実空間とサイバー空間とが融合した
デジタル社会の安全・安心の確保

～マルチステークホルダーで作り上げる安全・安心～

サイバーセキュリティ政策会議

令和３年12月17日

はしがき

近年の IoT、人工知能などの情報通信技術の発達や社会のデジタル化の進展により、今や我々の社会経済活動の多くはサイバー空間を通じて非対面・非接触で行われるものへと大きく移るなど、サイバー空間は、実空間の社会・経済の重要な機能を広く代替し得る空間となったといっても過言ではない。そのような中、金融機関等を装ったＳＭＳ等を用いてフィッシングサイトへ誘導する手口等によりインターネットバンキングに係る不正送金被害が引き続き大きな被害が生じているほか、病院がランサムウェアの被害を受けて診療業務に支障が生じるなど、日常生活に影響を受け、国民は大きな不安を抱えている。このようにサイバーセキュリティの位置付けも転換点を迎えており、重要インフラだけでなく、まさに一人一人の国民をどのように守っていくのかということが問われているのではないだろうか。

サイバーセキュリティ政策会議は、平成 13 年に設置された「総合セキュリティ対策会議」を引き継ぎ、20 年にわたりサイバー空間の脅威への対処に向けた産業界等と警察との連携の在り方について検討し、都度、報告書を取りまとめてきた。令和２年度には、今後のサイバーセキュリティにおける新たな基本理念に「公共空間としての安全性確保」を据えることが必要である旨を提言したところ、警察庁が同提言を踏まえながら、極めて厳しい情勢に対処するため、今次の組織改正を決意するに至ったことは実に感慨深いものである。

そして、本年度のサイバーセキュリティ政策会議は、昨年度の議論を引き継ぎ、顕在化しつつあるリスク等を幅広く洗い出した上で、新たに設置されるサイバー局及びサイバー隊が掲げるべき理念や取り組むべき具体的な施策について検討・議論を行った。

御参画いただいた委員には、それぞれが属する組織や専門分野における知見を背景としつつも、国民目線を持って、中立的かつ相互に対等な立場で積極的に意見を述べていただき、その結果、幅広い内容を報告書として取りまとめることができた。

本報告書が、サイバー局及びサイバー隊が真に実効性ある組織として機能することだけにとどまらず、産学官の関係者とも共有され、多様な主体の取組に活かされることを通じて、国民が安心して生活できるデジタル社会の実現の一助となれば幸いである。

サイバーセキュリティ政策会議委員長

前田雅英

目　次

はじめに

令和２年度サイバーセキュリティ政策会議では、デジタル化の進展等によりサイバー空間が全国民の参画する公共空間へと進化しつつある中、今後のサイバーセキュリティにおける新たな基本理念に「公共空間としての安全性確保」を据えることが必要である旨を提言した。この理念は、政府の新たなサイバーセキュリティ戦略においても「「公共空間」として実空間と変わらぬ安全・安心を確保」することが必要であるとされるなど、社会的な共通認識として定着をみたところである。

その一方で、現在のサイバー空間における脅威の情勢は、国内の企業・団体等におけるランサムウェアによる被害が大幅に増加しているほか、我が国の政府機関、研究機関等に対するサイバー攻撃が多数発生するなど、極めて深刻な情勢が続いている。また、SNS に起因する略取誘拐の被害の増加など、デジタル化の進展等に伴うサイバー空間と実空間との融合を背景として、両者をまたがって行われる犯罪もその脅威の度合いを増している。

こうした深刻な脅威に対処するためには、これまで分散していた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ことや、的確な事案の全容把握と捜査・対策の調整、さらには海外治安機関等と連携した国際捜査の推進等が不可欠である。殊に、近年の重大サイバー事案の捜査等においては、次のような特性が顕著となっている。

- 国家性：海外治安機関等との国際共同オペレーションや特定の国家の帰責性を解明するための捜査等においては、捜査主体が国を代表する立場を有し、事象によっては国自体も捜査主体となり得ることが必要となること。
- 無地域性：攻撃者等の所在地と被害発生地との地理的なつながりが希薄であり、被害も容易に拡散するほか、捜査を要する地域も散在していること。
- 対処リソース集約の必要性：事案解明のためには高度な技術力や態勢構築を要するが、リソースが全国に散在する状態では対応が困難又は非効率であり、これらを集約することが必要となること。

そこで、こうした情勢認識から、警察庁では、令和４年度に、警察庁の内部部局にサイバー事案に関する政策を一元的に担うサイバー局を、関東管区警察局に国の捜査部隊としてサイバー隊を設置することを検討している。サイバー局は、各種サイバー情報の一元的集約・分析、サイバー事案に関する効果的な対策・連携の実施、海外治安機関等との緊密な連携等を担い、サイバー隊は、先に述べた国家性、無地域性、対処リソース集約の必要性を踏まえ、現行の都道府県警察のみによる捜査を補完し、国の機関として自ら国際共同オペレーションや重大サイバー事案の捜査を担う役割が期待される。

サイバー局及びサイバー隊を真に実効性ある組織として確立するためには、掲げるべき理念といった大所高所の観点から具体的な取組に至るまで巨細にわたり検討する必要があ

り、そのためには、まず、デジタル化の進展や新技術の普及等により顕在化しつつあるリスク等を幅広く洗い出す必要がある。そして、この検討を適切に進めるためには、警察部内に限らず、専門性を備え、大所高所かつ国民目線を持つ多様な者が関わることが不可欠である。

そこで、令和３年度サイバーセキュリティ政策会議では、「サイバー局等新組織において取り組む政策パッケージ」をテーマとして、令和３年９月以降、幅広い視座から議論を重ねてきたところである。

本報告書は、サイバー空間を取り巻く情勢とリスク、サイバー局及びサイバー隊に求められる役割、その役割を全うする上での政策課題及びその解決のための具体施策について、本会議における議論の結果を取りまとめたものである。

１　情勢認識

１．１　公共空間化するサイバー空間

(1) 公共空間化するサイバー空間

サイバー空間は、技術革新や新たなビジネスモデルなどの知的資産を生み出す場、創意工夫によって活動を飛躍的に拡張させることができる空間として「無限の価値を産むフロンティア[1]」と捉えられてきた。

実際に、令和２年には個人のインターネット利用率が83.4%に至ったほか、SNSや通話アプリの利用、情報検索、商品・サービスの購入などその利用内容も多様になる[2]など、サイバー空間の利用は広く国民生活に浸透してきた。また、サイバー空間が取り扱えるデータ量の増大やIoT（Internet of Things)、AI（Artificial Intelligence）などの情報通信技術の発達などを経て、サイバー空間において提供されるデジタルサービスの高度化も飛躍的に進んできた。

加えて、新型コロナウイルスの感染拡大を受けた「新しい生活様式」の定着や、これに伴う社会のデジタル化の進展によりこうした状況は更に加速することとなった。この間、これまでサイバー空間とはつながりのなかった様々な業種・業態の事業者がサイバー空間を利用したサービス提供に参入し、また、実空間において対面で行うことを前提としていた社会活動はサイバー空間を通じて非対面・非接触で行われるものへと大きく変容を見せた。その中で、サイバー空間は子供や高齢者も広く参加し、実空間の社会・経済の重要な機能が広く代替される空間となったといっても過言ではない。

今や、スマートフォンで朝のニュースをチェックし、ECサイトで買った食品を食べ、オンラインで業務や授業に参加し、SNS等を通じて友人と交流し、ネット動画を見て余暇を過ごすという光景は、完全に日常のものとなった。サイバー空間は社会経済活動の場として、例えば実空間における学校や公園や図書館といった広く国民に開かれ、利活用される公共施設に勝るとも劣らない機能と役割を担っている。

確かに、サイバー空間は、「空間」としての実体が存在するものではなく、その実体は、端末、ネットワーク機器、ストレージ機器等の物理的な設備の集合体である。また、その機器の多くが民間の事業者により管理される私有財産の集積として存在している。しかしながら、こうした様々な種類・性質を持つ物理的設備の集合体によって構成された「場」は、端末等を用いることにより何人も利用可能な「場」として観念されるものであり（観念としての公共性)、そうした認識が共有されているからこそ、当該「場」を通じて日々膨大な情報がやりとりされ、経済活動が頻繁に行われる現実

[1] サイバーセキュリティ戦略（平成 30 年７月 27 日閣議決定)、１頁。
[2] 令和３年版情報通信白書、50 頁及び 55 頁。

がある。今日、個人レベルはもとより、社会全体のネットワークへの依存度は急速に高まっている（現実社会における公共性)。そうだとすると、この「場」をもって「サイバー空間」と認識し、公共空間そのものとして、現代社会におけるその高い公共性と重要な役割について共通理解を深めていくことが肝要である。

(2) 公共空間としての安全と安心

警察庁が令和２年に実施した犯罪情勢に関するアンケート調査[3]によると、サイバー犯罪に遭うことへの不安感を持っているとの回答は約75％に上っている。これは、日本について誇りに思うこととして長年にわたり最上位に「治安のよさ」があげられている状況[4]とは実に対照的な結果となっている。

国民がこうした不安感を抱える一方で、不安感が必ずしも個人レベルでの具体的な対策の実施に十分に結びついていないなど[5]、個人がそれぞれ有するサイバーセキュリティに対する意識や知識には大きなギャップが存在していることもうかがわれる。一例を挙げると、内閣府によるインターネットの安全・安心に関する世論調査[6]では、インターネットを安全・安心に利用するための対策を行えていない者の６割以上が「何を行ってよいかわからない」ことをその理由に挙げている。事業者におけるセキュリティ対策も、同様に事業者の規模や業種によりばらつきがみられている[5]。

このように、国民がサイバー空間に対して広く不安感を感じているという事実に加えて、個人や事業者ごとのサイバーセキュリティに関する知識や取組に大きな差異がある状況は、公共空間としてのサイバー空間の機能や役割を低減させ、攻撃者に付け込まれるリスクに直結する深刻な問題となっている。

サイバー空間への参画者が、サイバーセキュリティについて自らの役割を認識し、サイバーセキュリティに関する取組を自律的に行うことは、社会全体のレジリエンスを高め、悪意ある主体の行動を抑止するために欠かせないことは言うまでもない[7]。その上で、サイバー空間は、誰もが参画する公共空間としての機能と役割を果たす場となり、安全性と安心感が期待される場となっている。国民や事業者それぞれの自律的な取組に加えて、警察などの公的な機関が必要な役割を果たし、サイバー空間において実空間と変わらぬ安全安心の確保を図っていくことが必要ではないだろうか。

---

[3] 令和２年の犯罪情勢（警察庁長官官房）
[4] 社会意識に関する世論調査（令和２年３月 27 日内閣府)、２．２(3)。
[5] サイバーセキュリティ意識・行動強化プログラム（令和元年１月 24 日サイバーセキュリティ戦略本部決定)、４頁～６頁。
[6] インターネットの安全・安心に関する世論調査（平成 30 年 11 月２日内閣府）
[7] サイバーセキュリティ戦略（令和３年９月 28 日閣議決定）は、サイバー空間を「自由、公正かつ安全な空間」とすべきとの考え方の下、サイバーセキュリティ施策の立案・実施の基本原則のひとつとして「自律性」（サイバー空間の秩序維持に当たり、様々な社会システムがそれぞれの任務・機能を自律的に実現すること）を掲げている。

