコミュニティの一員である警察の情報力の強化も不可欠である。具体的には、ＬＯによる犯罪等への対処のため、現実空間とサイバー空間における情報の収集・分析を一層効率化・高度化するほか、対日有害活動に対する我が国のカウンターインテリジェンス機能強化のため、高い捜査能力と全国的ネットワークを有する警察の機能や態勢を強化すべきである。

２　治安を支える民間力の更なる充実

（１）警備業の育成のための取組の推進

警備業は、治安基盤の強化において重要な役割を担う存在であり、治安を支える民間力として育成していくことが必要である。しかし、警備業界の抱える深刻な「人手不足」の解消が急務であることから、適切な労務単価の設定をはじめとする警備員の処遇改善や業務の生産性の向上等が必要である。

また、特に重要施設や基幹インフラの警備については、従事する警備員に特別な訓練を行うとともに、防犯カメラ等の警備機器の使用に当たってはその安全性に配慮し、そのコストに応じた特別な価格設定をするべきである。また、重要施設や基幹インフラの警備の発注に当たっては、適切な警備業者が受注できるよう当該インフラを所管する省庁が警察と連携して、発注に関するガイドラインを作成し、指導するといった態勢を構築すべきである。

（２）防犯カメラ設置の推進

防犯カメラは、治安基盤の強化と国民の安心感の醸成に不可欠な存在といえるところ、物価高により安全かつ高機能な防犯カメラの導入コストが上昇している状況を踏まえ、引き続き、保存期間の十分な防犯カメラの増設に向けた働き掛けを、強力に推進していくべきである。また、重要施設や基幹インフラに設置する防犯カメラについては、その安全性に十分な配慮をすべきである。

（３）サイバー保険等を活用した民間企業のサイバーセキュリティ対策の推進

ア　サイバー保険の普及に向けた支援

サイバー保険は、企業がランサムウェア攻撃等の被害を受けた際の金銭補償のみならず、ぜい弱性診断、復旧支援等の付帯サービスの面でも重要な役割を果たしていることから、その普及のための取組を推進すべきである。

ランサムウェア攻撃の際の損害額が高額となることやサプライチェーンリスクの観点を踏まえれば、特に中小企業にとってサイバー保険は不可欠なインフラといえ、これら企業に対して更なるサイバー保険の加入を促進する必要がある。中小企業がサイバー保険に加入する場合の金銭的支援や、サイバー保険に加入した企業を評価する枠組み等の新設も含め、対策を検討すべきである。

また、検挙による抑止を一層推進する観点や、保険金の不正取得及び保険加入によるモラルハザードを防止する観点から、事案発生時の警察への通報を保険金支払いの要件とすることなどを検討すべきである。

イ　サイバーセキュリティ向上のための支援策の更なる推進

サイバーセキュリティに関する適切なサービスの提供を受ける中小企業や小規模事業者に対して「デジタル化・ＡＩ導入補助金」を活用した支援を行う「サイバーセキュリティお助け隊サービス」事業等を活用し、平素からのデータのバックアップ等の備えも含め、民間企業のランサムウェア対策に対する支援を推進すべきである。

ウ　サイバーセキュリティ対策に関わる企業の信頼性向上

ランサムウェア攻撃に際してフォレンジックやデータ復旧を行うなどと称する業者等が、実際には犯罪グループに身代金を支払っているとの実態も指摘されている。こうした悪質なサービスが横行しないよう、デジタルフォレンジックサービス等のサイバーセキュリティに携わる企業の信頼性を確認する制度を導入し、民間企業に広く周知すべきである。

エ　官民連携の強化

個々の民間企業では、最新の手口や対策等に関する情報収集に限界があることから、日本サイバー犯罪対策センター（ＪＣ３）における多数の企業が連携した取組やサイバー対処能力強化法に定める協議会における官民連携等を通じて、情報共有を更に進めるとともに、政府としても対策に資する国際連携を一層強化すべきである。

以上