別添

原議保存期間	5年（令和14年3月31日まで）
有効期間	一種（令和14年3月31日まで）

警察庁乙サ発第１号、乙官発第２号
乙生発第１号、乙刑発第１号
乙交発第１号、乙備発第１号
令和８年４月２日
警察庁次長

庁内各局部課長
各附属機関の長
各地方機関の長
各都道府県警察の長　殿

警察におけるサイバー戦略について（依命通達）

サイバー空間が重要な社会経済活動が営まれる公共空間へと変貌を遂げた中、サイバー空間をめぐる脅威は、引き続き極めて深刻な情勢にある。

警察においては、これまで「警察におけるサイバー戦略について（依命通達）」（令和４年４月１日付け警察庁乙サ発第１号ほか）に基づき、サイバー空間の脅威に関する諸対策を推進してきたところであるが、昨年12月に「サイバーセキュリティ戦略」（令和７年12月23日閣議決定）が策定されたこと、本年４月に「将来を見据えた警察組織の構造改革及び優秀な警察官の確保に向けた取組について（依命通達）」（令和８年４月２日付け警察庁乙官発第６号ほか）を発出したこと等を踏まえ、この度、別添のとおり、警察におけるサイバー戦略を改定することとした。

各位にあっては、本戦略に基づき、警察組織の総合力を発揮した効果的な取組を推進されたい。

命により通達する。

別添

警察におけるサイバー戦略

第１　情勢認識

我が国が戦後最も厳しく複雑な安全保障環境に直面する中、地政学的緊張を反映したサイバー空間を取り巻く情勢は一層深刻化しており、重大な事態へと急速に発展していくリスクをはらんでいる。特に、サイバー空間の匿名性を悪用したサイバー攻撃は露見するリスクが低く、攻撃者側が優位にあることから、その脅威が急速に高まっている。具体的には、サイバー攻撃による機微情報の窃取や他国の選挙への干渉等は、国家を背景とした形でも平素から行われているとされている。また、武力攻撃の前から、重要インフラの機能停止・破壊が行われるほか、偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が今後更に洗練された形で実施される可能性が高いとされている。例えば、ロシアは、侵略前にサイバー攻撃を行うなど、軍事的・政治的目的達成のためにサイバー攻撃を行っているとみられている。また、中国は、情報窃取を目的としたサイバー攻撃に加え、有事を見据え、重要インフラ等の機能妨害・機能破壊も視野に入れたサイバー攻撃を行っているとも評価されている。さらに、北朝鮮は、サイバー攻撃により暗号資産の窃取等を行っていることが明らかとなっている。

他方で、社会全体のデジタル化の進展に伴い、サイバー空間が、地域や年齢を問わず、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げた一方、その匿名性が様々な犯罪で悪用され、例えば、フィッシングに起因するとみられる証券口座に係る不正取引に加えて、匿名・流動型犯罪グループによって実行される、ニセ警察詐欺及びＳＮＳ型投資・ロマンス詐欺といった特殊詐欺、オンライン上で行われる賭博事犯、暗号資産を悪用したマネー・ローンダリング等が発生している。また、犯罪実行者募集情報等の違法情報及び爆発物の製造方法等の有害情報がＳＮＳを中心としたサイバー空間に氾濫しているほか、生成ＡＩといった高度な技術を悪用した事案や企業・団体の事業活動に大きな影響を与えるランサムウェア事案等も発生している。

これらの事案は、いずれも我が国の公共の安全と秩序に対する挑戦であり、我が国の国民生活・経済活動、ひいては国家安全保障及び危機管理に深刻かつ致命的な影響を及ぼすおそれがあることに鑑みれば、こうした観点も踏まえつつ、これらの事案に対処することは警察の責務である。

サイバー空間の匿名性を悪用した事案については、認知した段階においては、国家を背景とする事案及び犯罪組織による金銭目的の事案のいずれに該当するか等は判然としないことが多いものの、国民の生命、身体及び財産の保護の任に当たる警察として、平時から有事に至るまでシームレスに対処する必要がある。そのために、警察は、全国隅々にまで張り巡らされた対処体制による地域に根ざした事案の認知、実態解明、部門を越えた総合力に基づく横断的・俯瞰（ふかん）的分析、検挙及びパブリック・アトリビューション、ひいてはアクセス・無害化措置（警察官職務執行法（昭和23年法律第136

号）第６条の２に基づいて警察官が実施する措置をいう。以下同じ。）に至るまで、あらゆる手段を駆使して対処に当たることが求められる。また、こうした対処に当たっては、内閣官房をはじめとする関係省庁、民間事業者、外国治安機関等との連携を推進する必要がある。

