サイバーセキュリティ戦略

令和７年 12 月 23 日

この戦略は、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 12 条第５項において準用する同条第４項の規定に基づき、国会に報告するものである。

目次

Ⅰ. 策定の趣旨・背景

我が国でインターネットの商用利用が開始されてから 30 年余りが経過し、デジタル技術は目覚ましい進展と普及を遂げ、サイバー空間は、我々の社会経済に欠かせない基盤となった。世界のあらゆる場所から、多様なサービスや情報に対し、低廉なコストでのアクセスが可能となり、我々に多くの利便をもたらしている。サイバー空間が、これまで以上に実空間と密接に融合するとともに、もう一つの現実空間とも言うべき状況となる中、AI や量子技術等の先端技術が、デジタルサービスや産業に大きなインパクトを与えようとしている。

一方、サイバー空間では、相対的に露見するリスクが低く攻撃者側が優位にあるサイバー攻撃の脅威も急速に拡大している。この脅威は、今日の複雑な国際情勢や我が国が置かれている安全保障環境の文脈においても、大きな懸念となっている。

自由、民主主義、基本的人権の尊重、法の支配といった普遍的価値に基づく国際秩序は、戦後 80 年を迎えた今、普遍的価値やそれに基づく政治・経済体制を共有しない国家の勢力拡大や、力による一方的な現状変更及びその試みによって、これまで以上に深刻な危機にさらされている。

その影響はサイバー空間にまで及んでおり、サイバー攻撃による重要インフラの機能停止、他国の選挙への干渉、機微情報の窃取等は、国家を背景とした形でも、平素から行われている状況にある。

さらに、武力攻撃の前から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行われている。国際情勢が緊迫化し安全保障環境の厳しさが増す中、サイバー攻撃が国民生活・経済活動に深刻かつ致命的な被害を生じさせるリスクは、今後も一層高まっていくと考えられる。

我々は、サイバー空間のもたらす価値を十二分に享受するために、こうしたリスクに適切に対処していかなくてはならない。

我が国のサイバーセキュリティ政策は、能動的サイバー防御等の法制化等により、大きな転換点を迎えることとなった。

「国家安全保障戦略」（2022 年 12 月 16 日国家安全保障会議決定及び閣議決定）に基づき、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、法制度の整備等について検討するため、2024 年６月に「サイバー安全保障分野での対応能力の向上に向けた有識者会議」が立ち上げられた。

同年 11 月に取りまとめられた提言を踏まえ、能動的サイバー防御を導入可能とする、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。以下「サイバー対処能力強化法」という。）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（令和７年法律第 43 号。サイバー対処能力強化法とあわせて以下「サイバー対処能力強化法等」という。）が、2025 年５月に成立した。

また、同年７月には、サイバー対処能力強化法等の一部施行に伴い、サイバーセキュリティ戦略本部（以下「戦略本部」という。）について、内閣総理大臣を本部長とし、全大臣で構成するなどの改組により、新たな体制となった。あわせて、内閣官房に、サイバー安全保

障も含め、官民を通じたサイバーセキュリティの確保に関する司令塔として、「国家サイバー統括室」が発足した。

この新たな体制の下、我が国のサイバーセキュリティ確保に向けた対応も新たなフェーズに入ることとなった。広く国民・関係者の理解と協力を得て、官民連携・国際連携の下、我が国のサイバーセキュリティ対策を一体的に推進していくためには、我が国のサイバーセキュリティに係る諸施策の目標や実施方針を取りまとめ、新たなサイバーセキュリティ戦略として内外に示していくことが必要である。

サイバーセキュリティ基本法（平成 26 年法律第 104 号。以下「基本法」という。）に基づくサイバーセキュリティ戦略は、2015 年以来、おおむね３年おきに策定されてきた。今回のサイバーセキュリティ戦略においては、「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項[1]」に盛り込まれた施策や「国家安全保障戦略」及びサイバー対処能力強化法等に基づく取組を含め、サイバー空間を巡る脅威に対応するために行う様々な取組を一体的に推進するため、より中長期的な視点から、今後５年の期間を念頭に実施すべき諸施策の目標や実施方針を示す。

なお、サイバー対処能力強化法に規定された関係施策は、同法で閣議決定及び公表することとなっている基本方針に基づき、本戦略に基づく施策と相まって一体的・効果的かつ適正に実施する。

[1] 2025 年５月 29 日に開催された戦略本部において、「サイバーセキュリティ戦略」（2021 年９月 28 日閣議決定。特に「サイバーセキュリティ 2024」（2024 年７月 10 日サイバーセキュリティ戦略本部決定）における「特に強力に取り組む施策」）及び「サイバー安全保障分野での対応能力の向上に向けた有識者会議」で取りまとめられた提言等を踏まえ、サイバー対処能力強化法等の施行前の制度下において、喫緊に取り組むべき施策の方向性を取りまとめた。

II. 本戦略における基本的な考え方

１．　確保すべきサイバー空間の在り方及び基本原則

我が国はこれまで、サイバー空間が経済社会の持続的な発展の基盤であり、自由主義、民主主義、文化発展を支える基盤でもあることに鑑みて、基本法に掲げた目的[2]に資するべく「自由、公正かつ安全なサイバー空間」の確保を目指してきた。

そして、その実現のため、サイバーセキュリティに関する施策の立案及び実施に当たって従うべき基本原則として、「５つの原則」（「情報の自由な流通の確保[3]」、「法の支配[4]」、「開放性[5]」、「自律性[6]」、「多様な主体の連携[7]」）を掲げてきた。

自由、民主主義、基本的人権の尊重、法の支配といった普遍的価値に基づく国際秩序が深刻な危機にさらされている中で、サイバー空間が「自由、公正かつ安全な空間」であることや、「５つの原則」を施策の立案・実施の基本原則とすることの重要性を改めて確認する[8]。

他方、サイバー脅威が我が国の国民生活・経済活動、ひいては国家安全保障に深刻な影響を及ぼすおそれが高まる中、「５つの原則」に基づく施策を今日の情勢に適応させ、「自由、公正かつ安全なサイバー空間」を確保するために、国が積極的な役割を発揮すべき場面が、これまで以上に広がっている。

例えば、純然たる平時でも有事でもない幅広い状況であるグレーゾーンが拡大しているサイバー空間において、巧妙化・高度化を遂げる組織的なサイバー攻撃を、初期段階から把握し、被害の防止につなげるためには、官民連携・国際連携の下、情報の収集・分析、積極的な提供や発信、サイバー対処能力強化法等に基づく措置を含む能動的な防御・抑止等に取

---

2 「この法律は、インターネットその他の高度情報通信ネットワークの整備及びデジタル社会形成基本法（令和三年法律第三十五号）第二条に規定する情報通信技術（以下「情報通信技術」という。）の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、同法と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする」（基本法第１条）。

3 サイバー空間が創意工夫の場として持続的に発展していくためには、発信した情報がその途中で不当に検閲されず、また、不正に改変されずに、意図した受信者へ届く世界が作られ、維持されるべきであること。このことは、我が国の推進する「信頼性のある自由なデータ流通」の実現にとっても、必要となるものである。

4 サイバー空間と実空間の一体化が進展する中、自由主義、民主主義等を支える基盤として発展してきたサイバー空間においても、実空間と同様に、法の支配が貫徹されるべきであること。また、同様に、サイバー空間においては、国連憲章を始めとした既存の国際法が適用されることを前提として、平和を脅かすような行為やそれらを支援する活動は許されるべきではないことも明確にされるべきであること。

5 サイバー空間が新たな価値を生み出す空間として持続的に発展していくためには、多種多様なアイディアや知識が結びつく可能性を制限することなく、全ての主体に開かれたものであるべきであること。また、サイバー空間が一部の主体に占有されることがあってはならないという立場を堅持していくこと。これには、全ての主体が平等な機会を与えられるという考え方も含まれる。

6 サイバー空間は多様な主体の自律的な取組により発展を遂げてきたものであり、サイバー空間が秩序と創造性が共存する空間として持続的に発展していくためには、国家が秩序維持の役割を全て担うことは不適切であり、不可能であること。サイバー空間の秩序維持に当たっては、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により、社会全体としてのレジリエンスを高め、悪意ある主体の行動を抑止し対応することも重要であり、これを促進していくこと。

7 サイバー空間は、国、地方公共団体、重要インフラ事業者、サイバー関連事業者その他の事業者、教育研究機関及び個人等の多様な主体が活動することにより構築される多次元的な世界である。こうしたサイバー空間が持続的に発展していくためには、これら全ての主体が自覚的にそれぞれの役割や責務を果たすことが必要である。そのためには、個々の努力にとどまらず、連携・協働することが求められる。国は、連携・協働を促す役割を担うとともに、国際情勢の変化を踏まえ、価値観を共有する他国との連携や国際社会との協調をこれまで以上に推進していくこと。

8 他の先進民主主義国と共に、我が国が、自由、民主主義、基本的人権の尊重、法の支配といった普遍的価値をこれからも擁護すべきことに鑑みれば、施策の立案及び実施の基本原則として「情報の自由な流通の確保」、「法の支配」、「開放性」は引き続き重要であり、また、多様な主体で形成されるサイバー空間の安全確保のため、各主体の自律的な取組と多様な主体の連携が必要不可欠である。

り組んでいかなければならない。これらの取組には、国でなければできないものや、国が様々な主体と積極的に連携することで大きな効果をもたらすものが多く存在する。

そこで、我が国は、「５つの原則」を、引き続き施策の立案及び実施に当たって従うべき基本原則として堅持した上で、国が、これまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間を巡る情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保していくことを明確化する。

以下に示すような、我が国のサイバー空間を取り巻く現状を踏まえれば、こうした国の積極的な対応は、現下の厳しいサイバー攻撃に脅かされている「自由、公正かつ安全なサイバー空間」や「５つの原則」（「法の支配」等）を守るとともに、「自律性」、「多様な主体の連携」といった原則に基づく、幅広い主体によるサイバーセキュリティ確保に向けた取組の支援・強化に資するものである。

２．　サイバー空間を取り巻く情勢認識及び今後の見通し

（１）　厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大

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、近年、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。我が国においても、国立研究開発法人情報通信研究機構（NICT）が観測したサイバー攻撃関連通信数は増加傾向にあり、外国国家の関与が疑われる組織化・洗練化されたサイバー攻撃が顕在化するなど、質・量の両面でサイバー攻撃の脅威は増大し、国民生活や経済活動の基盤、ひいては国家及び国民の安全に深刻・致命的な被害を生じさせるおそれが現実のものとなっている。

我が国を取り巻く安全保障環境において特に注目すべき国・地域も、サイバー攻撃の国家的な利用を行っているとみられている。ロシアはサイバー攻撃を軍事的・政治的目的達成のために利用しているとみられ、2022 年のウクライナ侵略前に、同国の政府機関や重要インフラ事業者等の情報システム・ネットワークへの攻撃を行っていたとされている。これは、サイバー攻撃がその後の武力攻撃等を見据えた前段階のものとして行われる可能性があることを示唆している。中国は、政府機関や重要インフラ事業者、先端技術保有企業等の情報窃取のためにサイバー攻撃を行っているとみられ、最近では、同国が支援する「SaltTyphoon」が、世界中の電気通信事業者、政府機関等の情報システム・ネットワークを標的としていることが明らかとなってきている。また、同国を背景とすると指摘される「VoltTyphoon」が、Living Off The Land 戦術（システム内寄生戦術）[9]を用いてグアム等の米軍・政府機関や重要インフラ事業者の情報システム・ネットワークに長期間侵入したとされる事例にみられるように、同国は有事を見据え、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キャンペーン[10]を行っているという評価も出てきている。さらに、北朝鮮は、暗号資産の窃取や、外国に派遣した IT 労働者が身分を偽

[9] システムへの侵入後、システム内に組み込まれている正規の管理ツール、機能等を用いて、認証情報の窃取、システム情報の収集等の活動を行うことで、検知を難しくするサイバー攻撃の手法。
[10] 一定期間内において特定の主体が国・重要インフラ等の特定の組織・分野に対して特定の攻撃手法・攻撃インフラを用いて繰り返し行うサイバー攻撃活動。

って仕事を受注すること等を通じて、不法な資金の調達を図っており、こうした収入が核・ミサイル開発に利用されていることや、これらIT労働者が情報窃取等に関与している可能性が指摘されている[11]。また、サイバー攻撃を通じた軍事機密情報の窃取や他国の重要インフラへのサイバー攻撃能力の開発等も行っているとされている。こうした状況を通じて、サイバー攻撃に対しては、有事の可能性も念頭に置き、危機感を持って対応する必要があるとの認識が広まりつつある。

我が国においても、2019 年以降、中国の関与が疑われるサイバー攻撃グループ「MirrorFace」が、日本の安全保障や先端技術に係る情報窃取を目的としたサイバー攻撃キャンペーンを実行している[12]。2024 年５月には、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」によって、我が国の暗号資産関連事業者から約 482 億円相当の暗号資産が窃取された[13][14]。

そのほか、名古屋港を業務停止に陥らせたランサムウェア攻撃（2023 年）や、機微情報の窃取を目的としたとみられる、内閣サイバーセキュリティセンター（NISC）への攻撃（2023 年）、国立研究開発法人宇宙航空研究開発機構（JAXA）への攻撃（2021～2024 年）が発生している。

このように、政府機関や重要インフラ事業者等をターゲットにする、国家を背景とするものを始めとした巧妙化・高度化されたサイバー攻撃[15]は、我が国にとっても現に直面する安全保障上の脅威となっている。

（２） 社会全体のデジタル化の進展とサイバー脅威の増大

オンラインサービスやテレワークを結果的に後押しすることとなったコロナ禍等を通じて、IoT やクラウドサービス等の活用を始め、我が国の社会全体の DX（デジタル・トランスフォーメーション）化は大きく進展した。

