参考資料

サイバーセキュリティ戦略（令和3年9月28日閣議決定）【抜粋】

３　サイバー空間をとりまく課題認識

本戦略の策定に当たっては、サイバー空間がもたらす恩恵のみならず、この空間をとりまく変化やリスク（脅威、脆弱性いずれの観点も含む。）を的確に認識し、デジタル改革のビジョンである「一人ひとりのニーズにあ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」の実現に向けて、これら不確実性をできる限り制御していくアプローチが重要である。

サイバー空間そのものは、デジタルサービスが社会に定着していきサイバー空間に参画する層が増加をしていく過程で「量的」に拡大するとともに、取り扱えるデータ量の増大やIoT、AI技術、モビリティ変革、AR/VR技術をはじめとした最新技術の活用した新たなデジタルサービスの普及、「ニューノーマル」とも呼ばれる新しい生活様式の定着等を通じ、実現し得る価値の「質的」な多様化や、実空間との接点の「面的」な拡大が進んでいる。

これらが同時かつ相互影響的に進展する中で、サイバー空間が有する性質も変容しつつある。地域や老若男女問わず、全国民が参画し、自律的な社会経済活動が営まれる重要かつ公共性の高い場としての位置付け、すなわち、サイバー空間の「公共空間化」が進展するとともに、サイバー空間において提供される多様なサービスは、クラウドサービスの普及やサプライチェーンの複雑化等に伴い、サイバー空間内やサイバーとフィジカルの垣根を越えた主体間の「相互連関・連鎖性」が一層深化していくことが想定される。

一方で、サイバー空間におけるデジタル技術の利用は、新たな課題も提示する。不適切に悪意をもって利用されれば、国家間における分断や危険を増大させ、人権を阻害し、不公平を拡大し得ることが指摘されている。サイバー空間の変容は、従来では想定し得なかったリスクも同様に拡大させることも想定され、さらに、コロナ禍等により不連続な形で起こる変化は、予期しない形でリスクを顕在化させるおそれがある。サイバー空間が公共空間へと変貌を遂げつつある一方で、このような状況により、国民がサイバー空間に対する不安感を完全に払拭できていないことも事実である。

これらを念頭に、「自由、公正かつ安全なサイバー空間」を確保するためには、足元で起きている変化、又は近未来に起こり得る変化によって生じるリスクを適切に把握した上で、取り組むべき課題を明確化し、政策を推進していく必要がある。また、サイバー空間ではサービス提供の担い手は数年単位で入れ替わり、サイバーセキュリティの確保に大きな役割を果たす主体も変わり得ることから、中長期的にはその前提も大きく変わり得ることも同時に意識することが重要である。

以下では、経済社会をとりまく環境変化、国際情勢のそれぞれから、考慮すべきリスク要因を整理し、また、それらが具体的にどのように顕在化しているかについて示していく。

３．１　環境変化からみたリスク

我が国経済社会をとりまく環境変化は、さまざまな恩恵をもたらし得る一方で、それに伴うリスクも表裏一体に拡大し得る。その動向について、脅威、そして経済社会が抱える脆弱性というそれぞれの観点に分けて示す。

（１）脅威の観点

新たな技術の活用や、いわゆる「ニューノーマル」の定着等を通じ、新たなデジタルサービスが次々と生み出され、人々の生活に浸透していくということは、自らの生命、身体、財産に関わる情報を、量的にも質的にも、これまで以上にサイバー空間の場に委ねることを意味する。これらのデータが価値の源泉や利便性の向上に繋がることを通じて人々に対し恩恵を与えると同時に、そうしたデータは今後一層、攻撃者にとって、サイバー攻撃の対象となる誘引性が増すこととなり、結果としてサイバー攻撃の組織化・洗練化が、より計画的・大規模に行われる可能性がある。

また、このようにデジタルサービスが人々の生活に浸透していくことに伴い、デジタルサービス連携の間隙を突いたサイバー攻撃がみられるなど、攻撃手法も多様に変化・高度化していくことが考えられる。

加えて、技術革新の果実を攻撃側が活用することで脅威が増大する可能性も考えられる。例えば、AI 技術がサイバー攻撃に悪用されれば、人間の能力や技術的能力を超える速度と規模でサイバー攻撃が行われることもあり得、中長期的には、人間の制御によらない自律的攻撃の可能性も視野に入れなければならない。