警察においては、以上の情勢認識を十分に踏まえた上で、次に掲げる事項を推進することとする。

第２　推進事項

１　検挙に向けた取組

(1)　事案認知の徹底

事案の認知なくして検挙は達成されないところ、国民・事業者等からの通報・相談は、捜査の端緒となるものである。また、こうした通報・相談は、サイバー空間をめぐる情勢の変化を把握する観点からも重要である。こうした観点から、警察への通報・相談が積極的になされるよう、通報・相談しやすい気運の醸成や環境整備等を推進した上で、被害の届出の迅速・確実な受理も含め、通報・相談に対して適切に対応する。また、こうした通報・相談を官民連携して促進するため、サイバーテロ対策協議会等を通じた事業者等との平素からの信頼関係の醸成及びこれに基づく協力関係の構築を推進する。

さらに、通報・相談といった受動的な事案認知のみならず、能動的な事案認知も重要であることから、サイバーパトロールや能動的解明活動等を通じた積極的な端緒情報の入手に努める。加えて、官民連携の軸となる一般財団法人日本サイバー犯罪対策センター（ＪＣ３）の知見及び情報を事案認知に活用するとともに、内閣官房等とも連携しつつ、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７年法律第42号）の規定に基づく各種情報の把握・認知に努める。

(2)　検挙に向けた捜査の推進

サイバー部門は、国家を背景とする事案か否かにかかわらず、また、罪名のいかんにとらわれることなく、高度な専門的知識及び技術に基づき、サイバー攻撃や高度な技術的手法が用いられる事案等の他部門では対処困難なサイバー事案を中心に、その捜査に果敢に取り組む。

また、サイバー空間の匿名性が匿名・流動型犯罪グループによる特殊詐欺をはじめとした様々な犯罪に悪用されていることを踏まえ、サイバー部門は、他部門が主管するサイバー事案の捜査に対しても積極的かつ主体的な支援を行い、被疑者の特定や暗号資産の形で隠匿された犯罪収益の解明等に貢献するなど、匿名性の打破に取り組む。

その上で、こうした取組を通じて得られた情報を警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部（以下「サイバー特別捜査部」という。）に集約した上、横断的・俯瞰的分析を行うことで、これまで必ずしも明らかにならなかった複数事案同士の関連性、背景にある組織性、上位被疑者等を浮き彫りにし、更なる検挙を推進する。

(3)　国際連携の強化

国境を越えて実行されるサイバー事案の被疑者を検挙するためには、外国治安機関等との緊密な連携が不可欠であることから、都道府県警察は、警察庁を通じて、外国治安機関等からの共助要請に適切に対応するほか、被疑者が国内に所在しない場合であっても、警察庁を通じた国際共同捜査による検挙を目指して捜査を徹底する。

警察庁は、外国治安機関等とのハイレベルの調整を通じて、国際共同捜査への積極的な参画に向けた環境を整備するとともに、サイバー特別捜査部による国際共同捜査を推進し、検挙を通じたサイバー事案の抑止に向け、外国治安機関等との協力関係の強化に取り組む。また、いかなる国家も単独でサイバー攻撃に対応することは困難であることを踏まえ、外国治安機関等との情報・運用面での協力の強化を通じ、サイバー部門における分析・対処能力向上に資する協力を進める。

(4)　サイバー警察活動における適正性の確保

サイバー事案においては発信元を隠蔽するための多種多様な手段が用いられているほか、これらの事案は国境を越えて実行され、その被害も広域かつ不特定の者に及ぶことから、多角的な証拠収集、裏付け捜査並びに電磁的記録の適正な取扱い及び解析・分析の徹底、ログの迅速な確保等のサイバー事案の捜査における基本的留意事項を徹底する。

また、民間事業者又は他部門から提供を受けた情報等については、必要に応じて共有範囲を限定するなど、保秘の徹底を図るほか、各種法令等にのっとり、情報の適正な管理を徹底する。特に、サイバー特別捜査部においては、全国の情報を集約していることから、その情報の厳格な管理を徹底する。

こうした基本が徹底されなければ、国民の警察活動に対する信頼を裏切る結果につながりかねないことから、幹部による適時適切な指揮及び捜査主任官等による管理を通じて、緻密かつ適正な捜査を推進する。

2　未然防止・拡大防止に向けた取組

(1)　検挙による未然防止の推進

ランサムウェア事案等のサイバー事案に対しては、何よりも被疑者の検挙により大本を断つことが最も効果的であることから､外国からのサイバー事案についても、国家を背景とした事案を含め、積極的に事件化を図り、警察庁サイバー警察局及びサイバー特別捜査部並びに都道府県警察が緊密に連携して、国際共同捜査等も活用の上、検挙を通じた抑止を図る。