その結果、我が国の産業・サービスの効率性や利便性が大きく向上した一方、サプライチェーンの広がりや複雑化も背景に、個人・中小企業を含め、あらゆる主体がサイバー攻撃の標的となるリスクが高まっている。直接的な被害にとどまらず、サプライチェーンの停止、漏えい情報の拡散、IoT 機器の乗っ取り等により、更なる深刻な攻撃や被害の拡大に発展するおそれがある[16]。

---

11 日米韓「北朝鮮 IT 労働者に関する共同声明」及び「北朝鮮 IT 労働者に関する企業等に対する注意喚起」の公表（2025 年８月 27 日警察庁、外務省、財務省、経済産業省）

12 「MirrorFace によるサイバー攻撃について（注意喚起）」（2025 年１月８日警察庁、内閣サイバーセキュリティセンター）

13 「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について」（2024 年 12 月 24 日警察庁）

14 2025 年 10 月に公表された多国間制裁監視チーム（MSMT）第２回報告書では、北朝鮮は、2024 年は約 11 億９千万米ドル相当、2025 年は９月までに約 16 億５千万米ドル相当の暗号資産を窃取しており、2024 年の北朝鮮の外貨収入の大半は暗号資産窃取と露への武器販売が占めている、また、北朝鮮は、窃取した暗号資産を核・ミサイル開発計画の資金とするために、第三国に所在する非北朝鮮籍の協力者を利用し、資金を洗浄していると言及している。

15 国家を背景とするサイバー攻撃としては、脚注９で述べた Living Off The Land 戦術（システム内寄生戦術）のような検知を難しくするサイバー攻撃の手法も確認されている。

16 例えば、企業の事業活動の停止・漏えい情報の拡散の例としては、2024 年、出版事業等を行う大手企業がランサムウェアを含む大規模サイバー攻撃を受け、Web サービス等が停止したほか、個人情報や企業情報が漏えいし、SNS 等を通じて拡散される二次被害も発生した。また、委託先・サプライチェーンへの攻撃と業務停止の例としては、2022 年に大手自動車メーカーの取引先がサイバー攻撃（ランサムウェア）を受け、一部のサーバとコンピュータ端末のデータが暗号化され、同メーカーの国内全工場が一時停止したほか、同年、病院が、委託先の給食事業者を経由したサイバー攻撃を受け、通常診療の一時停止を余儀なくされた。大規模な DDoS 攻撃の事例としては、2024 年から 2025 年の年末年始にかけて、航空事業者、金融機関、通信事業者等が相次いで DDoS 攻撃を受け、サービス一時停止等の被害を受けた。

また、今日のサイバー攻撃では、攻撃の実行者が必ずしも技術的な専門知識を有する必要がなくなるなど、攻撃者の裾野の広がりが見られる。ランサムウェアの開発・運営を行う者が、攻撃の実行者にランサムウェア等を提供し、その見返りとして身代金の一部を受け取る形態（RaaS：Ransomware as a Service）が確認されている。標的企業のネットワークに侵入するための認証情報等を売買する者が存在するように、複数の者が役割を分担してサイバー攻撃を成り立たせている場合もある。

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、経済的な目的を含め、様々な動機に基づくサイバー攻撃が国民生活や企業活動、社会経済、ひいては国家安全保障に与える影響も、深刻さを増していくものと考えられる。また、サイバー犯罪の巧妙化等の新たな脅威にも直面しており、サイバー空間における脅威は質・量両面で増大していくと考えられる。

（３） AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

生成 AI を始めとする AI の急速な発展は、今後、産業や国民生活の利便性や効率性を大きく向上させる潜在力を持つ一方、サイバー犯罪の巧妙化等新たな脅威を生み、社会での活用・普及に伴い、AI に対する攻撃や 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。

また、量子コンピュータや、量子通信の社会的な実用化が、現実的なものとなりつつある[17]中、その進展に伴い、現在広く使われている公開鍵暗号の安全性の低下・危殆化が懸念されるなど、多岐にわたる課題への対応が必要になっている。

こうした新たな技術革新がサイバーセキュリティや安全保障等にもたらす効果・影響に対して、適時的確な対応を行っていかなければならない。

さらに、こうした技術革新が、サイバーセキュリティ分野にもたらす利便を最大限享受しつつ、そのリスクに的確に対応するためには、サイバーセキュリティ人材・技術の育成・確保に向けた対応は焦眉の急である。

３．　サイバー空間を取り巻く課題認識及び施策の方向性

我が国が直面している上述のような現状を踏まえると、サイバー空間を取り巻く課題としては、以下の３つが挙げられる。

- **我が国の国民生活・経済活動、ひいては国家安全保障に深刻な影響を与えるサイバー脅威への対応**

  サイバー脅威が我が国の国民生活・経済活動、ひいては国家安全保障に深刻かつ致命的な影響を及ぼすおそれに鑑みれば、被害の防止や事案発生後の的確な対処により、サイバー攻撃に対し実効的に防御していくことが求められている。他方、巧妙化・高度化したサイバー攻撃や、国家背景のサイバー攻撃キャンペーン等が顕在化する今日、あらゆるサイバー攻撃から我が国を完全に防御することは困難である。そのため、こうした従来の防御の取組のみならず、能動的サイバー防御を始めとした攻撃者側に対抗する

[17] 量子技術イノベーション会議「量子エコシステム構築に向けた推進方策」（2025 年５月 30 日）

様々な措置を粘り強く講ずることにより、平素から攻撃者側に継続的にコストを負わせ、サイバー脅威を抑止することで、安全保障や危機管理の観点を踏まえた実効的な防御・抑止の取組を進める必要がある。

・デジタル化の進展・浸透等とそれに伴い拡大するリスクに対応した、社会全体のサイバーセキュリティ及びレジリエンスの確保

社会全体のデジタル化の進展や新たな技術革新、サプライチェーンの複雑化等により、あらゆる主体がサイバー攻撃に直面するとともに、一主体の被害や事業停止が社会全体に大きな影響を与えるリスクが発生していることに鑑みれば、攻撃の標的となりうる幅広い主体それぞれにおいて、実効性のある対策の底上げを図らなければならない。前述の能動的な防御・抑止の措置がより実効性を持つためにも、個々の主体が適切な対策を講じ、社会全体のデジタル化とサイバーセキュリティ確保を同時に推進することが必要である。

・我が国のサイバー対応を支える人材・技術の確保と先端技術への対応

実効的な防御・抑止や、自律的な個別主体の対策のためには、我が国において、十分なサイバーセキュリティ人材や技術を確保する必要がある。しかし、我が国は、官民を通じて、サイバーセキュリティ人材の不足が課題となっており、さらに、サイバーセキュリティに関する技術の多くを海外に依存している状況にある。この問題に対応するため、サイバー対応に必要な人材・技術を我が国で持続的に産み出していく環境形成が急務である。また、AI や量子技術等の先端技術は、サイバーセキュリティ分野における活用も期待できる反面、AI の安全性への懸念やサイバー攻撃への悪用、量子計算機技術の進展に伴う既存の公開鍵暗号の安全性低下・危殆化等のリスクも指摘されている。我が国としてこうした先端技術への適切な備えを講ずる必要がある。

こうした課題認識の下、サイバー空間を取り巻く切迫した情勢、社会全体への DX の浸透や技術革新等に的確に対応し、「自由、公正かつ安全なサイバー空間」を確保し、もって基本法の目的に掲げられた「経済社会の活力向上・持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安全の確保」、「我が国の安全保障」の達成を図るためには、

・深刻化するサイバー脅威に対する防御・抑止
・幅広い主体による社会全体のサイバーセキュリティ及びレジリエンス[18]の向上
・我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

の３つの方向性に基づき、施策を推進する必要がある。

（１） 深刻化するサイバー脅威に対する防御・抑止

国家を背景としたサイバー攻撃は、組織化・洗練化されており、また巧妙化・高度化も著しく、我が国にとって現に直面する安全保障上の深刻な脅威である。厳しいサイバー安全保障環境に柔軟かつ適切に対応するため、我が国のサイバーセキュリティにおける司

[18] インシデントが発生した際に、その影響を最小化し、早急に元の状態に戻す仕組みや能力、耐性のこと。

令塔機能を担う国家サイバー統括室を中心に、政府機関等が緊密に連携し、通信情報の利用を含む情報収集等を行うとともに、官民連携・国際連携の下、サイバー攻撃による被害の防止や事案発生後の的確な対処に加え、サイバー対処能力強化法等の成立により可能となった能動的サイバー防御を含む多様な手段を組み合わせることで、平素から攻撃者側に継続的にコストを負わせ、我が国に対するサイバー脅威を能動的に防御・抑止する。

この取組に当たっては、サイバー対処能力強化法等に基づく措置を含め、国が主導して取組を進める必要がある。ただし、国だけで実現できるものではなく、「多様な主体の連携」を、国が積極的に推進する役割を担う。

（２） 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

攻撃の標的となりうる幅広い主体に対し、その主体自身の能力や社会に及ぼすリスクを踏まえ、適切な対策を求めていくことで、社会全体のサイバーセキュリティ及びレジリエンス向上を図る。

まずは、政府機関等が範となり、強固な対策を実践していくとともに、重要インフラ事業者・地方公共団体はもちろんのこと、サイバーセキュリティ確保に大きな影響・役割を持つサイバー関連事業者やベンダー、そして中小企業・個人等といった様々な主体に求められる対策と実効性確保に向けた方策を明確化し、迅速に実施していく。これにより、社会全体のデジタル化とサイバーセキュリティ確保を同時に推進する。

この取組に当たっては、様々な社会システムがサイバーセキュリティに関しそれぞれの任務・機能を「自律的に」果たしていくことが期待され、そうした各主体の取組が促進されるよう、国が支援・環境整備していく。

（３） 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

産学官を通じて、サイバーセキュリティ人材の確保・育成・裾野拡大にこれまで以上に注力していく。また、研究・開発から実装・運用まで、産学官の垣根を越えた協働による、国産技術・サービスを核とした、新たな技術・サービスを生み出すエコシステムを形成するとともに、AI や量子技術等の新たな技術革新がもたらすサイバーセキュリティ分野の変革に備え、対応していく。

これについても、関係する各主体の「自律性」、「多様な主体の連携」とともに、これまで我が国でサイバーセキュリティ分野での人材・技術が十分育ってこなかったことに鑑み、国がより積極的な役割を果たしていく。

これら施策の実現には、官だけ、民だけ、一国だけで対応することには限界がある。官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進していく。

これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す。

くわえて、本戦略に基づき施策を推進するに当たっては、以下の点に留意する。

・我が国全体のサイバーセキュリティ確保のためには、政府機関・重要インフラ事業者等を標的にしたサイバー脅威に対するサイバー安全保障の観点に基づく対応から、個人や企業による主体的・自律的な対策、それを支援する取組に至るまで、切れ目のない取組が必要であり、これらは互いに補い合う関係にある。また、サイバー空間には国境がなく、サイバーセキュリティに係る内外の施策は有機的に連携し推進されるべきものである。本戦略では、これらの必要な施策を切れ目なく一体的・総合的に実施し、施策の実効性を高めることを目指す。
・生成 AI 技術の進展等に伴い、サイバー空間を利用した外国からの偽情報拡散を含む影響工作の脅威の増大が懸念される。この問題は、我が国の健全な民主主義の基盤に影響を及ぼす可能性があるとともに、サイバー攻撃と連動し展開されるおそれもある。こうした状況を踏まえ、当該問題に係る関係府省庁は密接に連携しつつ、我が国のサイバーセキュリティ確保の観点から、本戦略に基づく適切かつ必要な対応を行う。
・これまで述べてきたようなサイバー空間における脅威の実態について、国民の認識と理解を得ることが必要である。国は、サイバー対処能力強化法等に基づく能動的な防御・抑止の措置を含め、国の対応・施策の推進に当たり、関係者と連携しつつ、広く国民の理解と協力を得るよう努めていく。

III. 目的達成のための施策

本項においては、これまで述べた我が国を取り巻く情勢とサイバーセキュリティに関する課題認識を踏まえ、基本法に掲げた目的を達成し、「自由、公正かつ安全なサイバー空間」を確保するため、Ⅱ．３．において示した３つの大きな施策軸の下、今後５年間に実施すべき諸施策の目標や実施方針を示す。

１．　深刻化するサイバー脅威に対する防御・抑止

国家を背景とした組織化・洗練化されたサイバー攻撃は、ゼロデイ脆弱性や、国内外のサーバ等の多数・多段階の組合せを活用して敢行されるなど、巧妙化・高度化も著しく、我が国にとっても現に直面する安全保障上の深刻な脅威となっている。

また、サイバー攻撃は平時と有事の境がなく、容易にエスカレーションし得るという特性がある。我が国に対する武力攻撃の前段階において政府機関や重要インフラ事業者等に対するサイバー攻撃が行われ、武力攻撃が生起した後も軍事的・物理的な手段と組み合わせたハイブリッド戦としてサイバー攻撃が継続されることも想定しなければならない。

このような厳しいサイバー安全保障環境に柔軟かつ適切に対応していくため、サイバー安全保障分野における情報収集、とりわけ国家を背景としたアクター等、サイバー攻撃の攻撃者側に関する情報収集・分析能力を一層強化することによって、的確に状況を把握した上で、我が国に対するサイバー攻撃を防御し、また、我が国にサイバー攻撃の脅威が及ぶことを抑止することで、被害を未然に防止し、又は被害の拡大を防止することが目標となる。そのため、これらの能力を高めつつ、政府全体としてシームレスな対応を抜本的に強化していくことが重要である。

2022 年の「国家安全保障戦略」においては、サイバー空間の安全かつ安定した利用、特に政府機関や重要インフラ事業者等の安全等を確保するために、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」ことを目標に掲げた。その具体策として、国、重要インフラ等に対する安全保障上の懸念を生じさせるサイバー攻撃による被害の防止のため、能動的サイバー防御を導入することとした。同戦略においては、我が国の防衛上の課題に対応する上で、防衛力のみならず、総合的な国力を活用することとされ、防衛力の抜本的強化を補完し、それと不可分一体のものとして、能動的サイバー防御も含むサイバー安全保障の取組を推進し、総合的な防衛体制を推進するとされている。