(3) 令和２年度サイバーセキュリティ政策会議における議論

令和２年度サイバーセキュリティ政策会議においては、「生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進」をテーマに幅広い議論を行った。

議論の中では、

○　今後、サイバー空間は、地域や年齢を問わず、子供から高齢者まで全国民が参画し、重要な社会経済活動を営む、これまで以上に重要かつ公共性の高い場へと変貌を遂げていく。

○　サイバー空間に公共空間としての役割を果たすことが求められるようになってきていることを踏まえれば、たとえ私有財産の集積として構成されるものであったとしても、サイバー空間を公共空間と捉え、実空間と変わらぬ安全安心が確保されることが必要である。

ことなどが確認され、今後のサイバーセキュリティにおける新たな基本理念に「公共空間としての安全性確保」を据えることが必要である旨を提言するに至った。

この理念は、サイバーセキュリティ戦略（令和３年９月28日閣議決定）11頁においても、「サイバー空間においても、「公共空間」として実空間と変わらぬ安全・安心を確保していくため、攻撃者との非対称な状況を看過せず、（略）環境・原因の改善に正面から取り組んでいくことが求められる」とされるなど、社会的な共通認識として定着をみたところである。

１．２　実空間とサイバー空間との融合

(1) 加速するデジタル化

令和２年度サイバーセキュリティ政策会議による報告書提出後も、社会のデジタル化の進展はさらに加速を続けた。

令和３年９月にはデジタル社会の形成に向けた司令塔としてデジタル庁が設置され、「誰一人取り残さない、人に優しいデジタル化」の実現を目指して「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」[8]をビジョンに掲げ、デジタル改革を強力に推進していくこととされるなど、政府における体制の整備が進められたほか、関連事業も積極的に進められている。

【事例】

[8] デジタル社会の実現に向けた改革の基本方針（令和２年 12 月 25 日閣議決定）、２頁。

○　*令和３年７月末時点において、GIGA スクール構想[9]の下、全国の公立小学校等の 96.2%、中学校等の 96.5%が、端末の利活用を開始した。*

○　*令和３年 10 月、デジタル庁においてガバメントクラウド[10]の先行事業等に係る公募が行われ、対象クラウドサービスが決定されたほか、８自治体を事業対象に採択した。*

また、民間セクターにおいても、デジタルトランスフォーメーション（DX）に係る取組を始めていると回答した企業の割合は、令和２年の 28.9%に対して令和３年は 45.3%と大幅に増加[11]しているほか、既存業務の IT 化という範囲にとどまらない事例も見受けられるなど、デジタル化の進展は著しい。

【事例】

○　*令和３年４月、大手商社は海外鉱山の DX プロジェクトに着手したことを発表。同プロジェクトでは、第一段階として操業データや経営・財務データの可視化、関連資機材の予防保守等の実装を予定しているほか、第二段階以降では鉱山操業から港湾操業までのデータ連携や本社機能・マーケット情報との連携による効率化を目指している。*

○　*令和３年４月、国立大学等産学官のグループは、商用５Ｇネットワークを介した手術支援ロボットの遠隔操作に係る実証実験を実施したと発表。当該取組は、遠隔ロボット手術の前段階として位置付けられている。*

また、米国においては、手術後の縫合を AI に学習・実施させる実験が行われるなど、様々な取組が始まっている。

○　*令和３年９月、大手コンビニエンスストア事業者が AI や各種センサーを活用した無人店舗について、令和６年度末までに約 1,000 店の展開を計画していることが報じられた。*

(2) 技術やインフラの進展による実空間とサイバー空間との融合現象

技術やインフラの整備・普及も大きく進んでいる。

常時携帯可能なスマートフォン端末の個人保有率は令和２年には 69.3%に達している。また、スマートフォン、パーソナルコンピューターなどの個人が保有する端末の計算処理機能や通信機能が飛躍的な向上を続けてきたことなどにより、映し出される

---

[9] 全ての子供たちの可能性を引き出す個別最適な学びと協働的な学びを実現するため、児童生徒の１人１台端末と学校における高速大容量の通信ネットワークを一体的に整備する構想。数値は「端末利活用状況等の実態調査（令和３年７月末時点）（確定値）」（令和３年 10 月文部科学省）、１頁。

[10] 政府共通のクラウドサービス利用環境。デジタル社会の実現に向けた重点計画（令和３年６月 18 日閣議決定）13 頁において「全ての地方公共団体が、目標時期である令和７年度（2025 年度）までに、（略）移行する統一・標準化を目指す」こととされている。

[11] 一般社団法人日本能率協会「2021 年度（第 42 回）「当面する企業経営課題に関する調査」」

画像や音声の品質も向上し、入出力機能などのインターフェースの多様化も進んだ。加えて、端末上で利用可能なアプリケーションやサービスも質的・量的に拡大した。

いまやスマートフォンなどの個人の情報端末は、コミュニケーションなどの特定の目的を果たすにとどまらず、いわば「サイバー空間の入口」としての役割を果たしている。常時携帯して生活することが可能なスマートフォンは、利用者に対していつでもどこでもサイバー空間に高速でアクセスすることができる環境を提供する。また、高品質な画像や音声に加えて、直感的でインタラクティブな操作を可能とするインターフェースは、今後の更なる機能向上等により、利用者に対して実空間に近い臨場感や高い没入感を与えるものとなり得る。

加えて、実空間と高度に連動した便利なサービスや実空間以上に多様なエンターテインメントがより一層提供されることなどにより、国民生活にとっての実空間とサイバー空間は、明確な境界を意識することなく自由に行き来しながら活動する高度に融合した場として機能するものとなっていく可能性がある。

通信インフラ面での実例として、これまでサイバー空間へアクセスするための通信環境は、アクセスする主体である人が存在する居住地・勤務地等を中心に整備されてきたところであるが、近年、中・低軌道に多数の小型非静止衛星を打ち上げて連携させることで、陸・海・空問わず地表全域での高速大容量通信を可能とする衛星コンステレーションに係る取組が進められており、今後はいつでも、どこでもサイバー空間につながることが可能となる。加えて、超高速・大容量、低遅延、多数同時接続が可能な第５世代移動通信システム（５Ｇ）の普及は、遠隔地にある機器を正確に制御すること、あるいは人の手を介することなく関連するデータを、サイバー空間を介して機器が自ら収集し制御するという状況を現出させ得る。

このように、いつでも、実空間のどこからでも、誰でも（どんなモノでも）サイバー空間につながり、活動できる、カバレッジ100%を前提とした社会においては、これまでの地理的・時間的な制約を越え、日常生活から国家機能まであらゆる場面で実空間とサイバー空間との高度な融合が更に進展する可能性がある。経済発展と社会的課題の解決を両立するSociety5.0は現実のものとなりつつある。

【事例】

○　*令和２年３月に商用化された５Ｇ技術は、基地局の整備が進められており、令和３年１月、大手通信事業者は令和４年３月には人口カバー率90%に達する予定と発表した。*

○　*衛星コンステレーションについて、令和３年９月、大手通信事業者が米国企業と提携して令和４年を目処に導入を開始すると発表した。また、令和３年６月に策定された宇宙基本計画工程表改定に向けた重点事項（令和３年６月29日宇宙開*

発戦略本部決定）において、我が国独自の衛星コンステレーションの構築に向けた戦略的な取組推進が掲げられた。

○　５Ｇ技術の特徴のさらなる高度化や、衛星コンステレーション、成層圏を飛行する無人航空機を基地局とするHAPS（High Altitude Platform Station）等異なる通信システムとシームレスにつながり、あらゆる場所で通信を利用可能とする拡張性等を有したBeyond５Ｇに向けた研究開発も進められている。

このような状況を背景として、実空間とサイバー空間とが融合した社会においては、「21世紀の石油」とも呼ばれるデータが新たな価値を創出するData Driven Economyを通じて、例えば以下のような形で人々に多大な恩恵をもたらすと期待されている。

○　職人技等個人あるいは集団の内面に根付き、その継承・再現には長期間にわたる修練が必要であるなど、広範な活用が困難であった価値（暗黙知等）をデータ化し、普遍化・活用することが可能となり、より高品質なサービスを広く提供する

○　多様なデータがIoT機器等を通じて実空間にフィードバックされることで新たな製品・サービス（予防保守、自動運転、事業計画策定等）を創出する

○　登録された個人情報等に基づく柔軟かつ個人毎にカスタマイズされたサービスの提供等により生活の質が向上する

１．３　顕在化しつつあるリスク

１．３．１　デジタル化に伴うリスク

実空間とサイバー空間とが融合した社会においては、１．２(2)において述べたとおり、我々の生活の利便性の向上のみならず、サイバー空間を通じて流通する膨大なデータや各種情報通信技術の利活用を通じて創出される価値が飛躍的に向上することが期待される。

その一方で、表出し得るリスクにも目を向ける必要がある。データの価値の高まりは、データが窃取・破壊された場合の被害を今までになく拡大させることは確実である。また、サイバー空間を飛び交う情報の量や機器の計算処理能力は、早晩、あらゆる場面で人間の認知判断能力を遥かに超えるものとなりかねず、巧妙な欺罔行為の横行など、サイバー空間に参画する人間の誤認や判断の誤りが様々な事態を招く可能性がある。さらに、デジタルサービスやサプライチェーンの相互連鎖の進化は、発生し得るサイバー事案の影響範囲の見通しや事案の解明・対策をさらに困難なものとしかねない。このように、サイバー事案が発生した際の潜在的な被害の内容や影響範囲等が、これまでと比較して別次元といえるレベルにまで高まり、国民生活の安全・安心は大きなリスクにさらされるという脆弱性も有することとなる。

こうしたデジタル化の恩恵と表裏一体のものとして表出し得るリスクを網羅的に整理することは非常に困難であるが、データの価値の増大と潜在的被害の拡大、人間の認知判断能力の限界、拡大するサイバー事案の影響範囲という３つの視点から、いくつかの代表的な例と考えられるものを以下に示す。

(1) サイバー空間におけるデータの価値の増大と潜在的被害の拡大

① データ窃取を通じた「新たな価値」の窃取

サイバー空間を飛び交い蓄積されるデータは、通信技術やIoT技術の進展等に伴い質的にも量的にも増大の一途を辿っている。また、AIの発達等によりデータの処理や活用の方法が高度なものとなるにつれ、既存のデータが持つ価値自体も高まる傾向にある。このようなデータの価値の向上は、同時にそのデータが窃取された場合に失われる価値の増大を意味している。

従来、サイバー攻撃による情報の窃取は、企業が保有する先端的な技術情報や顧客情報といったものが対象であった。これは窃取の対象物が複写や伝送が可能な電磁的記録として保管されている情報に限られるという窃取行為の内在的な制約によるものであった。

しかし、前述のように、職人技等個人・集団の内面に存在し、従来は可視化（言語化）が困難であった価値までもがデータ化されれば、その価値自体を窃取し、再現することが可能になる。

例えば、日本の製造プロセス技術においては、バリューチェーンの中での密接な擦り合わせに基づいて蓄積された技術者の経験とノウハウが我が国の強みとなっているとされている[12]が、我が国経済の強みの１つであるこれらの価値が窃取されることとなれば、経済安全保障の観点から我が国の社会基盤全体を揺るがす脅威となり得る。