(2)　情報発信の推進

ア　国際連携によるパブリック・アトリビューション及び注意喚起の推進

警察活動により得られた情報等を活用するほか、外国治安機関や関係省庁等と連携して、サイバー攻撃の攻撃者を公表し非難するパブリック・アトリビューション及びサイバー攻撃の手口や未然防止対策等に関する注意喚起を実施することにより、サイバー攻撃の抑止を図る。

イ　官民連携による情報発信の推進

限りある警察のリソースのみで地域社会全体のサイバーセキュリティの水準を向上させることは困難であることから、サイバー防犯ボランティア、学校、商工

会議所等の地域に根ざした多様な主体と連携しつつ広報啓発活動等を推進するとともに、管理者対策及びサイバーテロ対策協議会等を通じた事業者等への情報発信を推進する。

(3)　犯罪インフラへの対処の推進

ア　犯罪インフラの解体に向けた取組の推進

サイバー空間の匿名性に起因するなりすましを助長したり、警察による追跡を阻害したりするような技術等について、関連法令を所管する省庁及び行政処分権限を有する監督官庁に対して情報提供を行うことにより、サイバー空間の悪用を容易にする犯罪インフラの解体に努めるとともに、いわゆる「道具屋」（不正に調達した預貯金口座等を犯罪者グループに提供する者）や「相対屋」（暗号資産取引所等の市場を通さずに違法な取引を行う者）等を事件検挙を通じて解体する。また、サイバー攻撃の攻撃元であるサーバ等について、その管理者に情報提供を行うことにより、その閉鎖を促進するほか、サイバー事案の踏み台とされている家庭用インターネット通信機器等の対策を推進する。

イ　違法・有害情報への対処の推進

警察活動を通じて認知した違法・有害情報について、ＳＮＳ事業者等に情報提供を行うとともに、インターネット・ホットラインセンターの運用や投稿者に対する個別警告等によりその削除を促進する。また、フィッシングサイト等の実在の事業者のウェブサイト等を装った偽のウェブサイトについて、ＪＣ３や関係事業者等とも連携しつつ、閲覧防止措置等が講じられるよう取組を推進してサイバー空間の環境浄化を図るとともに、不正な口座情報や悪用のおそれのあるクレジットカード番号等の金融機関等への提供を推進して官民が連携してサイバー空間の犯罪インフラ化を防止する。

(4)　効果的なアクセス・無害化措置の実施

検挙及び情報発信・提供を通じた被害の未然防止・拡大防止のほか、サイバー攻撃に対しては、既存の防御の取組とアクセス・無害化措置をはじめとする能動的サイバー防御に係る新たな施策を組み合わせ、多様な手段で粘り強く能動的に対応していく必要がある。そのため、サイバー特別捜査部に、全国の人的・物的リソースを集約した上、国家安全保障上の脅威をはじめとしたあらゆる情報を集約し、内閣官房や防衛省等と緊密に連携しつつ、アクセス・無害化措置を実施する。また、事案の影響が容易に国境を越えるというサイバー空間の特性及び高度化したサイバー攻撃に一国で対応することが困難であることを踏まえ、外国治安機関等との効果的な国際連携を推進する。

3　基盤整備に向けた取組

(1)　人材の確保・育成

社会全体においてサイバー分野における高度な専門的知識及び技術を有する人材の重要性が高まっている一方で、少子高齢化・人口減少、地方の過疎化と都市部への人口集中等の急速な進行により、社会構造が変化し、警察職員の採用情勢も厳しさを増していること等から、サイバー人材の確保・育成を総合的かつ一体的に推進する。

特に、あらゆる犯罪にサイバー空間が悪用されていることから、深刻化するサイバー空間の脅威に的確に対処するため、組織を挙げて全職員の対処能力の向上を図るとともに、アクセス・無害化措置をはじめとする能動的サイバー防御を担い得る高度サイバー人材の確保・育成とキャリアパス管理を推進する。

(2) 資機材の整備

サイバー空間の匿名性を打破するためには、スマートフォンやコンピュータ等の解析を行う解析用資機材、暗号資産追跡ツールといった高度な資機材が不可欠である一方で、財政事情は厳しいことから、効果的かつ効率的な資機材の整備・運用を確保するため、警察庁はサイバー警察局及びサイバー特別捜査部を中心に高度な資機材を整備・集約するほか、ＡＩに対する攻撃及びＡＩを利用した攻撃が新たなサイバーセキュリティ上のリスクとして深刻さを増すことが想定されることを踏まえ、ＡＩ等の先端技術を活用した分析・解析の高度化・効率化を更に推進する。