能動的サイバー防御は、①国がより積極的に関与して官民一体でサイバーセキュリティを確保していく官民連携の強化、②複雑化するネットワークからサイバー攻撃の攻撃元を探知するための通信情報の利用、③サイバー攻撃の攻撃元であるサーバ等に対し我が国の政府機関がアクセスし、脅威を無害化する措置（アクセス・無害化措置）の導入の３点を柱とする。

防御側である被害企業等からの情報収集や対処支援といった既存のサイバーセキュリティに関する施策の強化に加え、攻撃者側に対抗する、能動的サイバー防御を始めとする多様な措置により、平素から攻撃者側に継続的にコストを負わせ、我が国をシームレスに防御す

る態勢を構築していく。これは、我が国の総合的な防衛体制の強化にも資するものと言える。

そのため、今後は、防御側に係る施策と攻撃者に対抗する施策を言わば“車の両輪”とし、我が国のサイバー防御の総合的な向上を図ることで、平素からサイバー攻撃の攻撃者側に一層のコストを継続的に課すことを目指していく。

また、官民の信頼関係と協働体制を基盤とした官民連携エコシステムの形成・横断的な対策を強化するとともに、深刻化するサイバー脅威に対し一国だけで対応することは困難であることを踏まえ、これまで以上に国際連携を推進・強化する。

こうした取組により、上記の目標を達成すべく、必要な投資等を含め、国家サイバー統括室の総合調整の下、官民が連携して、以下のような施策を有機的かつ効率的に組み合わせて実施する。

（１） 国が要となる防御・抑止

国家を背景とした攻撃を含め巧妙化・高度化するサイバー攻撃からサイバー空間を守るため、司令塔の役割を担う国家サイバー統括室が中心となって、関係府省庁や専門機関と連携し、能動的サイバー防御を含む多様な手段を組み合わせることで、被害が生じる前の脅威の未然排除、事案発生後の的確な対処を含め、安全保障の観点も踏まえた実効的な防御・抑止に向けた取組を進めていく。

これまで、国は、迅速かつ的確なインシデント対応や、被害の防止に向け、ナショナルサートとしての機能を担ってきた。情報の収集・分析・提供・発信の円滑化や強化等の取組により、サイバー対処能力強化法等に基づき強化された情報収集・共有等の枠組みも活用しながら、その機能を高度化していく。

また、サイバー対処能力強化法に基づき取得する通信情報や、官民連携・国際連携によって蓄積される情報等のサイバーセキュリティ関連情報を集約・分析し、必要とする主体に対して適切な形で提供していく。

さらに、アクセス・無害化措置を含む攻撃者側に対抗する各種措置の実施体制を早期に確立し、強化を図っていく。

あわせて、こうした取組を実施するに足る体制・基盤・人材等を、諸外国の例も参考に速やかに総合的に整備・運用していく。

① インシデント対処の高度化による被害の拡大・深刻化の防止

サイバー攻撃がもたらすインシデントに対し、いかに迅速かつ効果的に初動対応、調査、原因究明といった対処ができるかが、被害の拡大や深刻化を防ぐために重要である。サイバー対処能力強化法に基づく新たな枠組みも活用し、この対処を更に強化していかなければならない。

国家サイバー統括室は、我が国のナショナルサートとして、インシデントの迅速かつ的確な把握・分析・評価を行う。また、インシデント発生時、関係府省庁や専門機関と連携し、国内の組織や国民向けに適時・適切な注意喚起や情報発信を行うことで、被害の防止を目指す。

迅速な初動対応に向け、国は、サイバー対処能力強化法に基づく、基幹インフラ事業

者（経済安全保障推進法[19]に基づく特定社会基盤事業者）等による国への特定重要電子計算機の届出やインシデント報告のための情報共有基盤を整備する。また、民間企業が安心して情報共有を行えるよう、国は、的確な情報保全に取り組む。さらに、被害組織が対処活動に集中できるよう、国は、被害組織からのインシデント報告にかかる負担の軽減を目指し、サイバー対処能力強化法に基づく報告も含めた報告様式の一元化とともに、報告先の一元化に向けて所要の調整を進める。

被害の防止のための情報発信については、国は、ワンボイスで機関ごとにその内容に差異が生じないように取り組む。国家を背景としたアクターと疑われる組織によるシステムやソフトウェアの脆弱性の悪用に対する懸念が増しており、国による対応の必要性が高まっている。このため、脆弱性情報についても、政府が集約した情報を整理・分析し、率先して、民間事業者等に対し、被害防止に効果的な情報を提供する。また、サイバー対処能力強化法の下での事業所管大臣によるベンダー（電子計算機等供給者[20]）に対する措置要請を含め、サイバー攻撃による被害防止に向けて必要なベンダーの対応を促していく。

くわえて、大規模なインシデントについては、個々の政府機関等での対応に加え、政府全体で統一的に対応することが、被害の拡大・深刻化の防止のために必要である。このため、国は、迅速かつ的確な初動対応のための体制を整備するとともに、政府機関等だけでなく、重要インフラ事業者や地方公共団体、関係機関等とも連携したインシデント対応力を高めるための実践的な演習に取り組む。

② 通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用

サイバー攻撃に的確に対処するためには、その攻撃を早期に検知し、攻撃アクターの特徴を含む攻撃態様を分析する必要がある。

しかしながら、現状においては、攻撃を検知できたとしても断片的な情報しか得られず、被害の防止に資する分析を行うことは困難なケースが多い。そこで、サイバー攻撃に関する公開情報等に加え、サイバー対処能力強化法に基づく基幹インフラ事業者等によるインシデント報告を含む被害報告や、同盟国・同志国等との連携により共有された情報、政府機関等端末の監視・分析で得られた情報、サイバー空間の観測[21]を通じて得られた情報等、分析に有用なあらゆる情報を国家サイバー統括室に集約していく。各府省庁は、同室と連携して、所管業界で起きたインシデントについて、被害組織による対応状況に配慮しつつインシデント情報の収集に努めるとともに、当該情報をサイバー脅威の分析に活用するため、同室へ共有する。独立行政法人情報処理推進機構（IPA）等の関係機関においても、引き続き、被害組織の了承の上で、収集したインシデント情報や分析情報を同室に共有する。

特に、外国国家の関与が疑われる組織化・洗練化されたサイバー攻撃においては、攻撃アクターは攻撃元を隠蔽するため、通常の情報収集の手段では攻撃関連通信の検知や

19 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第 43 号）
20 電子計算機等（重要電子計算機として用いられる電子計算機又は当該電子計算機に組み込まれるプログラムをいう。）の供給（電子計算機等を他人の情報処理の用に供する役務の提供を含む。）を行う者をいう（サイバー対処能力強化法第 42 条第１項）。
21 例えば、NICT が主導する NICTER（Network Incident analysis Center for Tactical Emergency Response）プロジェクト等。

追跡を困難にさせる手法を用いることが確認されている[22]。このようなサイバー攻撃については、そもそも被害側で認知できず政府にインシデント報告等が行われないことも多いため、サイバー対処能力強化法に基づき新たに利用可能となった通信情報を政府自ら利用することにより、潜在的被害の発見や攻撃態様の把握を目指すなど、サイバー脅威に関する情報収集、情報集約を一層強化する。

通信情報については、国家及び国民の安全の確保の観点から、サイバー攻撃により、国、基幹インフラ事業者等の重要な機能が損なわれることを防止することを目的とした上で、通信の秘密との関係で厳格な取扱いを確保しつつ、アクセス・無害化措置の実施においても有効に活用されるよう、分析を行う。その際、防衛省を始めとする関係府省庁等の専門的知見を活用する。

さらに、サイバー関連情報に加え、関係府省庁等の協力の下、サイバー以外の地政学的な情勢を含む安全保障情報等も用いて、攻撃側の意図や目的、外国国家の関与の状況、現実空間における事象との関連性等について、アクセス・無害化措置等における活用も念頭に分析を行うだけでなく、我が国に対する脅威に関する定期的な分析・評価を行う体制を構築し、サイバー分析能力を抜本的に向上させていく。

こうした体制の整備に向け、国家サイバー統括室を始めとする関係府省庁等における分析官の人員拡充・能力向上、AI や諸外国の最先端技術を含む資機材の導入、施設の整備等を進める。これに加えて、民間サイバーセキュリティアナリストとの分析協力を始めとした積極的な連携を推進する。

政府は、分析の結果を政府部内、同盟国・同志国等、サイバー対処能力強化法により新たに締結される協定の当事者、同法により新たに設立される協議会（以下「新協議会」という。）の構成員、さらには、重要電子計算機の使用者やベンダー（電子計算機等供給者）等に率先して提供し、官官・官民双方向の情報共有を促進することによって、情報エコシステムを確立させ、社会全体のサイバーレジリエンスを向上させる。その際は、法令に従い、Need to Share[23]の原則を踏まえ、適切な形で情報を提供するとともに、Need to Know[24]の原則を始めとする保全等の基本的な考え方を踏まえ、適切な情報の取扱いを確保する。

③ アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止

国家を背景としたサイバー攻撃キャンペーンを含め、日常的、持続的に行われているサイバー攻撃に対しては、既存の防御の取組と、アクセス・無害化措置を始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。そのための体制を早期に確立し、強化を図っていく。

具体的には、武力攻撃に至らないものの、安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、攻撃者のサーバ等への直接的な働きかけを通じ、攻撃による被害の防止を目的として、国際法上許容される範囲内でアクセス・無害化措置を実施する。この措置は、サイバー攻撃の脅威の抑止にもつながるものであり、我が国の総

[22] 通常発生する通信に偽装して被害側での検知を難しくさせる手法や、一般利用者の通信機器を乗っ取った多数のボットや C2 サーバを国外も含めて多段階で構成するなどの手法がある。
[23] 情報を、必要な関係者やコミュニティに対しては積極的に共有するという考え方。
[24] 情報を、知るべき必要性があり、知るべき立場の人物に対してのみ共有するという考え方。

力を十全に活用する必要があるため、不正プログラムの解析等の高度なフォレンジック能力や、攻撃者やサイバー攻撃の手口等を解明する高度情報分析能力等を有する警察と、武力攻撃事態等における高烈度なサイバー攻撃に対処するための高度なサイバー防衛能力等を有する防衛省・自衛隊が共同して対処する体制を構築する。

この措置は国家安全保障の観点から整合性のとれた形で行われ、平素から有事に至るまでシームレスな対応を確保する必要がある。サイバー安全保障担当大臣[25]の下、司令塔組織である国家サイバー統括室が国家安全保障局と連携して総合調整機能を発揮し、統一した方針の下で、警察と防衛省・自衛隊が当該措置を適切かつ効率的に実施できる体制を確立する。また、国家サイバー統括室が関係府省庁と平素から情報共有や連絡調整、意見交換等により緊密に連携するとともに、特にアクセス・無害化措置の実施主体である警察と防衛省・自衛隊との間で運用上の連携を確保するため、サイバー攻撃に対処するための新たな拠点を含む運用環境を整備する。

関係行政機関、とりわけ実施主体である警察、防衛省・自衛隊の能力を大幅に強化する必要がある。関係部署や部隊等の体制強化に加え、必要となるシステムや資機材の整備・確保、運用環境について、これらが平時から有事に至るシームレスな対応に寄与する点も念頭に置きつつ、綿密な検討の下、可及的速やかに整備等を進める。

さらに、サイバー対処能力強化法に基づく新たな官民連携の枠組みと既存の取組を組み合わせ、高度な侵入・潜伏能力を備えた攻撃に関し、民間事業者等の情報ニーズを踏まえ、国からサイバー脅威情報等を積極的に情報提供する。これにより、民間事業者等が具体的な行動をとることが可能となり、サイバー攻撃による被害の防止にも寄与する。

以上のようなサイバー対処能力強化法等に基づく取組に加え、従前から行われているサーバ等の管理者と連携した任意のテイクダウン、パブリック・アトリビューション、攻撃手口の公表等も、極めて重要な措置である。重大なサイバー攻撃の脅威の抑止、サイバー攻撃による被害の防止のためには、サイバー対処能力強化法等に基づく措置のみならず、あらゆる選択肢を、関係府省庁との緊密な連携を確保しつつ国家サイバー統括室の総合調整の下で検討し、実施していかなければならない。

以上の能動的な防御・抑止の取組を行っていくため、関係府省庁等の間で共同訓練・演習を実施し、その結果を踏まえた知見や教訓の共有等を着実に進める。また、システムや資機材の整備・確保に当たっては、AI を始めとする先端技術の活用を積極的に検討するとともに、民間事業者が有する高い能力を最大限に引き出せるように努める。

あわせて、事象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や、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れば、サイバー分野における同盟国・同志国等との効果的な国際連携及び国際協調は極めて重要である。特に、アクセス・無害化措置やパブリック・アトリビューション等、能動的な防御・抑止に係る各種措置の検討、実施に際しては、同盟国・同志国等と必要な情報を共有し、共同して対応を図るなど適切に連携するとともに、国際的な枠組み・ルール形成等のための多国間の議論にも積極的に貢献する。

[25] サイバー安全保障の推進、サイバーセキュリティの確保を担当する国務大臣をいう。

④ 体制・基盤・人材等の総合的な整備・運用

我が国のサイバー安全保障の確保に持続的かつ的確に取り組んでいくため、必要となる体制・基盤・人材等を総合的に整備するとともに、関連施策の立案・実施の推進の強化や、サイバー対応・対処に係る能力強化を図っていく。また、運用上の課題や懸念があれば、速やかな見直しや改善に努め、深刻さを増すサイバー脅威に対して的確な対応を行う。このために、司令塔機能を担う国家サイバー統括室を始め、重要インフラ・基幹インフラ所管省庁、サイバー対処能力強化法等に基づくアクセス・無害化措置等の実施省庁やサイバーセキュリティ政策推進省庁においても、体制等の整備・強化等に努めていく。また、政府機関のみならず、公的関係機関[26]、民間団体[27]、民間事業者等が連携し、高度な情報収集・分析能力を担う体制・基盤・人材等を総合的に整備する。