また、データの窃取のみならず、既に広範に流出し、又は公開されているデータや、それらをAIなどの情報通信技術を用いた高度な分析・加工して得られるデータが悪用されることも脅威となり得る。

例えば、顔画像や容貌を撮影した動画等を用いてオンラインで本人確認を行うeKYC（electronic Know Your Customer）認証が広く世の中で用いられているが、窃取したと思われる顔画像や動画といった認証用データが既にダークマーケット等において流通しており、攻撃者がこれを用いて認証を不正に突破するというおそれがあることは、現在においても指摘されている。今後は、このような本人から窃取したと考えられるデータではなく、ディープフェイクのような技術等を用いて「作

[12] マテリアル革新力強化戦略（令和３年４月27日統合イノベーション戦略推進会議決定）、16頁。

成（流出等したデータを組み合わせるなどの加工）」した生体認証データを用いて画像照合をはじめとする様々な認証システムを突破し、不正な口座開設を行うといったことがなされるおそれもある。

また、中学、高校等の卒業名簿が振り込め詐欺グループの架電先の選定に悪用された例などはこれまでも確認されているが、サイバー空間においても同様の情報の悪用が想定される。一例を挙げると、今後、攻撃者がSNSへの投稿等のサイバー空間上のデータを収集・分析し、攻撃対象となる者の出身小学校やペットの名前など、本人しか知り得ないはずの情報を推測・把握することで、知識認証（IDやパスワード、秘密の質問への回答といった本人のみが知る情報を用いて利用者を認証する方式）を不正に突破するなどのリスクが広範に発現する可能性もある。

このように、既に広範に流出し、又は公開されているデータ自体にAIなどの情報通信技術を用いた高度な分析・加工が施されることにより新たなリスクの要因となることや、相互連鎖が進化するデジタルサービス等において当該データが新たな目的で悪用されるなどのリスクにも留意すべきである。

② データ汚染による被害の拡大

DNSサーバ[13]のキャッシュ情報を書き換えて意図しないWebサイトに誘導するキャッシュポイズニングや、チャットボットに悪意あるデータを習得させ適切でない反応をさせるなど、不正なデータの混入等によりデータが汚染されることで生じる被害は、比較的限定的な範囲の被害に収まっていた。

しかし、データの信頼性は、様々な機器の制御や企業活動がデータに依存することとなる中で社会経済活動にとって死活問題となる。例えば、入力されるデータを不正なものにすり替えられるとライフラインを支える制御機器、自動運転車、遠隔手術ロボット等を誤作動させることで人命に関わる重大事故が発生するおそれがあり得るし、データ汚染により事業計画や操業判断を混乱させられると、事業者にとっては企業存続にかかわるほどの経済的損害が発生するおそれも生じる。

また、AIに関しては、学習データに不正なデータを混入させ、特定の入力データを攻撃者が意図したものとして誤って認識させるバックドア攻撃と呼ばれる手法が存在する。このような手法が用いられると、入退室認証に画像認識カメラが使用されていた場合に本来権限を持たない者が認証を突破して入退室してしまったり、特定の者が認識された場合に遠隔手術機器に誤作動を起こさせ危害を加えるなどといったことも生じるおそれがある。

[13] 名前解決（ドメイン名やホスト名とIPアドレスを変換すること）のサービスを提供するアプリケーション及びサーバ装置。

このように、攻撃者によるデータ汚染の脅威は、人命や企業存続に影響を及ぼすほどに高まり得る。

(2) 人間の認知判断能力の限界の悪用

① 欺罔能力の高度化による被害の拡大

現在も、他者になりすまし金銭をだまし取るなどの他人の認知判断の誤りを悪用する犯罪手口は多くの被害を生んでいる。

インターネットバンキングの不正送金被害の多くの発端となっているフィッシングについて、フィッシング対策協議会に令和２年中に届け出されたフィッシング情報の件数は 224,676 件（前年比 168,889 件、303％増）[14]と、前年から著しい増加を見せている。

また、実空間においても、特殊詐欺[15]の被害が、依然として高齢者を中心に高い水準で発生している。特にオレオレ詐欺に預貯金詐欺（前年まではオレオレ詐欺に包含）を合わせた令和２年中の被害額は 126.1 億円（前年比 8.5 億円、7.2％増）と、前年より増加している。

さらに、インターネット検索で表示されたウェブサイトにおいて、巧みに電話を架電するよう誘導して犯行に及ぶテクニカルサポート詐欺のように、サイバー空間と実空間とを連携させる手口も確認されている。

デジタル化の進展は、サイバー空間上を流通する個人の嗜好・行動履歴等の膨大なデータや情報通信技術を悪用する機会を犯罪者側にも与えることとなる。例えば先に述べた既存の脅威に関して、サイバー空間上の膨大な情報と合わせて機械学習等を悪用することで、実在する人物をサイバー空間上で高精度に再現することが可能となり、個々の標的が持つ属性・背景を踏まえた内容によるフィッシング詐欺、特殊詐欺、ビジネスメール詐欺、標的型メール攻撃等が可能となる。また、内容の巧妙化に加え、機械学習により現実の人物を模した映像・音声を生成するディープフェイク等の技術が組み合わさることで、視覚的・聴覚的にも高度な欺罔手段が機械的に量産することが可能となれば、特殊詐欺（現在欺罔手段の大半を占める電話だけでなく、テレビ電話等にも進出可能になる）等の脅威が爆発的に拡大する可能性もある。

---

[14] フィッシング対策協議会の月次報告書（https://www.antiphishing.jp/report/monthly/）から集計

[15] 被害者に電話をかけるなどして対面することなく信頼させ、指定した預貯金口座への振込みその他の方法により、不特定多数の者から現金等 をだまし取る犯罪（現金等を脅し取る恐喝及びキャッシュカード詐欺盗を含む。）の総称。

このように、他人を欺罔して金銭をだまし取るという既存の脅威が技術の悪用により質的にも量的にも別次元といえる段階まで引上げられ、拡散するという新たな脅威についても認識する必要がある。

② インフォデミックの発生

SNS 等の発達に伴いインフォデミック（information と epidemic を合成した言葉であり、正確・不正確の別を問わず大量の情報が伝染病のように広がり、現実社会に影響を及ぼす現象を指す）への対応、特に偽情報の流布や偏向した情報の氾濫への対処は社会的課題となっている。

【事例】

○ 総務省が実施した調査[16]によると、新型コロナウイルス感染症に関する偽情報（「こまめに水を飲むと新型コロナウイルス予防に効果がある」など）に対して、「正しい情報ではないと思った・情報を信じなかった」と答えた人の割合は、一部の情報を除き、３割～６割程度となっており、間違った情報や誤解を招く情報について、情報を信じてしまった人やその真偽が分からなかった人が相当数存在していた。

○ 令和２年に全国的に発生したトイレットペーパーの買い占め騒動に関し、トイレットペーパーが品切れになるとのデマ投稿自体ではなく、当該デマ投稿を否定する投稿が爆発的に広がったことが要因との報道もなされている。

このような偽情報の流布は、インターネット上に限った問題ではなく、これまでも人々の口コミ等で真偽が不明で信頼性の低い情報が拡散される事例は存在したが、SNS 等が有する情報流通の特性である情報の拡散されやすさ、価値観の似た者同士で交流・共感することで特定の意見等が増幅され影響力を持つ「エコーチェンバー[17]」、利用者が好ましいと思う情報ばかりが選択的に提示されることで思想的に社会から孤立する「フィルターバブル[18]」等が一因となってインフォデミックと呼ばれるほどの大きな問題として顕在化していると考えられる。また、情報発信の当事者が必ずしも意図せぬ形で混乱が助長される場合も多いとされる。他方で、当該特性を悪用し、意図的に偽情報や偏向した情報を広く流布させることにより何ら

16 新型コロナウイルス感染症に関する情報流通調査（総務省）、18 頁。

17 令和元年版情報通信白書 102 頁によると「ソーシャルメディアを利用する際、自分と似た興味関心をもつユーザーをフォローする結果、意見を SNS で発信すると自分と似た意見が返ってくるという状況を、閉じた小部屋で音が反響する物理現象にたとえたもの」をいう。

18 令和元年版情報通信白書 103 頁によると「アルゴリズムがネット利用者個人の検索履歴やクリック履歴を分析し学習することで、個々のユーザーにとっては望むと望まざるとにかかわらず見たい情報が優先的に表示され、利用者の観点に合わない情報からは隔離され、自身の考え方や価値観の「バブル（泡）」の中に孤立する情報環境」をいう。

かの不正な利益を得たり、世論を誘導するなどの社会的混乱を生じさせようとする行為も行われ得る点にも十分注意を払うべきである。

(3) 拡大するサイバー事案の影響範囲

① サプライチェーンの複雑化・ブラックボックス化により拡大する被害

デジタルサービスの相互連鎖の拡大やサプライチェーンの複雑化は、ひとたびサイバー事案が発生した場合の影響範囲を飛躍的に拡大させてしまうというリスクを内在している。

例えば、国民生活や産業分野における IoT 機器の普及により、あらゆるモノがインターネットに接続される社会に確実に近づきつつあるが、このことは同時にサイバー攻撃が直接的に国民生活や産業のあらゆる場面に影響を与えることを意味している。広範に普及する IoT 機器の所有者等によるセキュリティ対策が十分に行われず脆弱性が放置されれば、膨大な数の IoT 機器の乗っ取りによる DDoS 攻撃に悪用されるなど、ますます多様な観点からリスク要因を捉える必要が生じている。また、重要インフラ事業者の有する制御システムへのサイバー攻撃が当該重要インフラサービスの供給等に支障を与えることとなれば、当然に国民生活への影響は重大なものとなる。

実際に、複雑に入り組んだサプライチェーンの連鎖やサービス連携の発達等に伴い、通信等のインフラへの障害やサイバー攻撃の影響が広範に拡大する状況が見受けられる。

【事例】

○ 令和３年 10 月に発生した大手通信事業者の大規模通信障害においては、通話やデータ通信が利用できなくなったユーザーが約 100 万にのぼり、同社のデータ通信に依存していたキャッシュレス決済サービスの利用が一部困難となる等市民生活に広く影響を及ぼした。

○ 令和２年 12 月、米国の大手 IT インフラ管理ソフトウェア会社がサイバー攻撃を受けた結果、同社製品に係るアップデートファイルに不正なコードが埋め込まれ、アップデートを行った顧客全体に脆弱性が拡散し、米国の多数の政府機関を始めとする世界中の組織に影響が生じた。

○ 平成 28 年から平成 29 年にかけて行われた JAXA を始めとする約 200 の国内企業等へのサイバー攻撃においては、攻撃者が我が国のみで販売されていた IT 資産管理ソフトを事前に入手し、脆弱性を調査した上で攻撃した蓋然性が高いと報じられた。

また、令和２年中に発生したキャッシュレス決済サービスに係る不正振替においては、当該サービスと銀行口座の連携時における本人確認方法の脆弱性が悪用された。

さらに、キャッシュレス決済サービスの普及に伴い、様々なサービスにクレジットカード情報がひも付けられることにより、サイバー空間、実空間を問わずクレジットカード不正利用事案が多発しており、その被害額も令和２年下半期の 132.2 億円に対し令和３年上半期は 155.6 億円となるなど増加傾向にある[19]。

このように、サービスが複雑に連携する中で、連携サービスの全体を通じてどのように本人確認がなされ、どのようなセキュリティ対策がとられているかといった全体像が不透明となり、想定外の被害が生じるおそれもある。