（２）経済社会が抱える脆弱性の観点

経済社会全体でみれば、デジタル化の進展により、これまでサイバー空間とは繋がりのなかった様々な業種・業態の企業や、若年層・高齢者を含めた個人までもが不可避的にサイバー空間に参画することとなる。サイバー空間がこれまで以上に誰もが安心して参画できる空間となることへの期待がより一層高まることとは裏腹に、サイバーセキュリティに関するリテラシーの差異や人材不足・偏在等が、攻撃者に狙われ得る弱点となる可能性がある。

また、企業組織や技術分野における人材不足は、サイバーセキュリティに係る製品・サービス、技術を、過度に海外に依存する状況を招き得る。リテラシー不足は、機器・サービスの誤用等を通じ、新たな脆弱性を経済社会に顕在化させる危険性もはらんでいる。

加えて、クラウドサービスの利用拡大や複雑かつグローバルなサプライチェーンを経由する製品・サービスの拡大・浸透、産業分野での IoT 機器の利用拡大（あらゆるモノがネットワークに接続されるようになること）や AI 技術の様々なシステムへの活用などにより、インシデントが発生した場合の経済社会活動への影響は、より広範に、多様な主体・場面に及ぶおそれがあり、それ故に解決に向けた困難性を増すと考えられる。

さらに、クラウドサービス利用の拡大は、テレワークの定着などとも相まって、従来の「境界型セキュリティ」の考え方の限界も顕在化させつつある。

３．２　国際情勢からみたリスク

サイバー空間は平素から、地政学的緊張を反映した国家間の競争の場の一部ともなっているが、サイバー攻撃が匿名性、非対称性、越境性という特性を有する中で、重要インフラの機能停止、国民情報や知的財産の窃取、民主プロセスへの干渉など国家の関与が疑われるものをはじめとする組織化・洗練化されたサイバー攻撃の脅威の増大がみられるなど、足元では、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。

経済社会のデジタル化が広範かつ急速に進展する中、こうしたサイバー攻撃の増大等は、国民の安全・安心、国家や民主主義の根幹を揺るがすような重大な事態を生じさせ、国家安全保障上の課題へと発展していくリスクをはらんでいる。サイバー攻撃者の秘匿、偽装等が巧妙化しているが、特に国家の関与が疑われるサイバー活動として、中国は軍事関連企業、先端技術保有企業等の情報窃取のため、ロシアは軍事的及び政治的目的の達成に向けて影響力を行使するため、サイバー攻撃等を行っているとみられている。また、北朝鮮においても政治目標の達成や外貨獲得のため、サイバー攻撃等を行っているとみられている。さらに、中国・ロシア・北朝鮮において、軍をはじめとする各種機関のサイバー能力の構築が引き続き行われているとみられている。

加えて、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する中、一部の国が主張するように、国家によるサイバー空間の管理・統制の強化が国際ルール等の潮流となれば、我が国の安全保障にも資する「自由、公正かつ安全なサイバー空間」や従うべき基本原則の確保が脅かされる。安全保障の裾野が経済・技術分野にも一層拡大する中で、技術覇権争いが顕在化し、また、国家によるデータ収集・管理・統制を強化する動きも見られる。

また、サイバー空間を構成するシステムのサプライチェーンの複雑化やグローバル化を通じ、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など、サイバー空間自体の信頼性や供給安定性に係るリスク（サプライチェーン・リスク）が顕在化している。

このように、サイバー攻撃の脅威に晒される対象の拡大とともに、その手段が組織化・洗練化され、サイバー空間の安定性が揺らぐ中で、個々の主体、あるいは一国のみで対応することが極めて困難な国際社会共通の切迫した課題となっており、まさに我が国が目指すべきグローバル規模での「自由、公正かつ安全なサイバー空間」の確保は危機に直面していると言えよう。

３．３　近年のサイバー空間における脅威の動向

以上で示したリスク要因は、近年のサイバー空間における脅威の動向をみても、明らかな傾向として表れている。

組織犯罪や国家の関与が疑われる攻撃が多く発生しており、海外では選挙に対する攻撃をはじめとする民主プロセスへの干渉や、サプライチェーンの弱点を悪用した大規模な攻撃、制御系システムを対象とした攻撃をはじめ広範な経済社会活動、ひいては国家安全保障に影響を与え得るインフラへの攻撃が猛威を奮っている。