通信情報の利用やアクセス・無害化措置の適正確保のために独立機関として設置されるサイバー通信情報監理委員会については、内閣官房担当部署においてその体制整備等の準備を進め、設立後、適切な承認や検査等、サイバー対処能力強化法において同委員会に付与された権限が的確に行使され、サイバー対処能力強化法等が適正に執行されることを担保していく。この際、これらの手続きを円滑に実施し、法の実効性を高めていくため、同委員会が諸外国の例も参考に運営を検討するとともに、国家サイバー統括室を始めとする関係府省庁は、平素から、同委員会に対して、サイバーセキュリティ情勢やそれを踏まえた認識等、関連する情報を同委員会に前広に共有するなど、認識の共有を図り良好なコミュニケーションに努める。

（２） 官民連携エコシステムの形成及び横断的な対策の強化

サイバー攻撃の巧妙化・高度化により、官のみ、民のみの防御では限界がある中、官民が連携し、一体となって我が国全体のサイバー防御能力を高めることが必要である。

このためには、まず官民が、信頼できるパートナーとして、サイバーセキュリティ対策が企業の存続の鍵となる重要な経営課題であるとの企業的な視点と、サイバーセキュリティ対策は日本全体の安全や産業・技術基盤の自律性や不可欠性の確保といった安全保障に直結するとの国家的な視点について、互いに理解を深めることが重要である。

そして、被害者側に焦点を当てたインシデント対応力の強化に加えて、官民連携を通じた我が国全体のサイバー防御の強化と、攻撃者側に対抗する施策である能動的な防御・抑止に取り組むという、我が国におけるサイバーセキュリティ確保に向けた目指すべき方向性を、官民間で共有していく。

その上で、官民間の双方向・能動的な情報共有と対策のサイクル、すなわち、官民が共に協力し合う、新たな官民連携のエコシステム形成を目指す。

具体的には、国は、民間企業からの情報も踏まえ、サイバー空間における脅威の分析を行い、後述の新協議会の枠組み等を活用し、積極的に民への情報提供を行う。インシデント発生時には、政府機関・民間企業等からのインシデント情報等も踏まえ、被害拡大の防止に向け注意喚起を行う。

---

[26] NICT、IPA 等

[27] 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）、ISAC（Information Sharing and Analysis Center：サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織）等

民間企業は、こうした国の情報も活用しつつ、対策に取り組むとともに、関連する情報を国へ共有するなどの連携を図る。

こうした情報共有と対策のサイクルの構築に加えて、民間における対策強化に向けたリスクアセスメント、官民における脅威ハンティングの実施拡大、演習の体系的な実施を通じた継続的な改善等、官民横断的な対策強化を講ずることにより、官民全体としてのセキュリティ能力及び国家全体としてのレジリエンスの向上を図る。

① 官民間の双方向・能動的な情報共有と対策強化のサイクルの確立

官民連携の前提となる認識共有と信頼関係の醸成には、官民間の複層的な対話の継続的な実施が重要である。実務者層から経営層まで参加し、必要に応じて個別又は分野横断的に異なる階層で行うなど、多角的な視点から対話に取り組む。

組織全体の方向性や戦略を担う民間の経営層が、長期的なリスクやサイバーセキュリティ対策の経営的意義を認識し、広い視野で経営判断を行えるよう、国はニーズを踏まえた脅威、分析、対策に関する情報（以下「脅威情報等」という。）を積極的に提供するとともに、随時、民間の経営層との意見交換を行う。また、サイバーセキュリティの最前線に立つ実務者層が、経営層の理解の下で実効性の高い対策を講じられるよう、国は技術的な脅威の動向や具体的な攻撃手法、対応方法といった実践的な情報を積極的に提供する。

緊急時に初めて連携を模索するのではなく、平素から信頼関係を築き、予測困難なサイバー攻撃の脅威に対し、官民が一体となって効果的に対応できる体制を構築する。これを具体化するために、新たな官民連携のエコシステムの構築に向けて、2026 年秋から、新協議会を立ち上げる。新協議会には、我が国の国民生活と経済活動を支える役務を提供する基幹インフラ事業者を始め、機微情報取扱事業者、セキュリティベンダー、政府機関等が構成員として参加し、国家サイバー統括室の総合調整の下、内閣府が、平素及び事案発生時における脅威情報等の相互共有等を行う。

内閣府は、構成員から汲み取ったニーズも踏まえ、インシデント報告や基幹インフラ事業者の登録資産情報、各政府機関等の資産情報や GSOC[28]ログデータ、国内専門機関や海外当局からの提供情報等、国だからこそ取得できる情報を活用した分析を行う。そして、この分析を踏まえた脅威情報等を構成員に積極的に提供することで、構成員の参画意欲を高め、持続的・発展的な新協議会内コミュニティ作りに取り組む。このため、情報リソースや分析能力の拡充、構成員との継続的なコミュニケーションを通じたニーズ把握に努めるとともに、新協議会内の情報交換の活性化のため、双方向でコミュニケーションを行う情報共有基盤を整備する。

また、特に機微度の高い脅威情報等については、必要に応じて、セキュリティ・クリアランス制度を活用した構成員への提供を行う。このため、国家サイバー統括室を中心に、当該制度の活用に向けた調整を進める[29]。

---

[28] Government Security Operation Coordination team の略（ジーソック）。政府関係機関情報セキュリティ横断監視・即応調整チーム。各機関に設置したセンサーやクラウド監視を通じた政府横断的な監視、攻撃等の分析・解析、各機関への助言、各機関の相互連携促進及び情報共有を行うための体制のこと。2008 年４月から運用を開始した各府省庁等に対する監視体制（第一 GSOC：国家サイバー統括室に設置）と、2017 年４月から運用を開始した独立行政法人等に対する監視体制（第二 GSOC：IPA に設置）がある。

[29] セキュリティ・クリアランス制度の活用に当たっては、クリアランス保有者が国際的なコミュニティ等への参画機会の獲得にもつながり得るなどの副次的効果の視点も考慮する。

将来的には、参加企業等のニーズも踏まえ、官民が協働するプロジェクトの提供等の機能を具備していくことで、新協議会を段階的に発展させるべく取り組む。

また、新協議会の構成員以外の者に対しても、秘密を含まない情報の提供を行うことで、広く国内のサイバーセキュリティの強化につなげていく。

あわせて、関係機関等との連携による対処支援・相談等に係る機能の提供や、民間における対策強化に向けたリスクアセスメントの実施支援等、大規模国際イベントである2025年日本国際博覧会で得られた知見や成果等を2027年国際園芸博覧会等に活かしていく。

② 官民における脅威ハンティングの実施拡大

近年、我が国の官民組織を対象にLiving Off The Land戦術（システム内寄生戦術）のような高度なサイバー攻撃が行われ、経済社会、国民生活、ひいては国家安全保障に悪影響を及ぼす脅威アクター（以下「高度脅威アクター」という。）が観測されている。

既存のセキュリティ対策を適切に実施することが重要であることは言うまでもないが、このようなサイバー攻撃は既存のセキュリティ対策を回避するものが少なくない。こうした中、検知を回避し侵入・潜伏した攻撃痕跡等を探索することによってサイバー攻撃の被害を検知する手法であり、かつ、アクセス・無害化措置を始めとする能動的サイバー防御に資する情報を得る手段として有効である「脅威ハンティング」を実施していく必要がある。特に、高度脅威アクターの標的となる政府機関、独立行政法人、サイバー安全保障を確保する上で重要な民間事業者等における脅威ハンティングの必要性は高いと認められる。そのため、2026年夏を目途に、脅威ハンティングの普及促進、実施等に関する基本方針を策定する。

その上で、以下の点に留意しつつ、セキュリティ能力等の向上を目指し、各種施策を講じていく。

まず、脅威ハンティングが浸透していない我が国の現状に鑑み、脅威ハンティングの普及を促進する必要がある。脅威ハンティングの定義や先端技術の活用を含めた手法の確立等を通じて認知度の向上を図りつつ、必要性や能力・体制等に応じた取組を整理し、脅威ハンティングの実施を促進することが肝要となる。

次に、脅威ハンティングについて、能動的サイバー防御を実施していくための手段としての位置付けを明確にし、期待される役割を明らかにする必要がある。くわえて、その実効性を確保するためには、関係組織における脅威ハンティング能力の継続的強化や強化に係る国家サイバー統括室による支援が必要である。

さらに、脅威ハンティングの実施は組織間の情報等の共有がその有効性を高めるため、官民間の情報共有や国際連携の推進が重要となる。

こうした取組を進めるに当たり、警察や防衛省・自衛隊が有する脅威ハンティング能力を、政府機関や独立行政法人、サイバー安全保障を確保する上で重要な民間事業者等に対して活用することについて検討する。

③ 演習の体系的な実施

インシデント対処等における実践的対応力を強化するためには、現実的かつ最新の脅

威動向を踏まえた演習を実施し、対処体制の有効性を検証していくことが不可欠である。また、演習は、参加者間の相互理解の促進や信頼関係の構築にも資するものであり、官民連携や国際連携の強化にも活用できる。現状、サイバーセキュリティに関する演習は、様々な主体・分野等で行われているものの、各演習相互の連携は限定的であるため、効率性、合理性の観点も考慮しつつ、目的や規模に応じて各種演習の適切な役割分担を図ることにより、その成果を最大化することが求められている。このため、官民連携エコシステムや国際連携の継続的な強化の観点も考慮して、体系的に演習を実施する。これにより、分野を横断して効率的・効果的な演習実施を可能にするとともに、演習ノウハウや成果の相互共有を促進し、演習を通じて国家全体としてのレジリエンス向上を図る。

（３） 国際連携の推進・強化

サイバー攻撃は、匿名性、非対称性とともに越境性という特性を有しており、その攻撃手法等は、近年、一層巧妙化・高度化している。このようなサイバー攻撃に対し、いかなる国家も単独で対応することは困難であり、国際連携の推進は、我が国のサイバーセキュリティ政策における基軸である。

こうした認識の下、同盟国・同志国等との情報・運用面での協力の強化を通じ、我が国のサイバー分析・対処能力の向上を目指すとともに、悪意あるサイバー活動の抑止に向けた国際的な取組に積極的に参画する。

また、インド太平洋地域の安定と繁栄が我が国の発展の基盤であることを踏まえ、同地域における対応能力向上のための支援を進める。

さらに、同盟国・同志国等と連携して国際的なルールの形成に積極的に参画し、我が国の基本的な理念を反映するなどにより、サイバー空間における国際秩序の維持・発展に寄与していく。

以上の取組を一体的・総合的に推進することにより、国際社会において責任ある主導的な役割を果たし、「自由、公正かつ安全なサイバー空間」の実現を目指す。

① 同盟国・同志国等との情報・運用面での協力の強化

深刻化するサイバー攻撃に対しては、各国政府・民間等様々なレベルで、情報・運用面を含め、重層的な協力・連携を進めることが重要である。

同盟国・同志国等の関係機関との間で継続的な対話を行い、政策面でのベストプラクティスのみならず、脆弱性情報やIoC（Indicator of Compromise[30]）情報、攻撃手法等のサイバー攻撃に関する技術情報やサイバー攻撃の背景・目的に関する情報等を的確に共有し、我が国のサイバー分析・対処能力向上に資する情報協力を進める。この際、必要な情報保全措置を徹底する。

多国間では、日米豪印、日米韓、日ASEAN等の協力枠組みに加え、CRI[31]等の脅威対処に係る多国間会合や国際的なCERT間のネットワークにおける連携強化を進める。

---

[30] セキュリティ侵害インジケータ。システムに対する攻撃発生やどのようなツールが使われたかなどを明らかにする手がかりとなる情報。

[31] カウンターランサムウェア・イニシアティブ（Counter Ransomware Initiative）。ランサムウェアに対する国際連携をテーマに、米国主導で2021年10月に設立された多国間会合。2025年10月27日現在、74の国及び機関が加盟し、ランサムウェアの対処、普及啓発活動、脅威情報の共有等について議論している。

また、国際共同捜査を引き続き推進し、検挙を通じたサイバー脅威の抑止に向け、インターポール及びユーロポールとの更なる連携強化を含む多国間における捜査機関の協力関係の確立等に積極的に取り組む。

その上で、悪意あるサイバー活動の抑止に向け、脅威の主体を特定し、公表するパブリック・アトリビューションや、悪意あるサイバー活動の技術的情報をまとめた国際技術文書の公表等の取組について、国際的に主導できる能力を構築するとともに、外交面での対応を含め、同盟国・同志国等との間で緊密に連携して推進する。また、能動的な防御・抑止に係る各種措置の検討及び実施について、同盟国・同志国等と適切に連携し、運用面における当局間の協力を深化させる。

② インド太平洋地域におけるサイバー安全保障分野の対応能力向上の支援・推進

サイバー攻撃が国境を越える中において、インド太平洋地域を始めとする諸外国の安全保障環境は、我が国のサイバー安全保障政策に直結する。このため、サイバー安全保障分野における対応能力の向上の支援・推進を通じて、域内の「弱い環のない」サイバー安全保障環境の醸成をリードするとともに、対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安全の確保にも貢献する。

能力構築支援については、同盟国・同志国、国際機関、産学といった多様な主体と連携して重層的に、かつオールジャパンで戦略的・効率的に実施していく。その際、特にASEANを含むインド太平洋地域については、その地政学的な重要性等を踏まえ、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）等の活用や同盟国・同志国・国際機関等との協力を通じた能力構築支援の強化により、サイバー外交・安全保障における連携を深化する。

また、人材育成やサイバー演習のみならず、サイバー行動に適用される国際法の理解・実践、政策形成等や次世代のサイバー空間を形成する先端技術等に関する分野においても、能力構築支援を実施していく。くわえて、国際会議等を通じて、我が国のサイバーセキュリティのブランド化を図り、我が国のサイバー対応能力を支えるエコシステムの発展に繋げるとともに、海外へのサイバーセキュリティに係るビジネス展開を後押ししていく。