今後、新技術の普及や、デジタル化によるサプライチェーン等の一層の複雑化とそれに伴うブラックボックス化により、事故やサイバー攻撃等の影響範囲も格段に広がり、かつ、影響がどこに発現するのか把握することが困難となることが予想される。

１．２(1)において述べた鉱山に係る事例のほかにも、例えば農業分野においても農薬散布や収穫時期の決定等にデータが活用されるなど、第一次・第二次産業のデジタル化が進んでいる。このような原料等の供給者に対しサイバー攻撃を行って操業を停止させたり、データの窃取により供給量を事前に把握することで、商品先物市場等における不正な利益の獲得を狙った攻撃が行われることもリスクの一例として考えられる。また、例えばキャッシュレス決済サービスのアカウント開設時の本人確認を、当該アカウントと連携する銀行等による本人確認により代替するなど、様々なサービスが本人確認や認証等の様々なフェーズでの連携を深める中で、セキュリティが脆弱であったり、本人確認手続がずさんな別のサービスを経由することで、それ自身は強固なセキュリティを備えた既存の重要なサービスにおいても被害が生じる可能性がある。

②　拡大する子供・若者の被害

多くの国民がサイバー空間に参画する中、サイバー空間を通じた子供・若者の被害も広がっている。

【事例】

[19] 「クレジットカード不正利用被害の発生状況」（令和３年９月一般社団法人日本クレジット協会）

○　認知されたいじめの態様として「パソコンや携帯電話等で、ひぼう・中傷や嫌なことをされる」が小学校・中学校・高等学校合わせて18,870件と過去最多となった[20]。

○　SNSに起因する略取誘拐の被害に遭った18歳未満の子供が75人（前年比63%増）に上ったほか、児童福祉法、青少年保護育成条例、児童売春・児童ポルノ禁止法、重要犯罪等を合わせた全体の被害児童数も1,819人と引き続き高水準を記録した[21]。

なお、上記被害児童のうち、フィルタリングの利用については、回答があった者1,151人のうち、利用していない者が984人と約85%を占めるに至っている。

○　GIGAスクール構想の下で端末が広く整備される中、学習用端末を児童・生徒が使用する際にネットトラブル（コミュニケーショントラブル、不適切サイトの閲覧、個人情報・プライバシー関連等）が発生したことがあると回答した者が中学校では39.3%に上っている[22]。

実空間においては、少年の健全な育成を阻害するおそれのある行為や環境が条例等により規制され、一部の施設への青少年の深夜入場が規制されたり、有害図書等の青少年への販売が禁止されるなど、子供・若者の健全育成のための枠組みが多角的・複層的に存在する。これに対し、サイバー空間では、例えばSNSアプリの利用等が保護者等の判断に委ねられているといった状況も見られる。今後、子供・若者のデジタル社会への参画が更に加速していく中、デジタル社会における青少年の健全な育成が課題となる。

③　クロスリアリティ技術の進展による被害の拡大

仮想空間（VR）や拡張現実（AR）等のクロスリアリティ技術の進展に伴い、メタバース（「meta」と「universe」から作られた造語であり、サイバー空間上に構築される多人数参加型の３次元仮想世界を指す）は、今後、急速に普及する可能性がある。

【事例】

○　令和３年９月、大手通信事業者は仮想空間上に様々な活動を行うことが可能な仮想都市基盤を構築し、令和４年から提供予定と発表した。

---

[20] 令和２年度 児童生徒の問題行動・不登校等生徒指導上の諸課題に関する調査結果について（令和３年10月13日文部科学省）、３頁及び31頁。

[21] 令和２年における少年非行、児童虐待及び子供の性被害の状況（令和３年３月警察庁）、20頁。

[22] 一人一台端末環境におけるICT活用と情報モラル教育の実践に関する調査報告書（令和３年８月一般財団法人LINEみらい財団）、20頁及び22頁。

○　令和３年 10 月、米国の大手 SNS 事業者は社名変更に合わせてメタバースへ注力すると発表した。

○　令和３年 11 月、米国の大手ソフトウェア開発事業者は仮想会議への参加や、仮想空間上での共同作業等を可能とするツールを令和４年に提供開始すると発表した。

メタバースは、従前の多人数参加型のオンラインゲームのように、限定された空間の中で一定の制限の下で活動するものではなく、アバター（仮想空間上における利用者の分身）がその空間の中で自由に活動し、他者との交流の場となり、様々な領域のサービスやコンテンツが取引され消費される場ともなるものとされている。

その普及により既に顕在化している、あるいは顕在化しつつある様々なリスクの深刻化や拡大につながることも想定される。例えば、ディープフェイクのように現実の人物等を模擬するものとは異なり、元来電子データに過ぎないアバターの外形を複製することは容易であり、本人確認等がますます困難となるほか、なりすまし等の被害の拡大や、事後追跡可能性への支障が想定される。

また、将来的には、実空間で行われていた取引や会議などの重要な活動がサイバー空間上に進出するという現状をさらに踏み越え、サイバー空間が実空間以上に重要な役割を担うこと、例えばメタバース内でのサービスの利用や「通貨」の流通により実空間を上回る経済圏が形成されることなども考えられる。そのような新たな形態の社会においては、現時点では想定し得ない新たな恩恵とともに、リスクも次々と生じ得る。

１．３．２　国際情勢から見たリスク

サイバー空間は、従来から地政学的緊張を反映した国家間の競争の場の一部となっているが、近年はサイバー攻撃の脅威の増大が見られる[23]。

国家の関与が疑われるサイバー攻撃として、政府機関や先端技術保有企業等の情報窃取、軍事的・政治的目的の達成に向けての影響力行使、外貨の獲得等を目的としたものが発生している[23]。

このように脅威が増大する中、今や、サイバー空間をめぐる情勢は、有事とは言えないまでも、最早純然たる平時とも言えない様相を呈していると評されるに至っている[23]。

また、直接的なサイバー攻撃以外にも、サイバー空間に関する基本的価値の相違や、国際ルール等をめぐる対立が顕在化している[23]。

【事例】

[23] サイバーセキュリティ戦略（令和３年９月 28 日閣議決定）、８頁。

○　平成 16 年（2004 年）から累次にわたり国際連合第１委員会（軍縮・国際安全保障問題を所掌）の下に国連政府専門家会合（GGE）が設置され、サイバー空間における責任ある国家の行動に関する 11 の規範[24]（国家はその領域が ICT を用いた国際違法行為に利用されることを了知しながら許すべきではない、国家はインターネット上の人権を保障すべきである、国家は故意に重要インフラに損害を与える ICT 活動を行ってはならない、国家はサプライチェーンの完全性を確保するための合理的な措置を講じるべきである等）の提言や、国連憲章全体を含む既存の国際法がサイバー空間に適用されることの確認等がなされてきたところ、GGE と同様の議題を扱いながらも別の枠組みとなるオープン・エンド作業部会（OEWG）を第１委員会の下に設置することが平成 30 年（2018 年）に決定された。

○　日米欧等 66 か国（令和３年（2021 年）９月末現在）が締結している欧州評議会策定のサイバー犯罪条約（通称ブダペスト条約。平成 13 年（2001 年）に欧州評議会において採択、同年中に署名式典が開催され、我が国も署名。）とは別に、情報通信技術の犯罪目的での利用に対処するための包括的な国際条約を検討するオープンエンド・アドホック政府間専門家委員会の国際連合への設置を求める決議が令和元年（2019 年）11 月に採択された。ロシア外務省は、「既存の多国間条約は 10～20 年前に作成されたもので、サイバー犯罪の動きに追いつけていない」、「国境を越えるデータへのアクセスに関する規定は国家主権の原則等を侵害する危険性が高い」などとの批判を行っている[25]。

さらには、安全保障の裾野が経済・技術分野にも拡大する中で、技術覇権争いも顕在化している[26]。

【事例】

○　米国は、令和２年（2020 年）８月に、クリーンパス（クリーンネットワーク）構想を発表し、悪意ある攻撃者から市民を守るため、通信キャリア、アプリストア、アプリケーション、クラウドサービス及び海底ケーブル事業から信頼できない事業者を排除する計画を発表した。また、令和３年（2021 年）６月には、米国連邦通信委員会が安全保障上のリスクとみなす外国企業５社の通信機器の認証を禁じ、米国内市場から事実上排除する方針を決定した。さらに、令和３年（2021

[24] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (https://digitallibrary.un.org/record/799853)

[25] International Community Has Become Closer to “Cybercrime Vaccine” (https://www.mid.ru/en/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2p053/content/id/4836268)

[26] サイバーセキュリティ戦略（令和３年９月 28 日閣議決定）、８頁。

年）10月には、サイバー攻撃に悪用される可能性のあるサイバーセキュリティ製品の取引を規制する案を公表（パブリックコメントを実施）した。

○　海底ケーブルについては、米政府の懸念表明により接続先を変更することとなった計画が存在するほか、太平洋諸島に係る海底ケーブル計画について入札実施後に必要な条件が満たされていないなどとして無効とされた事例等がある。また、北極海の海氷面積が縮小していることに伴い、同海域における海底ケーブル敷設について周辺各国の注目が集まっているところ、令和元年（2019年）６月に発表された国際プロジェクトが令和３年（2021年）５月に凍結された結果、ロシア単独のプロジェクトのみが残り、令和８年（2026年）の完成を目指して敷設が進められることとなった。

１．３．３　サイバー犯罪者集団等によるリスク

サイバー空間上の犯罪者集団による脅威が世界的に高まっている。令和３年（2021年）５月に発表された米企業の調査[27]によると、世界における漏えい・侵害に係る攻撃者の種類として「犯罪組織」が全体の約８割を占めると言われている。

ランサムウェアに関しては、実際に市民生活に多大な影響を及ぼした事例も多数発生している。

【事例】

○　令和３年（2021年）５月、米国の石油パイプライン事業者最大手がサイバー犯罪集団によるランサムウェアDarkSideを用いた攻撃を受け、操業を約１週間停止した結果、一部地域で燃料不足が発生した。

○　令和３年（2021年）５月、世界最大の食肉加工業者がサイバー犯罪集団によるランサムウェアREvil（別名：Sodinokibi）を用いた攻撃を受け、米国、オーストラリア及びカナダにある食肉加工工場の操業を３日間停止した結果、食肉価格が高騰した。

○　令和３年10月、国内の医療機関がランサムウェアを用いた攻撃を受け、約８万５千人分の電子カルテが暗号化され閲覧できなくなった結果、新規の診療や救急患者の受入れを停止した。

攻撃の方法も巧妙化しており、被害の未然防止がより困難なものとなってきている。

【事例】

○　令和３年（2021年）７月、世界各国の企業がランサムウェアREvilを用いた暗号化の被害に遭った事例では、米国のソフトウェア会社が提供するシステム管理

[27] Verizon社「2021年度データ漏洩／侵害調査報告書」

サービス VSA のゼロデイ脆弱性[28]を悪用したサプライチェーン攻撃が発端となっている。

○　警察庁が令和３年上半期中にランサムウェア被害を警察に申告した企業に対し行ったアンケート調査によると、感染経路はメール又はメールに添付されたファイルによるものが 13%であるのに対して、VPN 機器からの侵入が 55%、リモートデスクトップからの侵入が 23%となっており、テレワークの急速な拡大等に伴い生じた弱点を巧妙に突かれている傾向が見受けられる。