また、テレワーク等の普及に伴い個々の端末経由又はVPN機器の脆弱性を悪用しネットワークに侵入されるケースや、クラウドサービスが攻撃の標的とされるケースが増加しているほか、ワクチンに関するニュースに関連したビジネスメール詐欺やフィッシングなどのコロナ禍に乗じたサイバー攻撃や、比較的対策が行き届きづらい海外拠点を経由した攻撃、匿名性の高いインフラを通じて行われる攻撃など、足元の環境変化をタイムリーに捉えたサイバー攻撃も現にみられている。

これらに加えて、ばらまき型攻撃が2020年に入り急増するなど、標的型攻撃の被害は引き続き止んでいないほか、データ復元に加え窃取したデータを公開しない見返りの金銭要求も行ういわゆる「二重の脅迫」を行うランサムウェア、匿名化技術や暗号技術の悪用による事後追跡の回避など、従来の脅威が複雑化・巧妙化している。背景として、マルウェアの提供や身代金の回収を組織的に行うエコシステムが成立し、悪意のある者が高度な技術を持たなくても簡単に攻撃を行える状況が指摘されている。

こうしたサイバー攻撃により、生産活動の一時停止、サービス障害、金銭被害、個人情報窃取、機密情報窃取など、経済社会活動、ひいては国家安全保障に大きな影響が生じ得る状況となっている。

４　目的達成のための施策 ～Cybersecurity for All～

４．１　経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity の推進～

４．１．３　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

（３）セキュリティ製品・サービスの信頼性確保

サイバーセキュリティに向けた自律的な取組が広がりを見せるためには、市場において提供されるセキュリティ製品・サービスが信頼の置けるものであることが前提である。また、今後は、サプライチェーン・リスクへの懸念に加え、オープン API や OSS の活用が一般的となったことで開発者自身もシステム全体のリスクを把握する困難性が高まっている中で、自社製品等の信頼性を企業内外に示す観点から、第三者による客観的な検証・評価への需要が拡大し、そうした需要に応えるビジネスが産業として一層重要になっていくと考えられる。こうした観点から、信頼性確保の基盤づくりに取り組み、ひいては先端技術・イノベーションの社会実装に係る取組と相まって、他国に過度に依存しない日本発の製品・サービスの育成に取り組む。

具体的には、セキュリティ製品・サービスの有効性検証を行う基盤整備や実環境における試行検証を通じてビジネスマッチングを促進するほか、一定の基準を満たすセキュリティサービスを審査・登録しリスト化する取組や当該サービスの政府機関における利用促進に取り組む。また、検証ビジネスの市場形成に向け、国としても、検証事業者の信頼性を可視化する取組を検討する。

（４）先端技術・イノベーションの社会実装

デジタル化が進展するにつれて、エビデンスが明確で組織内外への説明性の高い、又は自動化等を活用し効率的なセキュリティ対策が一層求められることとなる。こうした社会的要請に応える形で、産学連携が活発に行われるような産学官にわたるエコシステムの構築を推進し、オープンイノベーション活動を活性化していくことが急務である。

また、我が国におけるセキュリティ製品・サービスは海外に大きく依存している状態であり、製品・サービスの開発に必要なノウハウや知見の蓄積が困難となっている。

こうした状況を打破する取組の一環として、サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築し、安全保障の観点から情報管理に留意しつつ、産学官の結節点として、当該情報を産学官の様々な主体に効果的に共有する。この際、産学官が研究開発や製品開発等に利用しやすいものとなるよう、関係者との意見交換やコミュニティ形成を積極的に実施する。

このほか、IoT システム・サービス、サプライチェーン全体での活用に向けた基盤の開発・実証の取組について、様々な産業分野を念頭に置いた社会実装を促進する。

これら新技術の社会実装に向けた取組の一環として、政府機関における新技術の活用に向けた技術検討を促進する。さらに、国産セキュリティ製品・サービスのグローバル展開に向けて、国際標準化に向けた取組や海外展示会への出展支援等を引き続き推進する。

４．４　横断的施策

「経済社会の活力の向上及び持続的発展」、「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・安定及び我が国の安全保障」の 3 つの政策目標を達成するためには、その基盤として、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組んでいくことが重要である。

なお、「デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進」、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」、「安全保障の観点からの取組強化」という 3 つの方向性を意識して、取組推進を図る。