③ 国際的なルール形成の推進

国際連合憲章を始めとする国際法は、サイバー空間において適用される。サイバー空間における国家による国際違法行為は当該国家の国家責任を伴い、被害国は、一定の場合には、当該責任を有する国家に対して均衡性のある対抗措置及びその他合法的な対応をとることが可能である。また、先行する悪意あるサイバー行動が国家に帰属することが確認できない場合であっても、一定の条件に合致する場合には、国際法上の緊急状態を援用して一定の措置をとることも認められる。

かかる考え方の下、「自由、公正かつ安全なサイバー空間」の確保に向け、政府職員の様々なレベルが、国際場裡において「顔」となり、我が国の基本的な理念を発信するとともに、同盟国・同志国等と連携し、サイバー空間における法の支配の推進及び我が国の基本的な理念に沿った国際的なルール形成に積極的な役割を果たしていく。また、

アクセス・無害化措置を含む能動的サイバー防御は、我が国の国家実行として国際法規範の形成に影響を与え得る事項であることに留意し、サイバー行動に係る国際法及び国際的なルール形成の議論に積極的に参画・貢献していく。

国際的なルール形成は、国連や G7 を始めとする同盟国・同志国間や多国間の枠組みにおいて進展している。サイバー空間における国際的なルール形成及びその運用が、国際社会の平和と安定及び我が国の安全保障に資するものとなるよう、あらゆる取組を行っていく。健全なサイバー空間の発展を妨げるような試みについては、同盟国・同志国や民間団体等、あらゆる主体と連携して対抗する。

さらに、AI・量子技術等の先端技術がサイバー空間に及ぼす影響を踏まえ、サイバー脅威に対する防御・抑止の観点から、国際的なルールの形成等に向けて早急に対応を進める。

２．　幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

サイバー空間に参画する各主体は、誰もが攻撃の標的となりうる。また、サイバー攻撃を受けた場合、自らが保有する第三者の情報資産の漏洩や、自身の機器・システムが更なる攻撃の踏み台にされること等により、第三者の被害につながるリスクもある。

また、経済安全保障の観点からも、外部に流出した場合に国家及び国民の安全を損なうおそれのある重要なデータ等について処理や保存を含めた適切な取扱いを確保する必要性が高まっている。

このような状況の下、各主体は、自らが攻撃の標的となり得ることを前提に、その主体自身の能力や社会に及ぼすリスクを踏まえ、自身のみならず社会全体のサイバー被害を防止・低減するために、適切な対策を講ずる責務がある。こうした対策は、安全保障への深刻な脅威となるサイバー攻撃に対する防御・抑止との相乗効果も期待されるため、各主体の前向きな取組が促進されるよう、国も総合的な施策を講ずるなど、積極的な役割を担っていく。

政府機関等や重要インフラ事業者等は、今日、国家を背景とした組織化・洗練化されたサイバー攻撃の標的となっている。被害を受ければ、国民生活や社会経済、ひいては国家安全保障に甚大な影響を及ぼすおそれがあり、これらの組織は、自らの社会的責務を果たすためにも、サイバーセキュリティの確保に大きな責任を負う。

また、様々な製品・サービス、企業や組織が相互に依存し、サイバー空間と接続される今日、製品・サービスを製造・開発・提供するベンダーが果たす役割と責務も、ますます大きなものとなっている。中小企業も、サイバー攻撃による被害を受けた場合、サプライチェーンで連結している企業等に大きな影響を与える可能性があるため、委託元組織との連携や、公的な支援の活用も視野に入れながら、対策水準の向上を目指す。こうした取組を通じて、あらゆる組織が、自身の能力や、自身がサイバー攻撃を受けた際に社会に及ぼすリスクを踏まえ、自らが遂行すべき業務や製品・サービスからエンドユーザーに至るサプライチェーン全体の信頼性確保に務める「任務保証[32]」の考え方の下で、サイバーセキュリティを確保し、レジリエンスを高めていかなければならない。

さらに、国民一人一人が基本的な取組や対策を行うことができれば、各個人の被害の低減につながるだけでなく、社会全体のサイバーセキュリティ及びレジリエンスの向上にもつながることが期待される。そのためには、個人が適切な知識に触れる機会や、行動につなげる機会を増やすため、産学官民の多様な主体が連携し、適切な役割分担の下普及啓発・情報発信に取り組むことが重要となる。

こうした幅広い主体による対策や必要な投資、ルールメイキング・標準化等の取組と、アクセス・無害化措置を含む多様な手段による能動的な防御・抑止の措置の相乗効果により、我が国の社会全体のサイバーセキュリティ及びレジリエンスの水準を、これまで以上に向上させることを目指す。そして、社会全体のデジタル化とサイバーセキュリティ確保を同時に推進する。

---

[32] 企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。

（１） 政府機関等におけるサイバーセキュリティ対策の強化

政府機関等においては、自身が巧妙化・高度化するサイバー攻撃の標的となっていること、そのシステムのサイバーセキュリティ及びレジリエンス確保が我が国の安全保障の観点から重要であることも踏まえ、他の主体の範となるべく、セキュリティ対策水準の向上と監査等を通じた実効性の確保、継続的な見直しを実施していくとともに、自身を対象とする監視体制をより強化・高度化していく。

さらに、政府においては「誰一人取り残されない、人に優しいデジタル化」を実現するためのデジタル改革を推進しているが、サイバーセキュリティは国民がデジタル社会の恩恵を享受する上で不可欠のものであり、政府機関等の情報システムにおいては構築の段階からセキュリティの確保に配意して整備することが求められる。

また、人材面においても、分析能力の向上や官民連携の強化等を担う人材の育成等を一段と充実・強化していく。

① 対策水準の向上と継続的な見直し

各政府機関等は、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「政府統一基準群[33]」という。）を踏まえ、自らの責任において、自身の業務、取り扱う情報及び保有する情報システムの特性等を踏まえたリスク分析・評価を行い、講ずべき対策の優先順位や必要なセキュリティ対策水準を定め、適切な対策を講じていく必要がある。あわせて、国は、各政府機関等が準拠する政府統一基準群や、政府情報システムのためのセキュリティ評価制度（以下「ISMAP[34]」という。）等について継続的な見直しを行うなど、社会情勢や環境変化等を踏まえ新たな取組を進め、政府機関等全体としての対策水準の向上を推進していく。

ア 政府統一基準群の継続的な見直しや監視の結果等を活用したメリハリのある監査

国は、絶え間なく出現するサイバー脅威やリスクに対応するため、引き続き、政府統一基準群の継続的な見直しを実施する。その際、政府統一基準群の適用対象の範囲は広く、また、情報システムも多種多様であることを踏まえ、各政府機関等がより高いセキュリティ水準の対策を検討する際の目安となるよう、講ずべき対策のベースラインに加えて、より高いレベルの対策についても政府統一基準群において示していくなど、各政府機関等が高い水準のセキュリティ対策を柔軟に実施できるよう、より実態に即した改定を進めていく。

また、各政府機関等は、外局や地方支分部局、施設等機関を含め、自らの責任において、政府統一基準群に基づき情報セキュリティ対策を講ずることが求められている。情報システムの管理を始め、こうした対応が確実にとられるよう、国家サイバー統括室は、監視の結果等を活用したメリハリのある監査等を行い、戦略本部の下に発足した「サイバーセキュリティ戦略推進会議[35]」等を通じ、各府省庁における措置の徹底及び改善を

---

[33] 国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みであり、国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。

[34] Information system Security Management and Assessment Program の略（通称：ISMAP（イスマップ））。政府情報システムにおけるクラウドサービスのセキュリティ評価制度として 2020 年度に制度運用を開始。

[35] 我が国のサイバー対処能力の向上及びサイバーセキュリティの確保に関し、関係行政機関が情報交換・意見交換を行い、連携を図るとともに、総合的な施策を検討・推進するため、サイバー安全保障担当大臣を議長、各省官房長級を構成員として開催される会議。

図っていく。

イ　ISMAP の継続的な見直し

クラウドサービスの進展とともに、政府機関等によりクラウド上で取り扱われる情報は質・量ともに多様化しているところ、これらの状況に適切に対応するため、国は、取り扱う情報により求めるセキュリティ水準の合理化を図る、最新のセキュリティ対策の柔軟な導入を可能とするなどの制度の見直しを実施する。

その上で、クラウドサービスは日々進展していること等から、ISMAP の運用状況、海外の取組、国際規格の改定等を踏まえて、国は、制度の継続的な見直しを実施する。

ウ　政府機関等における機密性の高い情報の取扱いの検討

近年高度化が進むクラウド技術については、可用性・拡張性・冗長性の面で利点があることから、当該技術の活用拡大は我が国政府機関等においても不可避な趨勢（すう）である。

他方、政府機関等における機密性の高い情報の取扱いについては、我が国のコントロールが及ぶ形でその機密性・完全性・可用性を適切に確保する必要があるところ、情報保全・秘密保全を前提としたクラウド技術の活用の在り方に関し、諸外国の政府機関等におけるクラウド技術の活用状況も踏まえつつ、その運用範囲を含めて検討を行い、2026 年夏を目途に方向性を示し、同年度末を目途に一定の結論を得る。

エ　政府機関等の IT 調達等におけるサプライチェーン・リスクの軽減

政府機関等の IT 調達等においては、時代の変化や技術の進歩等に伴い、調達される機器・サービスが変化していくことが想定されるほか、サプライチェーンの広がりや複雑化を背景にリスクの潜在化も懸念されるところ、そのような環境変化の下にあってもサプライチェーン・リスク [36]を十分に軽減できるよう、関連制度との調和を図りつつ、技術的な検証方法の確立を含め、体制・制度の継続的な見直しを行い実効性を確保する。

② 政府機関等の監視体制・インシデント対応力の更なる強化・高度化

2025 年に改正されたサイバーセキュリティ基本法（以下「改正基本法」という。）において、新たな戦略本部事務として追加された政府機関等のサイバーセキュリティの確保の状況の評価の一環として、これまで行ってきた GSOC による政府横断的な不正な通信の監視等の取組を、公的関係機関（NICT 及び IPA）と連携し、強化・高度化する。

国家サイバー統括室は、検知能力の拡大に向け、GSOC センサーの高度化を進めるとともに、政府機関等の監視に必要な情報のより一層の収集・集約に向けた検討を進める。また、GSOC 機能のクラウド監視への対応を継続的に実施する。さらに、政府機関等の多層防御の一環として、CYXROSS センサー[37]を全府省庁を含む政府機関等の端末を対象に、効果的な監視先を判断しつつ導入して監視及び分析を行う [38]。くわえて、国家サイバー

[36] サプライチェーンの過程で製品に不正機能等が埋め込まれるリスクや政治経済情勢による機器・サービスの供給途絶等、サイバー空間自体の信頼性や供給安定性に係るリスク。

[37] NICT が開発した、安全性や透明性の検証が可能なセンサーのこと。

[38] さらに、CYXROSS で収集した一次情報の分析を通じて得られる知見等を民間部門に共有することにより、我が国のセキュリティ技術力・開発力の強化につなげる（Ⅲ．３．（２）参照）。

統括室は、インシデント発生時に適切な対応を行うなどの観点から、資産情報の把握に努めるとともに、各政府機関等の情報資産のうち、インターネットに露出しているものについては、引き続き脆弱性調査・随時是正の取組を行うなどにより、政府機関等における脆弱性対応の強化を図る。これらの取組の実効性確保のため、各政府機関等は、国家サイバー統括室との緊密な連携の下、監視に必要な情報の提供や対策水準の向上等を行う。

以上の取組を踏まえ、国は、政府機関等を対象としたサイバー攻撃の情報の分析を強化し、各政府機関等のサイバーセキュリティ確保に資する情報のみならず、未知のサイバー脅威に関する情報の作出を行う。このため、クラウド監視の拡大・CYXROSS の導入等により増大するログや収集・集約した監視情報をより効率的・効果的に分析するための検討を行う。特に、AI を使った巧妙な攻撃が既に行われている中で、防御側としても AI の活用を引き続き進めていく。また、各政府機関等の横断的な脅威探索やインシデントの相関分析を深化させ、発見が困難な攻撃に対する検知能力の拡大を図るとともに、巧妙化・高度化するサイバー攻撃に対するデジタルフォレンジック能力の向上を図る。

そして、こうしたサイバー攻撃による被害拡大防止のため、分析によって得られた知見を積極的に提供する。例えば IoC 情報等については、引き続き政府機関等内部で共有するほか、新協議会の場を活用し、情報提供を行う。

③ 強靭な政府情報システムの構築と運用

国民目線に立った利便性向上とサイバーセキュリティの確保を両立させるため、デジタル庁は、政府機関等の「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」（情報システムの整備及び管理の基本的な方針（2021 年 12 月 24 日デジタル大臣決定）別添）を策定しているが、サイバー脅威の高まりも踏まえつつ、引き続き、デジタル社会推進標準ガイドラインやセキュリティに関するドキュメントの整備、継続的な見直し等により、企画から運用までを含めた政府情報システム等におけるセキュリティの一層の実装に努める。

また、デジタル庁が整備・運用する国民に対するサービスの基盤システム、各府省庁が共通で利用するシステム等の重要な政府情報システムについての監視等によるインシデント対応能力強化、監査・脆弱性診断の実施等により、当該システムの強靭性確保とサイバーセキュリティ強化を図る。くわえて、稼働状況等を監視するシステム（COSMOS[39]）や、情報資産・脆弱性等を管理することでリスクを常時把握し対処する仕組み（CRSA[40]）等を整備し、さらにセキュリティの確保されたガバメントクラウドやガバメント・ソリューション・サービス（GSS）の利用機関の拡大等を通じて、政府機関等のセキュリティ向上を推進する。

さらに、各政府機関等においては、政府統一基準群やデジタル社会推進標準ガイドライン等を踏まえつつ、自らの業務、情報システムの特性等を踏まえたリスク分析・評価を行い、企画から運用まで一貫したセキュリティ対策を実施する考え方（セキュリティ・バイ・デザイン）を徹底し、適切なセキュリティ水準が確保された情報システムを構築