都道府県警察においても、上記のような警察庁における取組と緊密に連携しつつ、真に必要な資機材の計画的な整備・集約を推進する。

(3) 研究・開発の推進

警察の対処能力を更に高度化するとともに、被害の未然防止・拡大防止を図るべく、ランサムウェアに係る復号ツールを開発するなど、警察における研究・開発を推進する。また、その推進に当たっては、政府が推進する各種プログラムを有効に活用する。

第３　戦略の推進体制

１　警察庁

(1) サイバー警察局

サイバー警察局は、警察庁の所掌事務に関し、「サイバー事案に関する警察に関すること」をつかさどる立場から、サイバー特別捜査部及び都道府県警察を指揮監督し、都道府県警察から報告を受けたサイバー事案について、重大サイバー事案への該当性を判断するほか、国の警察機関として、外国治安機関や関係省庁等との調整を担う。また、サイバー特別捜査部の人的・物的リソースの配分やサイバー特別捜査部による捜査・支援が必要な場合における各部門との調整を担うなど、関係部門と緊密に連携しつつ、全国サイバー部門の中核的役割を果たす。

さらに、あらゆる犯罪に電子機器等が悪用されている中、情報技術解析の重要性が一層高まっていることを踏まえ、「犯罪の取締りのための情報技術の解析に関すること」をつかさどる立場から、全国の情報技術解析部門及び都道府県警察サイバー部門が、それぞれの強みを最大限に発揮して、現場の実情及びニーズに応じた一体的な捜査支援を行うよう指揮監督する。

(2) サイバー特別捜査部

「重大サイバー事案に係る犯罪の捜査その他の重大サイバー事案に対処するための警察の活動に関すること」を分掌するサイバー特別捜査部は、警察庁長官の指揮監督の下、極めて高度な国家性・国際性や無地域性といった特徴を有する重大サイバー事案の対処に当たることとし、そのために必要となる高度な専門的知識及び技

術を有する人材並びに高度な資機材を集約する。

その上で、都道府県警察の捜査により得られた情報や暗号資産の追跡といった高度な専門的知識及び技術に基づく分析により得られた情報等を長官官房企画課匿名・流動型犯罪グループ情報分析室と連携しつつ集約することにより、横断的・俯瞰的な分析を行う。また、分析に当たっては、国家安全保障の観点も踏まえることとする。さらに、こうした分析を生かして外国治安機関等との国際共同捜査を行うことにより、ランサムウェア事案や特殊詐欺事件等を含む様々なサイバー事案の検挙を遂げるとともに、アクセス・無害化措置における中核的な役割を担うなど、重大サイバー事案の対処を担う。

加えて、今後も、デジタル化の進展により、国民生活・経済活動のデジタルサービスへの依存が一層高まっていくとともに、サイバー攻撃が国家安全保障に与える影響も深刻化していくものと考えられることから、サイバー特別捜査部の人的・物的基盤の一層の増強を図る。

2　都道府県警察

都道府県警察のサイバー部門は、事案に係る罪名のいかんを問わず、その高度な専門的知識及び技術に基づき、他の事件主管部門のみでは対処困難な事案について、積極的かつ主体的に捜査を推進する。また、サイバー部門及び情報技術解析部門が一体となって各部門への支援を行い、これらを通じて得られた情報をサイバー特別捜査部に集約するなど、情報集約の結節点としての役割を果たす。さらに、警察の限られた人的・物的リソースを効果的・効率的に利用し、サイバー部門と情報技術解析部門との緊密な連携を確保する観点から、支援要請窓口の一本化やサイバー部門と情報技術解析部門との同一フロア化等を推進する。加えて、国家的背景が疑われるサイバー攻撃への対処に当たっては、国家的背景に関する分析及び外国による諸工作を総体として捉えた対策を効果的に推進する観点から、外国による諸工作に係る知見を蓄積する外事部門と緊密に連携する。もとより、サイバー事案であっても、発生地における住民からの相談受理や初動捜査等、現実空間における対処を伴うことから、警察本部及び警察署が緊密に連携して対処する。

本戦略に基づく取組を、全国警察において、斉一的かつ効果的に推進する観点から、都道府県警察のサイバー部門においては、捜査・支援のみならず、人材育成や官民連携等の各種対策・企画も含めた一体的運用を確保する。

その上で、都道府県警察は、各都道府県の実情を踏まえつつ、警察庁サイバー警察局と緊密に連携して、サイバー部門の一元化組織の整備を検討する。その場合には、サイバー部門が、他部門の捜査への支援及び都道府県警察全体のサイバー対処能力の底上げといった部門横断的な性質の強い任務を負っていることを踏まえ、人事の柔軟性を確保するなど、縦割りを排した上で、他部門と必要な協力を推進できるよう十分に配意する。