４．４．１　研究開発の推進

サイバーセキュリティ研究分野は、脅威に関する情報やユーザ等のニーズを踏まえ、実践的な研究開発を進めることが非常に重要な分野である。一方で、実践的な研究開発を有効に進めるためには、我が国においてその基盤となる研究開発の国際競争力が確保されていることや産学官エコシステムが築かれていることが大前提である。こうした基盤づくりに向けた中長期的観点からの取組と、それを基礎とした実践的な取組の双方の視点をあわせ持って取組を進めていく。

また、研究開発の推進に当たってはデジタル技術の進展に応じた観点も重要であり、中長期的な技術トレンドを視野に入れた対応を行う。

（１）研究開発の国際競争力の強化と産学官エコシステムの構築

サイバーセキュリティ研究分野は、様々な分野から研究者が流入すること等により、世界的に論文投稿数が急成長するとともに、国際共著・産学官連携論文などコラボレーションが活発である。今後、デジタル活用とサイバーセキュリティ対策の一体性が深くなる中、デジタル技術分野と相まって、重要な研究分野である。

我が国でもサイバーセキュリティ研究者が増えている一方、経済社会のデジタル化とそれに応じたサイバーセキュリティ対策及び技術に対する社会的要請が高まっていることから、その充実・発展・自給に向けて、中長期的観点から研究及び産学官連携を振興し、研究開発の国際競争力の強化と産学官にわたるエコシステムの構築に取り組んでいく。

具体的には、関係府省が提供する、科学的理解やイノベーションの源泉となるような研究及び産学官連携の振興施策の活用を促進し、研究コミュニティの自主的な発展努力と相まった、重点的な研究・産学官連携の強化を図る。これとあわせ、研究環境の充実等により、研究者が安心して研究に取り組める環境整備に努める。

産学官にわたるエコシステム構築が図られるためには、それぞれの主体の自主的な発展努力が必要不可欠であり、これらの取組状況についてフォローアップを行いながら、取組を推進していく。

（２）実践的な研究開発の推進

サプライチェーン・リスクの増大やサイバーセキュリティ自給、AI や IoT 等の進展による新たな脅威の発生可能性など、安全保障の観点を含め我が国をとりまく現下の課題認識に基づき、我が国において、以下の方向性で、サイバーセキュリティに係る実践的な研究開発を推進していく。

① サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備

不正なプログラムや回路が仕込まれていないことを確認するためのソフトウェア・ハードウェア両面の検証技術の研究開発・実用化を推進する。具体的には、IoT 機器等の信頼性を高度に検証するハイレベルな検証サービスの実証等を通じた包括的な検証基盤の構築や、5G に係る各構成要素におけるセキュリティを総合的かつ継続的に担保する仕組みの整備、チップの設計回路の解析や各種システム・サービスの挙動・動作の観測を通じた悪性機能を検出する技術や、セキュアな Society 5.0 の実現に向けた検証技術の研究開発及びその社会実装等を推進する。

また、これらの取組を踏まえ、国産技術の確保・育成のための取組や、政府調達における活用も視野に入れつつ、サプライチェーン全体の信頼性確保に向けた、ICT 機器・サービスのセキュリティの技術検証を行うための推進体制を、政府一体となって整備する。

② 国内産業の育成・発展に向けた支援策の推進

サイバーセキュリティ産業の育成・発展を目指し、製品・サービスを安心して利用するための有効性検証基盤や、中小企業のニーズに対応したビジネス創出など国内産業のビジネス環境を整備するとともに、シーズとニーズに係るビジネスマッチングを実施し、市場展開を促進する。

③ 攻撃把握・分析・共有基盤の強化

サイバー攻撃の巧妙化・複雑化・多様化や、IoT 機器の普及に伴う脆弱性拡大等のサイバー攻撃の脅威動向に適切に対処するため、AI 等の先端技術も活用しつつ、サイバー攻撃の観測・把握・分析技術や情報共有基盤を強化する。

具体的には、巧妙かつ複雑化したサイバー攻撃や今後本格普及する IoT 等への未知の脅威に対応するため、広域ダークネットや攻撃種別に柔軟に対応するハニーポット技術等を用いたサイバー攻撃観測技術の高度化や、AI 技術による攻撃挙動解析の自動化技術に係る研究開発を実施する。また、標的型攻撃の攻撃挙動の把握・解析やそのための迅速な対応を進めるために、サイバー攻撃誘引基盤の高度化、及びその活用の拡大を図り、標的型攻撃の具体的な挙動収集や未知の標的型攻撃等を迅速に検知・解析する技術等の研究開発を行う。加えて、脆弱な IoT 機器の確度の高い把握、及びそのセキュリティ対策のため、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャンのための研究開発を行う。このほか、サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築・共有する取組を推進する。