[39] COSMOS とは、Comprehensive Operation and Monitoring System の略（通称：COSMOS）。
[40] CRSA とは、Continuous Risk Scoring and Action の略（通称：CRSA）。

するとともに、情報資産・脆弱性等の的確な管理、インシデント発生時の早期復旧の確保等により、適切な運用を推進する。

④ 政府機関等におけるサイバーセキュリティ人材の育成・確保と体制の強化

サイバー空間を巡る脅威に的確に対処するためには、政府においても、分析能力の向上や官民連携の強化等を担う人材の育成等を一段と充実・強化する必要がある。このため、各組織で必要となるサイバーセキュリティ人材の定義を今後策定する人材フレームワークの考え方も踏まえて明確化した上で、リテラシー向上も含めた研修や演習の充実・強化等の育成施策、政府における官民交流や外部の高度専門人材を登用する仕組みの効率的・効果的な運用につなげる。

特に、攻撃者の手法に精通し、ネットワークに潜伏する脅威を早期に発見し、迅速かつ適切に対処できる、高度な対処能力を有する人材の育成が不可欠である。攻撃者の視座を持って訓練を日頃から行うことができる、現実に即した大規模な演習環境を新たに構築し、政府機関等の中核的な対処人材の育成を推進する。

また、各府省庁において「デジタル人材確保・育成計画」を作成し、「サイバーセキュリティ・情報化審議官」等による司令塔機能の下、必要な体制整備、総合職試験「デジタル」区分及び一般職試験「デジタル・電気・電子」区分の合格者からの積極的な採用、研修や演習の実施、資格取得の促進、適切な処遇の確保、業務特性を踏まえた任期の柔軟な運用についても着実に取り組むとともに、毎年度計画のフォローアップを行い、一層の取組の強化を図る。

また、関係事業者との協力の在り方の検討を含めて、優秀な人材が政府部内や民間企業との間を行き来してスキルアップを図れる環境の整備も推進する。

（２） 重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化

国民生活及び経済活動の基盤である重要インフラ[41]においては、そのサービスの安全かつ持続的な提供のため、官民が連携して重点的に防護していく必要がある。

また、地方公共団体が多数の機微な情報を保有していること等に鑑み、国は、地方公共団体においても適切にサイバーセキュリティ対策が実行されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施する。

さらに、組織全体としての画一的な対策の適用に困難が伴う大学・大学共同利用機関（以下「大学等」という。）は、法人のトップのリーダーシップの発揮による、主体的なセキュリティ水準の維持・向上が重要となる。このため、国は大学等による自律的な取組を支援していく。

① 重要インフラ事業者等におけるサイバーセキュリティ対策の強化

重要インフラ事業者等[42]におけるサイバーセキュリティ対策については、「重要インフラのサイバーセキュリティに係る行動計画」（2025 年 6 月 27 日サイバーセキュリティ戦略本部決定。以下「行動計画」という。）の下、官民が緊密に連携して取り組んで

[41] 他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもので、重要インフラ分野に属するもの。
[42] 基本法第 12 条第２項第３号に規定する重要社会基盤事業者及びその組織する団体並びに地方公共団体。

いるが、重要インフラを標的とするサイバー攻撃のリスクが顕在化する中、更なる対策の強化が必要となっている。

このため、改正基本法による新たな制度により、分野・事業者横断的に講ずべき基本的な対策の徹底を図るとともに、重要インフラを取り巻く環境変化を踏まえた行動計画の見直しを行い、重要インフラ分野全体のサイバーセキュリティ水準の引上げを図る。

ア　重要インフラ統一基準の作成とこれに基づく取組

現在、各重要インフラ分野においては、行動計画に基づく安全基準等策定指針等を踏まえ、基準やガイドライン等が定められている。他方で、各分野における取組の評価と改善につながるような具体的かつ統一的な基準はなく、サイバーセキュリティ確保の取組やその水準は分野・事業者によってばらつきが見られる。年々巧妙化・高度化の進むサイバー攻撃に対応するためには、重要インフラ事業者等において分野・事業者横断的に講ずべき対策（ベースライン）の徹底が求められる。

このため、改正基本法に基づき、重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施すべき施策について具体的かつ統一的な基準（以下「重要インフラ統一基準」という。）を新たに定める。

この重要インフラ統一基準を通じた PDCA サイクルを構築し、重要インフラ分野全体におけるサイバーセキュリティ水準の引上げを図る。具体的には、国家サイバー統括室による重要インフラ所管省庁を通じた各分野の重要インフラ事業者等の取組状況に対する専門的調査、所管省庁による当該調査結果を踏まえた施策の実施状況の取りまとめ、戦略本部による評価の実施により、所管省庁における各分野の施策や、各分野における重要インフラ事業者等の取組の改善につなげる。

官民の情報共有に関しても、重要インフラ統一基準や関係制度を踏まえ、情報共有の対象や情報連絡の流れ等、情報共有の在り方を整理し、より効果的な枠組みとする。

重要インフラ統一基準の作成は、現行制度や国際・技術・脅威の動向等を踏まえ、2026 年度に行う。また、行動計画についても、当該基準や、基幹インフラ事業者を対象とした制度等を踏まえた見直しを 2026 年度に行うほか、重要インフラを取り巻くサイバーセキュリティの環境変化も踏まえて更なる見直し[43]を行う。

イ　重要インフラ防護範囲の在り方

基本法に基づく重要インフラ事業者等と、基幹インフラ事業者は、法律の趣旨の下に対象分野・事業者が定められており、それらの間には差異が見られる。

基幹インフラ事業者は、サイバー対処能力強化法に基づきインシデント報告等が求められるなど、サイバーセキュリティ確保の重要性が増大していることに鑑み、例えば、現在、基幹インフラのうち重要インフラに含まれていない分野・事業者について、それぞれの特性を踏まえつつ、新たに重要インフラ防護の対象として位置付けるなど、重要インフラ防護範囲の在り方の見直しを検討する。

当該検討においては、基幹インフラ事業者を対象とした制度における届出やインシデント報告等に当たって前提となるサイバーセキュリティ対策を含め、重要インフラ統一

[43] 行動計画「VI. 評価・検証」及び「VII. 本行動計画の見直し」に基づく見直し。

基準に基づく、分野・事業者横断的に講ずべき基本的な対策の徹底を図り、関係事業者においてより効果的な取組がなされるようにする。

ウ 個別分野での取組

重要インフラでも、これまで特に深刻な被害にあっている一方、十分な取組が進んでいない分野や、国民生活・経済活動に大きな影響を与える分野等については、特に個別の取組を進めていく必要がある。

例えば、医療分野は、これまで、外部委託先におけるセキュリティ対策や委託元による監督が不十分だったこと等から、サイバー攻撃により長期間にわたり診療に大きな影響を及ぼす事案が発生している。医療機関等については、インシデント発生による診療等への影響を最小限とするため、「医療情報システムの安全管理に関するガイドライン」に係る周知啓発や、復旧に向けた初動対応支援等を実施するとともに、攻撃の侵入経路となり得る外部ネットワーク接続点（以下「外部接続点」という。）の管理支援を継続する。

さらに、外部接続点の管理状況調査結果を踏まえて、国は、外部接続点の適正化等を含めた上記のガイドライン遵守のための支援を進める。また、医療機関における外部接続点の一部である医療機器についても、サイバーセキュリティを強化するための製造販売業者向けガイドラインの作成や支援等を実施する。

② 地方公共団体におけるサイバーセキュリティ対策の強化

地方公共団体が、個人情報等の多数の機微な情報を保有し、国民生活や地方の経済活動に密接に関係する基礎的なサービスを提供していることに鑑み、国は、地方公共団体において適切にサイバーセキュリティ対策が実行されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施する。

2024 年に改正された地方自治法（昭和 22 年法律第 67 号）に基づき、地方公共団体は 2026 年度から、サイバーセキュリティを確保するための方針の策定が義務付けられることから、国は、当該方針に基づく対策の実効性を確保するため、新たに策定される重要インフラ統一基準[44]も踏まえ、地方公共団体のセキュリティ基盤の強化のための更なる取組を進める。

具体的には、自治体情報セキュリティクラウドの円滑な更新に向けた財政的な支援やデジタル人材の確保・育成に対する支援[45]及び人員体制構築に必要な実践的サイバー防御演習（CYDER）等の研修プログラム、地方公共団体情報システム機構（J-LIS）が運営する自治体 CSIRT 協議会の活用推進を図るとともに、地方公共団体の情報システムに内在する脆弱性等を診断するシステムを構築し、地方公共団体の脆弱性対処能力の向上を図るなど、更なる安全性の確保に向けた取組を実施する。また、各地方公共団体が情報セキュリティ監査等を実施できるよう、適切な財政措置を講ずるとともに、サイバーセ

[44] 本基準は、重要インフラ事業者等におけるサイバーセキュリティの確保に関する国の行政機関の施策についての基準であり、この「重要インフラ事業者等」には地方公共団体も含まれる。

[45] 都道府県が市町村と連携した DX 推進体制を構築し、その中で、市町村支援のためのデジタル専門人材のプール機能を確保できるよう、国は、都道府県による市町村支援のためのデジタル人材の確保に対し地方財政措置を講ずるとともに、計画的にデジタル人材の確保・育成に取り組めるよう伴走支援等の支援を実施。

キュリティ対策の実施に必要な予算や人員の確保に向けた取組を強化する。

さらに、全ての地方公共団体が確実にサプライチェーン・リスク対策を含むサイバーセキュリティ対策を実施できるような新たな仕組みの構築を検討する。

あわせて、「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づく対策が適切に実施されるよう、国は引き続き、地方公共団体の取組を支援する。

国民生活や国民の個人情報と密接に関わるマイナンバーについても、引き続き、国は利便性とセキュリティの調和を考慮して対策を強化し、安全・安心な利用を促進する。

③ 大学等におけるサイバーセキュリティ対策の強化

大学等は、多様な構成員によって構成され、多岐にわたる情報資産を有し、さらに学問の自由の精神に基づき各構成主体の独立性が尊重される文化を持つため、組織全体としての画一的な情報セキュリティ対策を適用することに困難が伴う。こうした中で、大学等が安全・安心な教育・研究環境を確保しつつ、教育・研究・社会貢献といった役割を果たしていくためには、サイバーセキュリティ対策が重要な経営課題となっていることへの認識を更に深め、組織の特性を踏まえた上で、法人のトップがリーダーシップを発揮し、情勢の変化に応じ、主体的なセキュリティ水準の維持・向上を絶えず図っていくことが重要となる。

そのため、国は大学等による自律的な取組を支援するべく、サイバーセキュリティ対策や体制整備等に関する助言・情報共有、研修・訓練の実施、事案発生時の助言等の支援を行う。また、経済安全保障の観点から特に技術流出の防止が必要とされる研究開発プログラムを実施する大学等において研究セキュリティが確保されるよう、サイバーセキュリティの観点からも必要に応じて支援を行う。

（３） ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保

従来、サイバーセキュリティは、各企業等が自ら確保するものと考えられてきたが、社会全体への DX の浸透に伴い、特定の企業へのサイバー攻撃が、その委託先や取引先等、サプライチェーンを構成する企業全体に影響を及ぼしうる事態が発生するようになった。こうした中、国際的な潮流であるセキュアバイデザイン・セキュアバイデフォルト原則、改正基本法における情報システム等供給者の責務規定[46]の新設等、サプライチェーン全体を通じてサイバーセキュリティが確保されるべきものとなったことを踏まえ、そのサイバーセキュリティ及びレジリエンスの確保に向けて取り組む。

なお、その際、阻害要因となりかねない現行制度の課題を抽出し、それらの解消を図ることも重要である。そのため、国家サイバー統括室は関係府省庁と連携し、例えば、セキュアバイデザイン・セキュアバイデフォルト原則の浸透やセキュリティガバナンス向上等、現場・実務におけるサイバーセキュリティに関する諸課題の掘り起こし、課題解決に向けた関係府省庁・民間企業等との総合調整、社会全体を俯瞰したルールメイキング、サイバーセキュリティ関係法令に関する普及啓発等を推進する。

[46] 改正基本法第７条第２項

①セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組の推進

情報システム等のセキュアな設計・開発・維持管理を促進するため、情報システム等供給者が利用者との関係で果たすべき責務を明確化する。また、供給者の責務が社会全体に浸透し、利用者がセキュアなサービス・製品に触れ、容易に自らのサイバーセキュリティを確保できることが当たり前となるための制度構築を推進する。

一定のセキュリティ水準を満たす IoT 製品を認証する「JC-STAR」制度について、更なる制度構築を進め、ガイドライン・補助金等各種施策と組み合わせつつ、政府機関・地方公共団体・重要インフラ事業者・産業界等、社会全体で活用を促進するとともに、諸外国の類似制度との相互運用性の確保を推進する。SBOM(Software Bill of Materials)を含めたソフトウェアの透明性確保に有用なツールの活用や安全なソフトウェア開発の実践についても同様に、社会全体で促進に取り組んでいくとともに、我が国が主導する形での諸外国との制度調和に向けた活動に取り組んでいく。

② サプライチェーンを通じたサイバーセキュリティ及びレジリエンスの確保

サプライチェーン全体でのサイバーセキュリティ及びレジリエンス確保に向け、単なるシステム管理の問題ではなく、包括的なリスク管理の問題として、サイバーセキュリティに係る視点を企業経営に取り入れる必要性がある。そのため、国は、経営者の意識改革や企業の行動変容をより強力に促し、各企業がセキュアな製品調達や取引先選定を行うための環境整備に取り組む。同時に、サステナビリティを重視する投資家等ステークホルダーへの可視化等、サイバーセキュリティ対策にインセンティブが生じる取組等を推進する。