さらに、攻撃手段となるマルウェアの耐解析機能（解析を妨害、遅延等させる機能）も高度化している。捜査機関やセキュリティベンダーによる解析を阻害するため、ソースコード改変によるパターンマッチング[29]の回避といったものだけでなく、文字列の暗号化や解析環境の検知といった様々な機能を搭載し、難易度を質・量両面で高めており、解析に基づく対策の実施に要する時間の増大、ひいては被害の拡大につながっている。

【事例】

○　ランサムウェア Conti は、大量の無意味な API を呼び出す、実行する全ての文字列を暗号化する等の耐解析性を備えている。

○　ランサムウェア EKANS(SNAKE)の一部は、特定ドメインに接続できた場合にのみ機能することにより、標的以外で機能が発現し発見されることを回避するとともに、当該標的と同様の環境を整えなければ解析することができない機能を備えている。

○　ランサムウェア Ragnar Locker は、解析されていることを検知するとランサムウェア自身を強制終了する機能等を備えている。

このように、犯罪者集団による攻撃が悪質・巧妙化していることに加え、一部のフォーラムサイト等では攻撃ツールの売買等がなされ、一定程度の技量があれば、特別な専門知識がなくても誰でもサイバー攻撃を行うことができる犯罪インフラ（犯罪を助長し、又は容易にする基盤）が構築されている。さらには、直接的な攻撃に関連するものだけでなく、例えば VPN やプライベートプロキシ等匿名化の手段の提供、窃取したクレジットカード情報が有効であるかの検証、マネー・ローンダリングの実行等を担うものも存在し、これらが広範につながり、ある種のエコシステムを形成しているとの指摘もある。

[28] 修正プログラム提供前の脆弱性

[29] 既知のマルウェアが持つ特徴的なコードをパターンとしてリスト化し、検査対象のファイルと比較することでマルウェアの検出を試みる手法。

令和３年（2021 年）10 月 13 日及び 14 日には、ランサムウェアを用いたサイバー攻撃に対する国際連携を強化するため、日・米・欧・EU など 32 か国・地域が参加するオンライン会議が開催され、ランサムウェアを深刻化する地球規模の安全保障上の脅威とする共同声明が発表[30]されるなど、サイバー犯罪者集団等による脅威は世界的に深刻化している。

[30] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021(https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/)

２　基本理念及び政策課題

２．１　基本理念　～新組織が果たすべき役割～

「世界一安全な日本」はかけがえのない社会の財産である。そして、その財産を育み、守り抜くことは警察組織全体が果たすべき役割である。

しかしながら、現下のサイバー空間の情勢を見ると、ランサムウェアによる被害やサイバー攻撃が多発するなど、その脅威は極めて深刻である。加えて、犯罪被害にあう不安感の第１位をサイバー犯罪が占めている点[31]も憂慮される。「はじめに」で述べたとおり、警察庁において令和４年度に設置することを検討している新組織、すなわちサイバー事案に関する政策を一元的に担うサイバー局、国の捜査部隊として国際共同オペレーションや重大サイバー事案の捜査を担うことが期待されるサイバー隊には、公共空間としてのサイバー空間の安全・安心を脅かす脅威への対処が強く求められていることは言を俟たない。

他方、サイバー空間と実空間とが融合した新たな社会においては、これまで述べてきたように、犯行手口やその被害・影響がサイバー空間の中だけにとどまらず、加えて脅威のレベルがこれまでとは次元の違うレベルにまで高まることから、サイバー空間のみを捉えて安全・安心を追求することは非現実的であり、特にサイバー空間と実空間にまたがる脅威に注意を払うべきである。

加えて、新組織が対策の対象として念頭に置くべき脅威は、インターネットバンキングに係る不正送金事犯等のような身近なものから、高速通信網や技術革新を悪用するものまで広範にわたる。１．３において整理したデジタル社会で顕在化しつつあるリスクは、必ずしも警察が主導して対応するべきものばかりではないものの、こうした広範な脅威を幅広い視点から捉え、警察として取り組むべき事項を検討する上で有益な観点となるものと考える。

新組織は、実空間と公共空間としてのサイバー空間とが融合したデジタル社会においても安全・安心を実現するための中心的な役割を果たすことが求められており、刑事部門、生活安全部門、交通部門、警備部門などの警察の既存部門と連携し、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することはもちろんのこと、多様な主体と手を携えて（マルチステークホルダー・プロセス[32]）、新たな社会においてもこれまで以上の安全・安心を実現しなければならない。

---

[31] 令和２年の犯罪情勢（警察庁）

[32] 内閣府資料（https://www5.cao.go.jp/npc/sustainability/concept/index.html）によると「多種多様なステークホルダーが対等な立場で参加し、協働して課題解決に当たる合意形成の枠組み」であり、参加主体間の信頼関係醸成、得られた合意に係る正当性の担保、参加主体による主体的な取組の促進、全体最適の追求等を可能とするものとされている。サイバー空間にあらゆる主体が参画する中、課題解決のため、特定の主体に限らず組織や個人を含め広く連携を図ることが求められる。

以上を踏まえて、サイバー局・サイバー隊に求められる役割、すなわち基本理念として、実空間と公共空間としてのサイバー空間とが融合したデジタル社会の安全・安心の確保、そしてその安全・安心をマルチステークホルダーで作り上げることを据えることとしたい。

２．２　政策課題

新組織がその果たすべき役割を全うするために解決すべき課題を、施策の的確な推進を実現するための「対処体制の強化」、サイバー空間に由来する越境性に対し実効的な取組を進めるための「国際連携・対応の強化」、実態を把握し、日々新たな技術・サービスが生み出され変化し続ける社会に対応するための「実態把握と社会変化への適応力の強化」、マルチステークホルダー・プロセスに基づく取組を進めるための「社会全体でつくる安全・安心」の４つに大別して整理する。

２．２．１　対処体制の強化

(1) デジタル社会全体の安全・安心を見据えた取組を行うことができる組織の確立

サイバー空間と実空間とが融合した新たな社会においては、犯行手口やその被害・影響がサイバー空間の中だけにとどまらず、脅威のレベルがこれまでとは次元の違うレベルまで高まる。このことに鑑み、新組織は、サイバー空間の安全・安心のみならず、既存の組織と連携し、実空間と公共空間としてのサイバー空間とが融合したデジタル社会全体の安全・安心を見据えた組織として確立することが必要である。

(2) 有為な人材層の拡充と機動的な活用のための環境実現

組織を実効的に機能させるためには、有為な人材をいかに集め、育成し、活躍させるかが鍵となることは言を俟たない。

一方、高度専門人材をはじめとする有為な人材は、地方においても重要な役割を担っており、単に新組織に人材を集中させることは適切ではない。

この状況に対処するためには、有為な人材層の拡充はもとより、その機動的な活用のための環境を実現する取組が必要である。

２．２．２　国際連携・対応の強化

(1) 海外治安機関等との強固な信頼関係の構築

サイバー空間の越境性を背景として、サイバー犯罪等の捜査に際しては海外に所在する情報の取得が必須となっているところ、捜査共助等の枠組みにより海外の捜査機関等を通じて海外所在のプロバイダ等が保有する情報の取得を行う国際照会が広く実

施されている。また、Emotet[33]やDouble VPN[34]のテイクダウン等に見られるように、諸外国では上記の捜査共助等を通じた国際捜査を進めた上で、各国の捜査機関等がそれぞれの捜査結果等を補完しあうことによりオペレーションの面での連携を行う国際共同オペレーションも進められている。

我が国では、サイバー犯罪条約を締結する等捜査共助に係る枠組みは一定程度整備が進む一方、捜査共助等を通じた国際照会の回答に長時間を要することなどにより国際捜査が十分に進展しないケースも多く存在するほか、継続的に国際捜査に携わる捜査主体が存在しないことなどにより国際共同オペレーションへの参画が低調な状況にある。

海外治安機関等との関係では、相手機関に協力を求める場面のみならず、日本側が相手機関側からの協力要請に応じることも含めてギブ・アンド・テイクの原則に留意して互恵的な関係を構築することが重要な鍵となる。また、組織と組織の間の継続的な関係構築のみならず、それぞれの組織に所属し捜査等に携わる実務者レベルでの信頼関係を構築することも同様に重要となる。上記のような状況を踏まえ、中長期的観点から、実務者レベルでの顔の見える関係の構築や、我が国警察の強みを生かした情報の収集・分析・提供等での地道な貢献を通じて海外治安機関等との強固な信頼関係を構築する取組が必要である。

(2) 関係国等と連携したサイバー空間の安全の確保

攻撃者優位とも言われるサイバー空間の環境改善に正面から取り組み、安全確保を図るためには、関係国等と連携した具体的な取組が必要である。

強固な信頼関係を構築した上で国際共同オペレーションに参画することは、国内外の犯罪インフラの壊滅、犯罪者集団の検挙、実態解明に資するものとなる。

加えて、国際共同オペレーションに加わり、継続的に検挙や実態解明を進めていくことで、攻撃者に日本への攻撃をためらわせる抑止効果も期待できること、また、捜査の結果として攻撃者の特定等に至ることができれば、我が国の国益の追求はもとより、重要な国際貢献ともなることにも留意すべきである。また、サイバー空間が、地政学的緊張を反映した国家間の競争の場の一部となっている観点を踏まえ、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である。

---

[33] コンピュータの利用者が送受信したメールの宛先、本文等の情報を窃取し、当該情報を基になりすましのメールを作成・送信することで感染を拡大させる機能を持つ不正プログラムであり、世界的に大きな被害をもたらした。

[34] 最大で四重のVPN接続を用いることで極めて高い秘匿性を提供すると宣伝されていたサービスであり、ランサムウェア攻撃やフィッシング等を行う者が所在地や身元を隠すために悪用されていた。

また、近年では、サイバー攻撃の多発や攻撃者優位とされる極めて厳しい情勢が、国際的なルール形成等の議論の背景となっているが、攻撃者の特定や実態解明において役割を果たすべき警察としても、「法の支配の貫徹」という我が国の理念が脅かされぬよう、これらの国際的なルール形成等の議論にも積極的に関与するとの観点を持つことが求められる。

２．２．３　実態把握と社会変化への適応力の強化

(1) 事案・情勢変化の早期把握

情報漏洩等の事実が公表されることによるレピュテーションリスクや捜査活動への協力により業務の早期復旧に支障が及ぶことなどへの懸念から、被害を受けた事業者等が警察への通報・相談をためらう傾向があるなど、現在も、被害の潜在化と、それに伴う実態把握の精度低下が生じているおそれがある。

ここ最近でも、スマートフォン決済サービスの不正振替、SMS 認証の不正な代行、暗号資産の匿名性を悪用したランサムウェア身代金の要求など、新技術・サービスを悪用した事例は枚挙にいとまがない。

次々と新技術・サービスが生み出され、情勢が時々刻々と変化する新たな社会において安全・安心のために適切な対策を講じるためには、事案の発生や情勢の変化を早期に把握するための取組が必要である。