具体的には、まず、2025 年度中に、発注元企業による取引先企業へのセキュリティ対策の支援・要請に係る関係法令等の適用関係を明確化したガイドラインにおいて想定事例を追加し、関係業界等への周知を図る。また、2026 年度には、サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度について、運用開始し、重要インフラを含む業界団体と連携した普及を目指す。そのほか、産業界向けの人材育成プログラムやサイバー攻撃への初動対処支援といった既存の施策の拡充を含め、サプライチェーン全体のサイバーセキュリティ対策強化に向けてあらゆる施策を総動員する。

また、「サイバー・フィジカル・セキュリティ対策フレームワーク [47]」について、企業・業種横断のデータ基盤・システム連携のプラットフォーム構築や社会・産業構造のアーキテクチャ設計での活用を促進し、対応する国際規格の改訂動向等も見据えながら継続的に更新することで、あらゆる主体が相互に連関・連鎖を自由に形成して新たな価値を創出していくための基盤としての役割を実効的な形で果たしていく。

さらに、国内投資が旺盛に進む分野や、経済安全保障確保の観点から自律性の向上が求められる分野等で、将来的に急速な普及が見込まれる AI・ロボット・量子等の先端技術について、セキュリティ上の課題に対応するためのガイドライン等の策定を進めると

[47] サイバー・フィジカル・セキュリティ対策フレームワークとは、「Society 5.0」において、①サイバー空間でのデータの流通・連携の拡大、②フィジカル空間とサイバー空間の融合、③企業間のサプライチェーンの複雑化によって生まれる、サイバー攻撃起点の拡散、フィジカル空間への影響の増大という新たなリスクに対応するために必要なセキュリティ対策の指針。

ともに、投資・技術開発支援策等政府の各種施策との連動等を図り、ガイドライン等が実効的に活用されるための仕組みを構築する。

デジタル社会の基盤となるデジタルインフラに関するセキュリティ確保や自律性向上の観点から、例えば、我が国と海外との通信の大部分を依存する国際海底ケーブル等のインフラについて、官民間・国際間で連携しつつ、安全性、信頼性及び冗長性の確保、防護を推進するとともに、自律的な生産・敷設・保守の体制を確保する。

③ 中小企業を始めとした個々の民間企業等における対策の強化

サプライチェーン全体のサイバーセキュリティ及びレジリエンス確保には、中小企業等におけるサイバーセキュリティ対策が不可欠である。一方、中小企業等には、依然として、対策の必要性に対する認識不足や、人材・予算等の十分なリソース確保が困難といった課題があることから、政府・業界団体・支援組織等が連携して行ってきた「自助」、「共助」、「公助」を組み合わせた施策を一層強化する必要がある。

中小企業等の「自助」を促す取組としては、サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の活用促進に向けたガイドライン等の整備・規程類のひな形の提示に加え、中小企業が身近に感じられる事例や防止策の発信等を行う。

サプライチェーン上の主体同士の「共助」を促す取組としては、サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の仕組みの整備と普及促進、地域で自主的に行われるサイバーセキュリティ啓発活動が活発ではない地域における先導主体の発掘・育成や、地域金融機関、士業といった地域に根付いた主体との連携等の促進、中小企業等を含むサプライチェーン全体のサイバーセキュリティ強化を目的として設立された産業界主導のコンソーシアムを通じた普及展開活動の強化、サイバー関連情報の発信・共有等を行う。

それでもなお十分な対応が難しい中小企業等に対しては、サイバーセキュリティお助け隊サービスの利用改善に向けた見直し、セキュリティの外部専門家による支援を容易に探索・依頼できるような仕組みの整備・活用促進等を通じた「公助」を推進する。また、基幹インフラ事業者等のサプライチェーンに属する中小企業等からテレメトリ情報[48]を収集・統合・分析し、サイバー攻撃検知情報等、対策の強化に資する有用な情報を還元する「集団的防御」の枠組みの導入を進める。こうした取組により、サプライチェーン全体を支える中小企業等のサイバーセキュリティ対策を支援する。

（4） 全員参加によるサイバーセキュリティの向上

個人・中小企業を含むあらゆる主体を標的としたサイバー攻撃リスクが増加している状況の下、国民一人一人がサイバーセキュリティに対する意識・理解を深め、基本的な取組や対策を平時から自発的に行うことは、各個人の被害の低減につながるだけでなく、国や企業等の講ずるセキュリティに関する対策・対応との相乗効果をもたらし、社会全体のサイバーセキュリティ及びレジリエンスの向上にもつながることが期待される。

[48] テレメトリ情報とは、システムの稼働状況やイベント（不正アクセス等）のログ等の形で収集されたデータであって、監視・分析等のために遠隔地に送信されたもの。

特に、個人レベルではシニア層や若年層へサイバー脅威の影響が拡大し、組織レベルでは規模の小さい企業・組織においてセキュリティ対策のリソース不足といった課題を抱えている。従前より、国、地方公共団体、民間団体を含めた様々なレベルの組織が普及啓発に取り組んできているが、各種の普及啓発が行き届きにくいことに留意しつつ、引き続き、シニア層や若年層、中小企業を重点的な訴求対象として、具体的なセキュリティ対策を理解し実際に行動できるよう、それぞれのニーズや背景に沿って効果的な普及啓発・情報発信に取り組む必要がある。

これまで国は、ウェブサイトやSNSでの情報発信、講習会等の開催、ハンドブック・教材等のコンテンツの整備のほか、サイバーセキュリティ月間の取組を推進し、関係者が連携・協働する仕組みを下支えしてきた。国は、引き続きこの役割を担いつつ、環境や多様なニーズに合わせて各コンテンツを適切にアップデートし、より広くその情報が届くように関係者との連携を拡大・強化していく。その際、様々な主体の対策や行動が促進されるように、厳しさを増すサイバー空間を取り巻く情勢等に関する情報発信も念頭に置く。

また、情報教育の重要性は一層高まってきており、初等中等教育段階においても、GIGAスクール構想の推進に伴って、学校教育における１人１台端末等のデジタル学習基盤の活用が進んでいる。GIGAスクール構想の推進に当たっては、教師のICT活用指導力の充実を図るとともに、学習指導要領に基づき、学習の基盤となる「情報活用能力」の育成を図るため、児童生徒に対する情報セキュリティを含む情報教育の充実[49]に取り組む。また、インターネット等を取り巻く最新の状況を踏まえつつ、青少年がインターネットを適切に利用できるようにするための普及啓発等[50]に取り組む。

さらに、国民に広く利用されているIoT機器については、各主体が適切な対策を講じられるよう、ユーザーやベンダーに対し機器の設定不備や脆弱性について注意喚起や助言、情報提供等を行い[51]、関係者が一丸となってサイバーセキュリティの確保に取り組む。

産学官民の多様な主体においては、各主体の活動が相乗効果を生み、適切な知識・行動が広がっていくよう、積極的に連携・協働しつつ、普及啓発・情報発信を実施することが望まれる。

これらの取組を関係者が連携して着実に推進するとともに、その取組状況や効果を継続的に調査・確認し、改善に取り組む必要がある。くわえて、重点的な訴求対象や情報発信の方法、内容等については、環境の変化に応じ、随時見直しを行っていく。

（５） サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保

サイバー空間が、あらゆる主体が参画する公共空間へと進化していることを踏まえ、実空間と変わらぬ安全・安心を確保するため、国は、暗号資産、SNS等のサイバー空間の匿名性を悪用する犯罪者や犯罪者グループ、トレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等に対する摘発を引き続き推進する。

また、重大サイバー事案[52]の対処に必要な情報の収集、整理及び総合的又は事案横断的な分析等を強力に推進するとともに、AI 等を悪用した犯罪やランサムウェア等の高度な

[49] 情報モラル教育ポータルサイト（https://www.mext.go.jp/zyoukatsu/moral/index.html）
[50] 青少年を取り巻く有害環境対策に向けて（https://www.mext.go.jp/a_menu/sports/ikusei/taisaku/index.htm）
[51] 例えば、NOTICEプロジェクト（https://notice.go.jp/）
[52] 警察法（昭和29年法律第162号）第５条第４項第６号ハに規定する重大サイバー事案をいう。

情報通信技術を用いた犯罪に対処できるよう、捜査能力・技術力の向上に取り組む。

さらに、犯罪捜査等の過程で判明した犯罪に悪用されるリスクの高いインフラや技術に係る情報を活用し、事業者への働きかけ等を行うことにより、官民が連携してサイバー空間の犯罪インフラ化を防ぐほか、情報の共有・分析、被害の防止、人材教育等の観点から、産学官連携の枠組みを活用するなどしたサイバー犯罪対策を推進するとともに、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。

あわせて、高度な情報通信技術を用いた犯罪に対処するため、最新の電子機器や不正プログラムの解析のための技術力の向上、サイバー空間の脅威の予兆把握や脅威の技術的な解明のための総合的な分析を高度化すること等、情報技術の解析に関する態勢を強化する。

こうした取組に加え、国境を越えて敢行されるサイバー事案に適切に対処するため、国は、諸外国における取組状況等を参考にしつつ、関連事業者との協力や外国関係機関との国際連携等必要な取組を推進する。

３．　我が国のサイバー対応能力を支える人材･技術に係るエコシステム形成

ここまで述べてきた、深刻化するサイバー脅威に対する多様な手段による防御・抑止や、幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上を具現化し、我が国のサイバーセキュリティ水準を世界でも高いレベルのものに押し上げるためには、それを支える人材と技術を我が国として確保する必要がある。

しかしながら、我が国では、その人材の不足が長らく指摘されている。戦略的にサイバーセキュリティ人材を育成・確保しなければ、人材不足からサイバーセキュリティの確保が一層困難となる事態も懸念される。

また、我が国は、デジタル技術・産業そのものも相当程度海外に依存しており、サイバーセキュリティ分野も同様である。安全保障の観点からも、我が国に基盤を持つ形での国内産業の育成や、技術力・開発力の向上等を通じた自律性の確保が求められる。

さらに、AI や量子技術等の技術革新が、サイバーセキュリティ分野に利活用されることへの期待とともに、AI の安全性やサイバー攻撃への悪用、量子計算機技術の進展に伴う既存の公開鍵暗号の安全性低下・危殆化等、リスクになることも指摘されている。

人材の育成・確保に関しては、サイバーセキュリティ人材フレームワークを軸とした人材の裾野拡大と、専門知識や実践スキルを備えた高度人材の育成・確保に取り組む。

また、我が国の対応能力の基礎となるサイバーセキュリティ関連技術について、サイバー分野における官側のニーズを踏まえた、研究開発・開発支援・実証の実施・拡充や、それらを通じた技術情報等の活用、スタートアップ支援等を通じて、我が国におけるサイバーセキュリティ産業の育成を進める。

さらに、AI や量子技術等の先端技術については、我が国として、先手先手の対応と対策を打っていかなければならず、サイバーセキュリティ分野に与えるメリットやリスクに対して、的確な対応を行うべく、国も必要な環境整備を積極的に行っていく。

産学官連携を通じ、必要な投資等を促進し、サイバー空間を支える人材、技術のエコシステムを形成することで、我が国のサイバー対応能力を支える技術・人材の確保に関する基盤を形成・維持し、サイバーセキュリティ分野において過度に海外へ依存することなく安全保障のリスクを低減するとともに、新たな技術革新がもたらすサイバーセキュリティ分野の変革へ備えた対応が行える体制を構築していく。

（１） 効率的・効果的な人材の育成・確保

経済社会のデジタル化が進展する中で、サイバー攻撃は一層複雑化・巧妙化の一途を辿り、あらゆる分野でサイバーセキュリティを担う人材の確保・育成が急務となっている。このため、人材フレームワークを軸に、様々な施策を有機的に連携させながら効率的・効果的な人材育成を進める。

① 人材フレームワークの整備と効果的な運用

サイバーセキュリティ分野における人材の確保・育成を効果的に推進するためには、多様な職務ごとに、必要な知識・スキル等を体系的に整理した人材フレームワークを速やかに策定し、社会の様々な場面で活用されることが重要である。これにより、企業や

行政機関、大学・教育機関等がサイバーセキュリティ人材像の共通理解の下、より効果的かつ計画的な育成や採用等が可能となる。

フレームワーク策定に当たっては、我が国の官民における対処体制を念頭に実用性の高い内容とした上で、国内外の既存フレームワークや職業分類等との整合を図ることで、人材が国内外を問わず活躍できる環境の整備を目指す。

フレームワークの整備後は、その人材定義に基づき、人材の需要・供給状況や教育・訓練機関の情報を網羅的かつ一元的に可視化し、国内の人材動向を俯瞰できる仕組みづくりのために、官民協働して取り組む。これにより、キャリアパスを可視化し、人材を活用しようとする様々な組織における採用・配置等の場面を通じ、人材のマッチングやキャリア形成支援の質と効果を一層向上させていく。

様々な主体によって行われる教育・訓練について、フレームワークとの関連付けを強化する。具体的には、資格試験の合格や実践的演習の修了等といった成果と、フレームワークにおける人材像・レベルとの関連付けを推進し、参加者のスキルの可視化を促進できる仕組みとするとともに、教育・訓練のカリキュラム設計にも活用する。政府においては、政府デジタル人材のスキル認定制度と連携を図るなど、フレームワークを基盤として適切な評価制度の整備や人材の適正配置を促進する。

これらの取組を通じて、多様な人材が社会で必要とされる場面で力を発揮する環境を整えることで、様々な現場で得られた知見や経験が人材を通じて有機的に循環することになり、社会全体のセキュリティ水準の持続的強化にもつながる。

② サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実

我が国では、依然として専門知識や実践スキルを備えたサイバーセキュリティ人材の不足が指摘されている。一方、官民において資格制度や研修・演習、学び直しの機会提供等の取組は進展しており、この潮流を加速させ、「質」と「量」の両面で人材の確保・育成を加速させることが重要である。

初等中等教育段階から高等教育、職業訓練、社会人の能力開発、高度専門人材の育成に至るまで、体系的かつ継続的な学びの環境整備が求められる中、基礎的素養（情報リテラシー）から高度な専門性まで段階的に習得できる場の整備を図り、産学官が連携を強化して実践的スキルや最新知見の学習機会を確保する。

具体的には、「数理・データサイエンス・AI 教育プログラム認定制度」を通じた大学や高等専門学校におけるサイバーセキュリティを含む数理・データサイエンス・AI 教育の強化や、「セキュリティ・キャンプ」等の若年層を対象とした高度な技術教育プログラムの推進を図る。若手技術者には、最先端のセキュリティ技術・製品開発に関するカリキュラムを提供し、応用力や実務スキルの習得を支援する。重要インフラ事業者等に向けては、「CYDER」、「CYROP[53]」及び「中核人材育成プログラム」等の対処能力向上に資する実践的な演習や演習基盤の提供、トレーニングの機会等を促進し、多様な学びの場を体系的に整備・拡充して、対象者が段階的に活用できる環境を整える。専門的なセキュリティスキルを有していない人材についても、組織内外のセキュリティの専門家と

[53] 分野に応じた実践的演習を容易に開発・実施可能とする NICT の演習基盤。

協働する上で必要な知識を習得したプラス・セキュリティ人材[54]となれるような学習機会の充実化を図る。また、国家資格である情報処理安全確保支援士については、資格更新時の負担軽減を図りつつ、中小企業のセキュリティ対策支援を含め、活用促進に向けた取組を進めることにより人数の拡大を目指す。さらに、実践的な課題解決能力を養成し次世代人材の早期発掘や国際的な人的ネットワーク形成にも資するCTF(Capture The Flag)について、人材育成上の効果も踏まえ活用する。

このような多様な学びの取組が、人材フレームワークを介して有機的に連携することで、学びの機会が継続的に提供され、それらを通じて得た知識・技能がキャリア形成や活躍の場につながるよう、各種教育・訓練制度を俯瞰しながら、不断の改善を進める。

（２） 新たな技術・サービスを生み出すためのエコシステムの形成

サイバーセキュリティ市場は拡大傾向にあるものの、我が国の事業者の供給能力や、製品を開発するトップ人材等の絶対数、産学官の連携は十分とは言えない。

サイバーセキュリティ分野において、我が国の対応能力を向上させるためにも、海外の技術やサービスに過度に依存することなく、国内において、新たな技術及びサービスの研究開発、実証等を活性化させ、早期の社会実装により、分析力・開発力を向上させるなど、国産技術・サービスを核とした、技術、人材を育成する好循環のエコシステムを形成していく必要がある。

こうしたエコシステムを形成していくため、脅威に関する情報収集・分析に不可欠であり、我が国の対応能力の基礎となるサイバーセキュリティ関連技術について、官のニーズを踏まえて、研究開発・開発支援・実証の実施・拡充及びそれらを通じた一次情報を含む技術情報等の活用等や、スタートアップ支援等を通じた政府機関等による積極的な活用等を進めるほか、国の研究機関等が有するデータや演習基盤の活用による若手人材や各産業分野における専門人材の育成等により、官民双方の分析力・開発力の向上、早期の社会実装及び国内産業の育成を推進する。

研究開発に関しては、政府は、国際社会において我が国が確固たる地位確保を続けるために不可欠な要素となる先端的な重要技術について、サイバーセキュリティ分野も含め、民生利用のみならず公的利用につながる研究開発及びその成果活用を推進している。こうした取組を含め、政府として、企業や研究機関等とも積極的に連携し、基礎研究を含むサイバーセキュリティ分野の技術開発、社会実装や国際標準化に向けた取組を引き続き推進していく。

また、技術情報等の活用等に関しては、例えば、我が国独自のセンサー（ソフトウェア）によるサイバー攻撃検知システムとして構築した CYXROSS を政府機関等へ導入することでサイバー脅威情報の収集・分析を強化するとともに、これらで得られた技術・情報・ノウハウを政府部内にとどめることなく、適切な情報保全の下で民間に広く開放するなどにより、国産セキュリティ技術の開発基盤を強化するための取組を進める。

さらに、サイバーセキュリティ産業の育成に関しては、政府機関等による有望なスタートアップ等の製品・サービスの試行的な活用や、有望な技術・事業を発掘するための懸賞

[54] プラス・セキュリティ人材とは、経営層やDXを推進するマネジメント人材層等、ITやセキュリティに関する専門知識や業務経験を必ずしも有していない場合にも、社内外のセキュリティ専門家と協働するに当たって必要な知識として、時宜に応じてプラスして習得すべき知識（「プラス・セキュリティ知識」）を補充している人材を指す。

金型助成事業の活用に加え、サイバーセキュリティサービス提供事業者が正当に評価される仕組みの整備や、我が国のサイバーセキュリティ製品・サービス提供事業者の海外進出等に資する施策を推進・検討し、我が国から有望なサイバーセキュリティ製品・サービスが次々に創出されるための環境を形成していく。

なお、こうした取組については、我が国の国際競争力の確保や、安全保障上の懸念が生じないことを前提として、必要に応じ、国際連携の下、推進していく。

（３） 先端技術に対する対応・取組

生成 AI を始めとした AI 技術の急速な進展によって、我が国は不正アクセスや詐欺を始めとするサイバー犯罪の巧妙化等の新たな脅威に直面している。また、AI の更なる活用・普及が見込まれる中、AI に対する攻撃が、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。

また、量子計算機技術の進展に伴う、現在広く使われている公開鍵暗号の安全性の低下・危殆化の懸念など、多岐にわたる課題への対応が必要な状況となっている。

上記（２）で述べたサイバーセキュリティ分野の技術開発等の取組の推進に加え、先端技術がサイバーセキュリティや安全保障等にもたらす影響を踏まえ、デジタル分野の技術革新に適時的確な対応を行えるよう、必要な取組を推進する。

なお、サイバーセキュリティに大きな影響を及ぼす新たな技術革新は、予測できない形で今後新たに発生する可能性があることを踏まえ、本戦略に例示されている技術以外においても、動向を注視の上、必要な対応を柔軟に実施する。

① AI 技術の進展及び普及に伴う対応・取組

AI 技術の進展と普及は、サイバーセキュリティ分野においても大きなインパクトを与えている。具体的には、AI に係る安全性確保（Security for AI）、AI を活用したサイバーセキュリティ確保（AI for Security）、AI を悪用したサイバー攻撃への対処の３つの観点があると考えられる。

これらの観点について、AI がサイバーセキュリティにもたらすメリットを最大限に享受しつつ、負の側面を最小化するために、国際的な動向及び技術の進展、サイバー攻撃の動向等を踏まえ、研究開発、ガイドラインの整備等のルール形成、社会実装、人材育成等の様々なアプローチを総合的に推進する。その際、AI への対応に関し、先進的な国々の後塵を拝することにならないように留意する。

AI に係る安全性確保（Security for AI）に関しては、AI に対する多様な種類の攻撃に柔軟に対応できるよう、引き続き技術力確保のための取組やガイドライン等の策定、国際協調等の取組を推進する。具体的には、AI セーフティ・インスティテュート（AISI）等と連携し、国際的な動向も踏まえ、開発・運用等に係るガイドラインの策定・改定や周知・浸透のほか、海外機関との連携を含め、AI に対する攻撃や信頼できる AI に係る研究開発等、サイバーセキュリティの確保に係る取組を推進する。また、2023 年 G7 議長国として我が国が立ち上げた広島 AI プロセスに関して、国内外においてサイバーセキュリティも含めた AI ガバナンスの確保を図る観点から、これを推進する。

さらに、政府機関等において、生成 AI の調達・利活用に係るガイドラインを踏まえ、

AI の利活用とリスク管理の両立を図った上で、サイバーセキュリティ上の懸念への対応を含めた AI の安全性を確保した形で、AI の利活用を推進する。

AI を活用したサイバーセキュリティ確保（AI for Security）に関しては、サイバー攻撃の質・量両面での増大に対応し、膨大なデータの処理や、高度な分析が求められる中、政府は、関係主体と連携しつつ、AI を活用したサイバー攻撃インフラの検知や関連情報の分析の精緻化・迅速化等を推進する。

AI を悪用したサイバー攻撃への対処に関しては、研究開発等により、AI により一層脅威が高まると予想されるサイバー攻撃の被害の防止に向けた取組を推進する。

あわせて、AI とサイバーセキュリティの両方の専門性を兼ね備えた人材の発掘・育成に向けた取組も推進する。

AI 技術とサイバーセキュリティは、安全保障面でも重要であるが、海外への依存が進んでいる。したがって、サイバーセキュリティ分野における AI に係る取組は、我が国を基盤とした研究開発や社会実装の推進、AI 開発資源の確保等の取組や、サプライチェーン・リスク対策等、AI 分野における安全保障や我が国の産業育成に係る様々な取組と緊密に連携を取りながら推進していくことが重要である。

また、これらの AI に関する取組は、人工知能関連技術の研究開発及び活用の推進に関する法律（令和７年法律第 53 号）に基づき、人工知能戦略本部において策定される人工知能基本計画を踏まえた上で推進する。

② 量子技術の進展に伴う対応・取組

量子計算機技術については、その進展に伴い、現在広く使われている公開鍵暗号の安全性の低下・危殆化が懸念されている。このような中で、米国や欧州連合（EU）等の諸外国においては耐量子計算機暗号（PQC）への移行についての方針をそれぞれ公表しており、その多くが 2035 年までを期限として進めている。サイバー空間の安全性・信頼性は、情報の秘匿や改ざんの防止、認証等のために用いられる暗号技術の基盤の上で成立しており、国際連携等の観点を踏まえれば、我が国における移行が遅れた場合、サイバーセキュリティや安全保障上の支障も懸念される。我が国のサイバーセキュリティの確保等のため、政府機関等における PQC への移行について、原則として、2035 年までに行うことを目指し[55]、政府機関等における暗号技術の利用状況等も踏まえ、関係府省庁の連携の下、2026 年度に工程表（ロードマップ）を策定し、我が国における円滑な移行を推進していく。

その上で、PQC への移行については、政府機関等に限るものではなく、重要インフラ事業者等や民間事業者等においても考慮しなければならない課題であるため、関係府省庁の連携の下、必要な対応について検討を進め、円滑な移行を後押ししていく。

量子暗号通信（QKD）について、諸外国における社会実装に向けた取組が加速していることを踏まえ、我が国においても、サイバーセキュリティ確保、国際競争力の強化等のため、テストベッド（実証基盤）の広域化・高度化、ユースケースやビジネスモデルの創出・実証等、2030 年頃の QKD の社会実装に向けた取組を加速する。

[55] ただし、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを検討し、適切に判断する必要がある。例えば、特に機微な情報や保護期間が非常に長期となることが想定されている情報等を扱う場合等においては、より早期に移行を行うことも含め、情報システムごとに適切に検討を行うこととする。

Ⅳ. 本戦略の推進体制

本戦略に基づく我が国のサイバーセキュリティ政策の推進に当たっては、これまでにも増して、政府一体となった推進体制が必要である。改正基本法に基づき、戦略本部は、内閣総理大臣を本部長とし、全ての国務大臣で構成される新たな組織に改組された。本戦略に基づく取組が、我が国の安全保障の確保やデジタル庁を司令塔とするデジタル改革に寄与するとともに、公的機関が限られたリソースを有効活用しつつその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図っていく。

あわせて、内閣官房に内閣サイバー官を置くとともに、サイバー安全保障も含め、官民を通じたサイバーセキュリティの確保に関する司令塔として、国家サイバー統括室が設置された。国家サイバー統括室は、戦略本部の事務局として、重要インフラ・基幹インフラ所管省庁及びアクセス・無害化措置実施省庁を含め、各府省庁間の総合調整の主導的役割を担う。特に、サイバー安全保障に係る取組に関しては、国家安全保障局と緊密に連携しつつ、同局次長を併任する[56]内閣サイバー官が掌理する国家サイバー統括室が、司令塔組織として総合調整を強力に行い対応をしていく。また、必要な場合は、国家安全保障会議で議論・決定を行う。

その上で、各府省庁は、本戦略に基づき施策を推進するとともに、サイバー空間を取り巻く状況の動向を踏まえ、一層の効果的な施策の在り方を見直し、対応していく。あわせて、施策の推進のため、所要の体制等の整備・強化等に努めていく。

また、本戦略に基づく施策を推進するに当たって、官民連携及び国際連携は欠かすことができないものである。国家サイバー統括室はもちろんのこと、関連府省庁は、積極的に官民連携及び国際連携を推進し、施策の実効性を高めていく。くわえて、国民・事業者、国際社会に対して、我が国の取組への理解と協力が得られるよう、各府省庁は連携して、本戦略、関係する取組やその効果を国内外の関係者に積極的に発信する。

今後、戦略本部は、本戦略を的確に実施するため、各種戦略等との整合性も図りつつ、各年度の年次計画を作成し、その施策の進捗状況を検証して年次報告として取りまとめ、次年度の年次計画へ反映する。また、施策の進捗状況の検証に関しては、従前より実施している政府機関等の監査を通じた政府のセキュリティ施策の取組に関する評価に加え、改正基本法に基づき戦略本部の事務として位置付けられた重要インフラ統一基準に基づく取組の評価や、政府機関等のサイバーセキュリティの確保の状況の評価も実施し、政府機関等や重要インフラ事業者等のセキュリティ対策の着実な改善につなげる。

さらに、サイバーセキュリティに関する法令を含む制度に関しても、サイバー対処能力強化法等の施行状況、本戦略やそれに基づく施策の実施状況や評価、サイバーセキュリティを取り巻く環境の変化等を踏まえ、不断の見直しを行う。

なお、本戦略は策定からおおむね５年間に実施すべき諸施策の目標や実施方針を示すものであるが、本戦略に掲げられていない施策の機動的な実施を妨げるものではない。その上で、我が国を取り巻く環境や国際情勢、技術革新による社会経済構造等の変化、そして関係する各種戦略等の動向も踏まえ、必要に応じて本戦略の点検・見直しを行い、時宜に応じて改定も検討する。

---

[56] 内閣法（昭和 22 年法律第５号）第 16 条第７項