(2) 実態解明と実効的な対策の推進

令和３年４月に中国共産党員の男を検挙するに至った JAXA 事案は、背景組織として中国人民解放軍第 61419 部隊が関与している可能性が高いことを解明したことに加え、警察から被害企業等に対し、速やかに不正プログラムへの感染可能性や有効な対応策について個別に情報提供を実施するなど、被害拡大防止につなげた事例である。また、令和３年７月には、中国政府を背景に持つ可能性が高いサイバー攻撃集団 APT40 によるサイバー攻撃に関して、悪意あるサイバー活動を断固非難する旨の外務報道官談話[35]が発出された。このようなパブリック・アトリビューション[36]によって、攻撃者を公表し、非難することでサイバー攻撃を抑止する取組の実績が着実に積み重なっているところであり、広範な関連情報を総合的に分析・評価し、国家の関与を明らかにするなど、実態解明と実効的な対策をさらに推進していくための取組が必要である。

---

[35] 中国政府を背景に持つ APT40 といわれるサイバー攻撃グループによるサイバー攻撃等について（https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html）

[36] アトリビューション（犯行主体やその手口、目的を特定する活動）により解明した攻撃者を公表し、非難することでサイバー攻撃を抑止する活動。

２．２．４　社会全体でつくる安全・安心

(1) 新技術・サービスの犯罪インフラ化の対策等

暗号資産の匿名性を悪用したランサムウェア身代金要求、SMS を介した配送状況の連絡に擬態したフィッシング等、新たな技術・サービスは時として犯罪者に悪用され、犯罪インフラとして機能している。

また、SMS 認証の不正な代行に見られるように、当初は安全と考えられ広く活用されるようになった技術が、制度の抜け穴を突いて悪用され、犯罪インフラとなる事態は、新たな技術・サービスが次々と生まれる社会ではさらに多発することが予想される。

制度設計、サービス設計、技術開発、研究等をそれぞれ担う者が協働し、人々に恩恵をもたらす新たな技術・サービスが犯罪インフラと化すことがないよう対策を進める必要がある。

(2) 地域全体で安全・安心をつくる土壌の育成

都道府県警察本部や数多くの警察署・交番等を持ち、地域社会と密着した活動を進めてきたことは警察の強みであるが、新たな社会の安全・安心を警察のみで担うことは到底不可能である。

一人一人が安全・安心の確保を自分事として意識し、一緒に安全・安心な社会をつくるという気運が不可欠であり、この様な土壌を育むための取組が必要である。

また、広報啓発等に際しては、知識の習得を目的としたリテラシーの視点だけでなく、セキュリティに係る習慣付け・意識付けを目指すアウェアネスや、知識を使いこなす能力の獲得を目指すコンピテンシーの視点を踏まえることも重要である。

３　具体的な施策

これまで情勢認識を示し、かかる情勢に対処するために新組織に求められる基本理念等を整理してきたところであるが、続いて、先に整理した政策課題を解決するため、サイバー局等において取り組むことが求められ、又は期待される施策の主なものを以下に例示することとしたい。

これらについては、従来の取組を継続的に推進するものや強化を図るべきもの、新組織立上げと同時又は速やかに取り組むことが求められるもの、新たな予算措置を必要とするもの、中長期的な検討を要するものなど多岐に渡るので、特に中長期的な検討・取組が必要となる個別施策については、一定期間を俯瞰したロードマップを作成するなどにより、計画的に推進することが必要不可欠である。

また、推進に当たっては、継続的な取組推進のための体制面、予算面等のリソース確保を進めることが重要である。

加えて、以下に挙げる施策は必ずしもサイバー部門のみで全てを実現できるものではなく、警察部内の他部門や内閣サイバーセキュリティセンターを始めとする関係省庁、産学の関係者等との連携が実現の鍵となることから、マルチステークホルダー・プロセスの考えの下で、関係者が一丸となって取り組むよう働きかけるという観点も不可欠である。

３．１　対処体制の強化

Ⅰ－１　デジタル社会全体の安全・安心を見据えた取組を行うことができる組織の確立

①　サイバー事案に係る分析高度化のための体制構築

令和４年度に設置されるサイバー局は、サイバー空間を通じて現れる身近な脅威から、高速通信網や技術革新を悪用する脅威まで、広範にわたるものに対処することが求められている。事案対応や政策立案の基礎となるのは情報であることから、特に情報の分析を高度化するための体制をサイバー局に構築し、以下の取組を進める。

○　実態解明から被害防止等対策までの広範な活用を念頭に置き、警察内のサイバー関連情報に加え、他機関や民間企業から提供される情報等多様な情報の分析を行う。

○　日々新たなリスクに直面・対処している事業者や、消費者からの声が集まる消費者団体等とは、ヒアリングを実施するなどにより連携を強化し、新たに顕在化したリスクの分析等を進める。

○　サプライチェーン等が複雑化・ブラックボックス化することによりサイバー攻撃等の影響範囲や発現箇所の想定が困難となっていることから、それらに対する分析評価を関係機関と連携しつつ進める。

②　警察内他部門等との連携体制構築

サイバー空間・実空間の両者に渡り隙間なく脅威に対処するためには、生活安全、刑事、交通、警備等他部門との間、あるいは警察庁と都道府県警察との間における実効的な連携体制を構築する必要があることから、以下の取組を進める。

○　令和４年度中に、警察庁サイバー局と生活安全、刑事、交通、警備局等他部門との間において、情報共有、政策立案に係る相互支援、技術的な助言・支援等を行う連携体制を構築する。

○　令和４年度中に、都道府県警察においても、新たな技術やサービスを悪用した犯罪、実空間とサイバー空間をまたがって行われる犯罪等に適切に対処するため、サイバー部門による他部門への技術支援、部門間の情報共有等を強化するなど連携強化を図る。

○　サイバー隊が成果を上げていくためには、都道府県警察との緊密な連携が不可欠となる。都道府県警察ごとの対処能力の差異を踏まえつつ、警察の対応に間隙が生じないような役割分担の整理を行うとともに、都道府県警察の対処能力の強化状況等も踏まえつつ、警察組織全体として最適な形となるよう、連携の在り方の不断の見直しを行う。

○　サイバー局と警察庁他部門、サイバー隊及び都道府県警察の役割分担について事業者等への適切な情報提供にも努める。

③　諸外国の体制、取組等に関する調査研究の推進

効果的・先制的に政策を立案・実行していく能力を維持・発展させていくためには、諸外国における先進的な取組事例や、組織改正動向等に学び、施策の見直しを随時図ることが必要であることから、諸外国の体制、取組等に関する調査研究を継続して推進する。

Ⅰ－２　有為な人材層の拡充と機動的な活用のための環境実現

①　優秀な人材の確保

サイバー局及びサイバー隊がその機能を十分に発揮するためには、有為かつ多様な人材を確保し、活用できることが不可欠であるため、以下の取組を継続して進める。

○　高度専門人材となる資質を特に期待できる情報分野に強い高等専門学校や大学等からの採用に努める。

○　人材の多様性を確保するため、解析以外の技術部門とともに技術職員の一括採用を進めるほか、外部人材の専門捜査員[37]への採用等を推進する。

②　高度専門人材・専門捜査員育成の充実・強化及び処遇改善

[37] 民間企業での経験や情報通信技術に関する高度な資格の保有を条件として中途採用・特別採用されたサイバー犯罪捜査官等、サイバー犯罪・サイバー攻撃への対処に高度な知見を有する捜査員。

確保した優秀な人材がその能力を遺憾なく発揮するためには、最新の知見等に触れる機会を設けるなど計画的に育成を図る必要があるほか、士気高く活躍できるよう処遇改善も合わせて進める必要があることから、以下の取組を進める。

○　引き続き、一般財団法人日本サイバー犯罪対策センター（JC3）や民間企業等への派遣、サイバー犯罪対策テクニカルアドバイザー[38]による捜査員への講習等の実施、高度な訓練施設を用いた民間トレーニングの活用等を推進する。

○　令和４年度中に、遠隔で高度な訓練環境等へのアクセスを可能とする人材育成プラットフォームを整備し、地方においても高度で実践的な教養を受講する機会を増やすほか、継続的に部内教養の内容充実を図る。

○　令和４年度中に、これまで別個で行われていた高度専門人材と専門捜査員等を対象としたサイバーセキュリティに係る全国競技大会について、両者混合のチームによる競技の新設等を検討するほか、引き続き相互の教養プログラムに参加させることなどにより、人的交流・知見共有等を促進し、捜査・解析の両者に精通した優秀な人材層の充実に取り組む。

○　極めて高度な専門技術を有する人材に対して、その能力に見合った活躍の場を与えるために、長期に亘り同一ポスト又は関連するポストを務め、高度な技術的知見を蓄積・活用できるキャリアパスの確立や、令和４年度中に整備する遠隔解析・相互支援を可能とする解析プラットフォームを活用した転勤回避等のインセンティブ付与を検討するなど、高度専門人材が活躍しやすい環境整備に努める。

③　警察職員全体の対処能力底上げ

全部門においてサイバーセキュリティへの理解・意識付け、デジタルを使いこなす能力等が必要とされる状況に鑑み、人材の裾野を広げるため、それら能力の修養を剣道・柔道等のように教養の根幹に位置付けるべき重要なもの[39]であると位置付け、重点分野であることを明確にし、以下の取組を進める。

○　自己研鑽を支援する方策として、令和３年度中に警察庁作成教養資料の都道府県警察への共有を進めるほか、令和４年度中に警察部内でのサイバーセキュリティ関連競技大会の拡充等を検討する。

○　令和４年度中に、人材育成計画の見直しを行い、サイバーセキュリティ等に係る修養の重要性を示すとともに、採用時や昇任時等節目ごとに設けた教養機会を有効

[38] 都道府県警察から任命を受け、サイバー犯罪捜査及び対策に係る必要な知識、技術に関する助言等を行う情報通信関連企業職員や大学教授等の専門家。

[39] デジタル庁から令和３年デジタルの日に関連して公表されたコンセプトによると、「個々人や組織はどのようにデジタル技術を活用していくとよいのか。その考え方を「道＝（デジ道（仮））」と見立て」、取り組んでいくという動きもある。

に活用するための教養内容の見直し、教養機会自体の拡大、初任科生を対象とした教養資料の整備等を検討する。

④　有為な人材の機動的な活用のための環境整備

全国に配置された有為な人材は、サイバー部門をはじめあらゆる部門の捜査に係る解析業務等を担ってきたところ、今後は、サイバー局及びサイバー隊の設置に伴う高度な分析・解析に携わるという側面での需要、サイバー部門自らが行う捜査に係る需要、他部門に対する技術支援の需要等が大幅に高まることが確実である。このような需要に対処するためには、有為な人材を機動的に活用するための環境を整備することが必要であることから、以下の取組を進める。

○　令和４年度中に、遠隔解析・相互支援を可能とする解析プラットフォームを整備するほか、引き続き資機材の性能向上や機能強化等に努める。

○　高度専門人材をより高度な解析に集中させるため、都道府県警察のサイバー部門における定型的な解析等を実施できる体制の構築・拡充を引き続き推進する。

３．２　国際連携・対応の強化

Ⅱ－１　海外治安機関等との強固な信頼関係の構築

①　海外治安機関等への職員の派遣・配置

海外治安機関等との信頼関係を構築するためには、職員を派遣し、顔の見える関係を構築することが不可欠であることから、以下の取組を進める。

○　令和４年度中に、欧州に海外連絡担当官（リエゾン）を派遣し、日常的な情報交換、対面での関係の構築等を推進する。

○　諸外国の例も踏まえつつ、海外派遣職員に係るキャリアパス（長期間配置、適切なポスト等）や海外治安機関等への職員派遣の拡大等も検討する。

②　海外治安機関職員等を招いた国際会議の主催や国際的な会合等への参加

海外治安機関等との信頼関係を構築するためには、定期的な会議等を通じて相互理解を深めることや、イベント等において存在感を発揮することなども有効であることから、以下の取組を進める。

○　引き続き国際的な民間イベント等にも参加し、警察の高度専門人材の高い技術力等を示すことで存在感を示し、海外治安機関等との関係構築の土壌作りを推進する。

○　令和４年度から海外治安機関職員等を招いた国際会議を主催するほか、引き続き他国主催の国際会議へ参加することなどを通じて、捜査・技術両面からの情報交換、担当者レベルでの相互理解、関係構築等を図る。

③　国際捜査共助等既存連携枠組の継続的推進

海外治安機関等との信頼関係構築には、個人間の顔の見える関係の構築だけでなく、国家間（組織間）の協力・互恵の積み重ねも有効であることから、以下の取組を進める。

○　引き続き、他国からの国際捜査共助に係る要請に対し、適切な対応を推進する。特にサイバー隊の設置に合わせて、従前は都道府県警察に対応を依拠してきたものに、国が直接関与することで、要請に一層迅速的確に対処することを通じて、国際的な信用向上にも努める。

○　引き続き、パブリック・アトリビューションの際に特に重要となる海外治安機関等との緊密な連携関係の維持・発展に努める。

Ⅱ－２　関係国等と連携したサイバー空間の安全確保

①　サイバー隊による戦略的な国際捜査の推進

サイバー空間の越境性を背景として、サイバー犯罪等の捜査に際しては国際捜査が不可欠であることから、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。特に、国際的なサイバー犯罪者集団や、複数国にまたがる犯罪インフラの壊滅等に係る国際共同オペレーションについて、従来から参画している諸外国の取組等を参考に、都道府県警察が収集した捜査関連情報や高度専門人材による分析結果等を活用した成果の提供等を足がかりにして、積極的に参画する。

②　国際ルール形成等国際的議論への積極的関与

攻撃者優位とも言われるサイバー空間の環境改善には、捜査により犯罪インフラの壊滅等を図るだけでなく、国際的議論を通じてサイバー空間における法の支配の推進等に取り組むことが必要である。引き続き、国家を背景としたサイバー攻撃等の脅威に係る情勢分析の結果や、捜査上支障となっている国際情勢等について、関係省庁等へ適切に情報提供することなどを通じ、サイバー犯罪に関する条約等既存の国際的枠組み等を活用し、条約の普遍化及び内容の充実化を推進する。

また、令和４年１月にオープンエンド・アドホック政府間専門家委員会第一回会合が開催される予定の国連における新条約策定に関する議論に十分関与する等、国際的議論に積極的に関与する。

３．３　実態把握と社会変化への適応力の強化

Ⅲ－１　事案・情勢変化の早期把握

①　警察への通報・相談促進に向けた気運の醸成

次々と新技術・サービスが生み出され、情勢が時々刻々と変化する新たな社会において安全・安心のために適切な対策を講じるためには、事案や情勢の変化を早期に把握することが必要である。そのためには、被害を受けた際に警察への通報・相談が行

われ、被害が潜在化しないことが不可欠である。しかし、現状は、レピュテーションリスクや捜査により業務の早期復旧に支障が及ぶことなどへの懸念から、被害企業からの警察への通報・相談が行われず、サイバー犯罪被害の多くが潜在化しているとも考えられている。

そこで、サイバーセキュリティ戦略において「サイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図る」[40]とされていることを踏まえ、警察として、引き続き被害通報を促進するための広報啓発に取り組むとともに、民間事業者とも連携して、通報・相談促進に向けた気運の醸成に取り組む。

② 警察への円滑な通報・相談を可能とする環境整備

警察への通報・相談を促進するには、広報啓発を行うだけでなく、通報・相談の障害となっている企業等の懸念や警察側の対応不備との指摘に対し、警察として通報・相談しやすい環境を整備することも不可欠であることから、以下の取組を進める。

○ レピュテーションリスクや捜査により業務の早期復旧に支障が及ぶことなどを懸念する企業等もあることから、令和４年度中に被害企業等に可能な限り配慮して捜査が実施されるよう、サイバー犯罪における初動捜査の在り方を検討する。

○ 通報・相談を受けた警察の対応が不十分であるとの指摘もあることから、Ⅰにおいて述べたとおり、令和４年度以降、警察職員全体のサイバーセキュリティに係るリテラシー底上げや部門間連携により適切な対応態勢を構築するとともに、より適切かつ円滑な対応を可能とするための相談対応の充実や官民連携の在り方について検討する。

○ 被害企業の担当者・経営者は、被害を受けた際に、警察への通報・相談に思いが至らないという指摘もあることから、平素から企業等の担当者との間でリスクコミュニケーションを図る方策を検討する。

③ サイバー事案に関する相談に係る分析の充実・高度化及び警察部内での早期伝達

情勢変化を早期かつ適切に把握するためには、通報・相談により得られた情報を１つ１つの点としてではなく、速やかに集約し、線あるいは面として分析することが必要であることから、以下の取組を進める。

○ 令和４年度以降、通報・相談により得られた情報について、Ⅰ－１において述べたサイバー局に設置される分析体制に全国から集約された捜査情報等と併せて俯瞰的な分析を行う。

[40] サイバーセキュリティ戦略（令和３年９月 28 日閣議決定)、19 頁。

○　警察署等－警察本部－警察庁という体系の中で、警察署等が把握した相談情報が警察本部・警察庁に迅速に共有され、分析に活用されるよう、情報伝達に係る運用を検討する。

④　事業者との共同対処の拡大・充実

通報・相談以外にも事案・情勢変化を把握するための方策も備える必要があるところ、企業の規模や業種を問わずサイバー事案の被害にあう可能性がある現状において、これまで以上に広範な事業者との関係を構築することや、従来の連携関係の強化を図ることが有効であることから、以下の取組を進める。

○　令和４年度以降、サイバー犯罪被害の潜在化防止や再発防止等を目的とした共同対処協定について、現在その大半を占める金融機関にとどまらず、中小企業を含む広範な業界の企業、商工会など地域の産業組織等とも締結が進むよう取り組むとともに、協定締結後においても、平素から顔の見える関係を構築するなど実効性の向上に取り組む。

○　令和４年度中に、警察と共にサイバー空間の安全・安心を確保する上で重要な役割を担っているセキュリティベンダー、脆弱性探索・悪用のリスクに直面するソフトウェア開発事業者、サイバー空間において欠かせないインフラの提供者であり、かつ、SASE（Secure Access Service Edge）[41]の進展等によりセキュリティの重要な担い手ともなっているクラウド提供事業者等との連携強化を図るため、より実践的な連携の在り方について検討する。

○　引き続き、事案発生時における事業者との緊密な連携にも努める。

Ⅲ－２　実態解明と実効的な対策の推進

①　サイバー事案に係る捜査関連情報等に対する分析の充実・高度化及び厳正な取締りの推進

通報・相談等を通じて事案を把握した場合は、被疑者の検挙だけでなく、犯行手口等の実態解明や被害の拡大防止等を図る観点も不可欠であることから、以下の取組を進める。

○　引き続き、一つの事案のみに着目するのではなく、その他の広範な関連情報を総合的に分析・評価し、サイバー攻撃において特定の攻撃グループ、国家機関等が関与していることを明らかにするなど、より広い範囲での実態解明を進めるとともに、サイバー事案の厳正な取締りを推し進め、解明された情報の適切な公表に取り組む。

[41] セキュリティ機能及びネットワーク機能を単一のクラウドサービスに統合する概念。

○　引き続き、被害の拡大防止、犯罪インフラ対策等も視野に入れ、より広範な視点から捜査関連情報等に対する分析に取り組む。特に、ランサムウェア被害については、多業種にわたって甚大な影響を及ぼしていることから、関係行政機関、団体等が連携してサイバー事案の分析を行い、被害の再発・拡大防止に向けた取組を推進する。

② アトリビューションのための分析・解析の高度化・効率化

特定のグループや国家機関等が関与するサイバー攻撃等、被疑者の検挙が著しく困難である事案に対しても、アトリビューションを通じた実態解明と対策の推進は有効であることから、以下の取組を進める。

○　引き続き、マルウェアの多様化・耐解析機能の実装等に対処していくため、機械学習の活用等を進めて解析態勢を強化し、解析の効率化・高度化を図る。

○　アトリビューションに不可欠である IoC（Indicators of Compromise）[42]等の大量データの総合的な分析、データ間の関連性検証等に多くの人材を投入しているところ、この種の作業を効率的に推進し、より高度な分析・判断等に人材投入を行うことが可能となるよう、令和４年度以降、AI の導入を検討する。

なお、AI の活用は、「人間中心の AI 社会原則」（平成 31 年３月 29 日統合イノベーション戦略推進会議決定）等を踏まえ、適切な検討・対応の下で行われるべきである。

○　通報・相談の促進により潜在化していた被害が多数顕在化した際に適切に対応するため、IoC の収集を効率的に行う必要があるところ、その方法について、警察への円滑な通報・相談を可能とする環境整備と併せて検討を進める。

③ インターネット上の脅威情報等の収集及び分析の高度化

インターネット上から実態解明に資する情報を収集することや、違法有害情報に対処することも、被害の予防・拡大防止対策として有効であることから、以下の取組を進める。

○　引き続き、児童ポルノや規制薬物広告、自殺誘引等の違法・有害情報に厳正に対処するため、インターネット・ホットラインセンターからの通報を端緒情報として、事件化や削除依頼等を積極的に推進する。

○　令和４年度に、先端技術を活用したサイバー空間における違法・有害情報の探索・分析に係る実証実験事業を実施し、同分野への AI の導入を検討する。

○　令和５年度に更新を検討しているインターネット上の脅威情報を収集・分析するリアルタイム検知ネットワークシステムについて、能動的に犯罪の端緒等を検知・

[42] 侵害指標。IP アドレスやハッシュ値等サイバー攻撃の痕跡となる情報をいう。

発見し、犯罪捜査及びアトリビューションを通じた実態解明と対策に資する情報を提供するための機能増強を図る。

３．４　社会全体でつくる安全・安心

Ⅳ－１　新技術・サービスの犯罪インフラ化の対策等

①　サービス提供事業者等への情報提供・働きかけ等

新技術・サービスが犯罪インフラとして悪用されることを防ぐため、個別具体のサービスに応じて、サービス提供事業者に対し、悪用の危険性や被害実態等の情報提供を行い、必要な対応がとられるよう働きかけを進める、関係団体等と連携した被害実態の把握と有効な対策の在り方について検討する等の対応が必要である。

また、誰もがインターネットを利用するようになり、インターネットバンキングやキャッシュレス決済サービスの悪用により経済的損失を受ける事案やインターネット上の誹謗中傷により精神的苦痛を受ける事案等も多く発生しており、適切な対策が求められている。

特に、現在も多くの被害が確認されている以下の事例について、引き続き対応の強化を図る。

○　インターネットバンキング及びキャッシュレス決済サービスをめぐるサイバー犯罪の対策については、金融機関・資金移動業者等への犯行手口に基づく注意喚起の実施、不正な送金先口座の凍結検討依頼等を進める。

○　SMS 認証の不正な代行については、被害実態について関連する業界団体等との情報共有を進めるとともに、SMS 機能付きデータ SIM 契約時の本人確認義務付けの必要性についても検討を進める。

○　インターネット上の誹謗中傷に係る相談に際し、その内容に応じて、関係する部署が連携して対応し、指導・助言、法務局人権擁護担当、違法・有害情報相談センター等の専門機関の教示等、相談者の不安等を解消するために必要な措置を講じるほか、刑罰法令に触れる行為が認められる場合には、捜査機関として適切に事件に対処する。

○　キャッシュレス決済サービスの普及に伴い、様々なサービスにクレジットカード情報がひも付けられることにより、クレジットカード不正利用の被害額が増加傾向にあることから[43]、e コマース（電子商取引、EC）に関連するクレジットカードの不正利用事案に関し、関係団体等と連携して被害実態の把握に努めるほか、被害実態を踏まえた有効な対策の在り方について検討を進める。

[43] クレジットカード不正利用被害の発生状況（令和３年９月一般社団法人日本クレジット協会）

○　知的財産に関しては、政府全体の議論を踏まえつつ、現在捜査の妨げとなっている様々な課題について検討・対策を進め、取締りや被害防止に取り組みつつ、内閣府等関係機関との連携に努める。

②　被害拡大防止に向けた関連団体への働きかけ

サービスの連携が進む中においては、利用者にサービス提供がなされる際に利用されるインフラ・プラットフォーム的なサービスも犯罪インフラとして悪用されるおそれがあることから、利用者に直接サービス提供を行う事業者と同様に、それら事業者に対しても、サービス等の悪用の危険性や被害実態等の情報提供を行い、サービスの見直しやトレーサビリティの確保等必要な対応がとられるよう働きかけを進める必要がある。

特に、現在も多くの被害が確認されている以下の事例について、引き続き対応の強化を図る。

○　フィッシングサイト等については、JC3 等の官民連携体制も活用して警察が把握した情報を、ウイルス対策ソフト事業者等に提供する。

また、特にショートメッセージによってフィッシングサイトへ誘導する手口であるスミッシングについては、フィッシングサイトに誘導するショートメッセージ自体の遮断に向けて関係事業者に働き掛けを進めるとともに、JC3 とも連携して、関係事業者の取組に必要となる捜査関連情報等の積極的な提供を検討する。

○　暗号資産による犯罪収益の移転[44]については、インターネットバンキングに係る不正送金事犯等の対策として犯罪収益の送金先に係る銀行口座の凍結措置が講じられていることを踏まえ、犯罪収益の送金先の暗号資産アカウントの凍結措置が講じられるよう、金融庁とも連携して業界団体に働きかけを行うほか、ランサムウェア等による被害の抑止に向けて事業者等と連携した広報啓発を進める。

③　JC3、セキュリティベンダー、研究機関等との連携強化

現在も JC3 やセキュリティベンダー、研究機関等からインターネットバンキングに係る不正送金事犯の犯行の分業構造の実態解明といった各主体の強みを活かした分析の結果や、高度な技術情報の提供等の協力を得ているところ、令和４年度中に、警察からの情報提供拡大を含めた情報共有の更なる推進に必要なルール整備等連携強化のための方策検討を進める。

④　判明した犯罪インフラのテイクダウン

[44] 令和３年上半期におけるサイバー空間をめぐる脅威の情勢等（令和３年９月９日警察庁）５頁によると、ランサムウェアに関し要求された金銭支払い方法の 90%を暗号資産が占める。

引き続き、サイバー攻撃事案で使用された不正プログラムの解析等を通じて把握したＣ２サーバ（Command and Control server）[45]等判明した犯罪インフラについて、管理者等への情報提供・対応依頼を通じて確実にテイクダウンが行われるよう取り組む。

Ⅳ－２　地域全体で安全・安心をつくる土壌の育成

警察に限らず、多様な主体が地域におけるサイバーセキュリティ向上に係る枠組みを構築し、様々な取組を進めているところ、社会全体としてより効率的・効果的に施策を講じていくため、それら既存枠組みとの連携強化に取り組む。

①　学校教育と連携したセキュリティ人材の育成

特に地方・中小企業においてセキュリティ人材の不足が顕著であるとの指摘もあるところ、その育成に警察としても貢献し、社会全体の防御力の向上を図るため、警察のサイバーセキュリティに関する知見を活用し、大学や高等専門学校等に対する講師派遣、出張講義等の取組を引き続き推進する。

②　サイバー防犯ボランティアの拡大・活性化

サイバー防犯ボランティアは、これまでも子供や高齢者等への教育・啓発活動、サイバーパトロールによる環境浄化等の面から、地域における安全・安心に貢献してきたが、全国民がサイバー空間に参画する中で、ニーズや期待が急速に高まっている[46]。この状況に対応するため、以下の取組を進める。

○　引き続き、関係省庁等と連携した活動事例の紹介等を通じ、サイバー防犯ボランティアのさらなる拡大・活性化に取り組む。

○　次世代を担う子供に対しては、小中学校とサイバー防犯ボランティアとの連携強化を図るなど、関係省庁が連携してサイバーセキュリティに関する注意事項等の啓発等に取り組む。

○　引き続き、これまで捜査員への講習や、捜査・対策等への助言を担ってきたサイバー犯罪対策テクニカルアドバイザーについて、サイバー防犯ボランティアに対する教養の場を構築するなど、活動参加者の専門性の向上等インセンティブを付与し、活性化を図る。

③　地域に根ざした各主体の防犯活動との連携

特に中小企業等においてサイバー空間の脅威に対して十分な対応ができていない実態が指摘される中、サイバーセキュリティの向上に向けて地域に根ざした防犯活動を

[45] 制御の中心として、不正プログラムに感染した端末に指令を送り動作させるなどするサーバのこと。

[46] サイバーセキュリティ戦略（令和３年９月 28 日閣議決定）18 頁において「国民一人一人の自主的な対策を促進し、サイバー犯罪の被害を防止するため、サイバー防犯に係るボランティア等の関係機関・団体と連携し、広報啓発等を推進する」とされている。

行っているサイバー保険を取り扱う損害保険会社等と連携し、引き続き、警察としても中小企業等に対する広報啓発活動を推進する。

④　官民連携に係る取組の継続的推進

サイバーテロ対策協議会、サイバーインテリジェンス情報共有ネットワーク等を通じた脅威情報の提供や助言、事案発生を想定した共同対処訓練の実施やサイバー攻撃に関する情報の共有、未知の不正プログラム、不正接続先等の情報の共有等官民連携に係る取組を引き続き推進する。

おわりに

令和３年度サイバーセキュリティ政策会議では「サイバー局等新組織において取り組む政策パッケージ」をテーマとして幅広く議論を行い、本報告書に取りまとめた。

本報告書では、デジタル化や、５Ｇ・衛星コンステレーション等の新たな技術・インフラの整備・活用が進む中、社会は「サイバー空間の公共空間化」という段階からさらに歩を進め、「実空間と公共空間としてのサイバー空間とが融合した社会」が現実となりつつあること、また、そのことにより恩恵だけでなく、新たなリスクが顕在化しつつあることを示した。

その上で、「世界一安全な日本」というかけがえのない社会の財産を育み、守り抜くことが警察組織全体の果たすべき役割であるという原点を再確認するとともに、警察庁サイバー局及びサイバー隊は、警察の既存部門はもとより、多様な主体とも手を携え、「実空間と公共空間としてのサイバー空間とが融合したデジタル社会の安全・安心の確保　～マルチステークホルダーで作り上げる安全・安心～」を実現するための中心的な役割を果たすことが求められていることを明確にした。

また、この役割を全うする上で解決すべき課題を、施策の的確な推進を実現するための「対処体制の強化」、サイバー空間に由来する越境性に対し実効的な取組を進めるための「国際連携・対応の強化」、実態を把握し、日々新たな技術・サービスが生み出され変化し続ける社会に対応するための「実態把握と社会変化への適応力の強化」、マルチステークホルダー・プロセスに基づく取組を進めるための「社会全体でつくる安全・安心」の４つに大別して整理し、それぞれの課題を解決するために取り組むべき施策を示した。

「実空間と公共空間としてのサイバー空間とが融合した社会」において、サイバー局及びサイバー隊は、今後も日本が世界一安全な国であるために必要不可欠な存在として重責を担うこととなる。同時に、取り上げた施策は、必ずしも警察のサイバー部門のみで全てを実現できるものではなく、マルチステークホルダー・プロセスの考えの下、警察部内の他部門や産学官の関係機関等、関係者と一丸となって取り組むという視点も忘れてはならない。

本報告書の提案が着実に実行され、サイバー局及びサイバー隊が真に実効性ある組織として確立し、その役割を果たすことで、今後到来する新たな社会が安全なものとなることはもとより、国民が安心して生活できるデジタル社会の実現につながることを強く期待したい。

また、新組織が始動し、具体的な取組が進められる中、今後も様々な課題に直面することが予想されるが、まさにマルチステークホルダーが結集する場であるサイバーセキュリティ政策会議としても、引き続き課題解決に向けた検討にコミットしていく所存である。

報告書を受けて

社会のデジタル化の進展により、今やサイバー空間は公共空間へと変貌を遂げつつあるが、これに伴い、サイバー事案が発生した際の被害や影響範囲が更に拡大することが懸念される。このような情勢においては、いわば「オールジャパン」でしっかりと対策を講じることが必要であり、警察には、その中心的な役割が求められている。

こうした情勢を踏まえ、警察庁では、令和４年度に、警察庁にサイバー局を設置するとともに、重大サイバー事案の捜査等を行うサイバー隊を関東管区警察局に設置する検討を進めている。これにより、サイバー事案の捜査、実態解明及び対策の一元化が実現するとともに、諸外国の捜査機関と信頼関係を構築し、国際共同オペレーションに参画することで、国境を越えるサイバー事案にもしっかりと対処できるようにしていく所存である。

このような局の改編を含む大規模な組織改正は、平成６年の生活安全局設置以来のものとなり、警察庁の最重要課題と位置付けて取り組んでいるところであるが、新組織を真に実効性ある組織として確立するためには、顕在化しつつあるリスク等を幅広く洗い出した上で、掲げるべき理念や具体的な取組について検討する必要があった。

令和３年度サイバーセキュリティ政策会議においては「サイバー局等新組織において取り組む政策パッケージ」をテーマとして、令和３年９月以降、幅広い視座から議論を重ね、報告書として取りまとめていただいた。

実空間と公共空間としてのサイバー空間が融合する新たな社会において、サイバー局及びサイバー隊が中心的存在として、国民の安全で安心な暮らしを守る重責を担うべきという指摘には、警察のサイバー部門一同、身の引き締まる思いである。

また、デジタル社会で顕在化しつつあるリスクに対しては、政府あるいは社会全体として対応すべきものもあるが、警察として取り組めることには率先して対策を講じるなど、しっかりと取り組んでまいりたい。

新組織の設置により、警察のサイバー部門としての本格的な取組はようやく緒に就くところとなるが、提言いただいた理念がサイバー部門のみならず警察全体、さらには産学官の関係者とも共有され、具体的な取組を通じて「世界一安全な日本」のさらなる発展に結実するよう、多様な主体と手を携えて進んでまいりたい。

警察庁長官官房サイバーセキュリティ・情報化審議官