④ 暗号等の研究の推進

実用的で大規模な量子コンピュータが実現することによる既存の暗号技術の危殆化を想定しつつ、耐量子計算機暗号や量子暗号等に関する先進的な研究を推進し、安全性を確保するための基盤を確立する。また、IoT 等のリソースの限られたデバイスにおいても、安全な通信が可能となるよう、軽量な暗号技術を確立する。

具体的には、実用的で大規模な量子コンピュータの実現や IoT 等の普及、新たな暗号技術の動向等を踏まえ、暗号技術の安全性・信頼性確保や普及促進等に関する検討を継続的に実施するとともに、耐量子計算機暗号、軽量暗号等に関するガイドラインの作成に向けた検討を行う。また、盗聴や改ざんが極めて困難な量子暗号等を活用した量子情報通信ネットワーク技術や、量子暗号通信を超小型衛星に活用するための技術の確立に向けた研究開発を推進する。

本戦略の計画期間において、これら関係府省の取組を推進するとともに、研究及び産学官連携の振興に係る関係府省の取組を含め取組状況をフォローアップし、取組のマッピング等による点検と必要な再整理を行う。あわせて、研究開発の成果の普及や社会実装を推進するとともに、その一環として政府機関における我が国発の新技術の活用に向けて、関係府省による情報交換等を促進する。

（３）中長期的な技術トレンドを視野に入れた対応

Beyond 5G をはじめとするネットワーク技術の高度化など、デジタル技術の進展に応じ、中長期的な視点から技術トレンドを捉え研究開発を推進していくことが重要である。特に、AI 技術・量子技術をはじめとする先端技術の進展を見据えた対応が求められるところ、それぞれの技術進展に関し、以下のような状況認識に基づいて、取組を推進していく。

① AI 技術の進展を見据えた対応

AI 技術は、近年、加速度的に発展しており、世界の至るところでその応用が進むことにより、広範な産業領域や社会インフラなどに大きな影響を与えている。サイバーセキュリティとの関係では、AI を活用したサイバーセキュリティ対策、AI を使ったサイバー攻撃、AI そのものを守るセキュリティの 3 つの観点があると考えられる。

まず、AI を活用したサイバーセキュリティ対策（AI for Security）に関しては、実際に AI を活用したセキュリティ製品やサービスの商用化が進んでいる。国は、AI 技術に関する総合的な戦略等に基づき、AI を活用した民間のサイバー対策を引き続き後押しするとともに、予防、検知、対処の各フェーズにおいて AI を活用した高効率かつ精緻な対策技術の確立を推進していく。

また、AI を使ったサイバー攻撃に対処する観点から、攻撃者の防御側に対する非対称性をさらに拡げないためにも、「AI for Security」の取組は重要となる。その際、攻撃の視点から知見を得て、先手を打ってセキュリティ対策を高度化するプロアクティブな研究のアプローチが重要であると考えられる。

さらに、AI そのものを守るセキュリティ（Security for AI）では、AI のセキュリティ面での脆弱性がどのようなものかまだ十分に理解されていないと考えられるとこ

ろ、学術面では、例えば、機械学習の誤認識を誘発し得る敵対的サンプルの生成を試みる研究や、一方でその防御に関する研究も海外では多くなっている。我が国においても基礎的な研究を振興するとともに、5～10 年先に実現を目指す長期的取組として、引き続き技術課題の検討を進めていく。

② 量子技術の進展を見据えた対応

量子コンピュータの進展により、現代のインターネットセキュリティを支える公開鍵暗号技術が解読される可能性が生じ、国際的に耐量子計算機暗号に関する検討が進められている。我が国においても、耐量子計算機暗号等に関する先進的な研究を推進し、安全性を確保するための基盤を確立することとしている。

一方、耐量子計算機暗号においても危殆化のリスクがあるため、各国が安全保障にも関わる重大脅威との認識の下、原理的に安全性が確保される量子通信・暗号に関する研究開発を急速に進めている。我が国としても、量子技術に関する総合的な戦略に基づき、国及び国民の安全・安心の確保、産業競争力の強化等の観点から、重要な情報を安全に保管する手段として、機密性・完全性等を有し、かつ市場化を見据えて国際競争力の高い、量子通信・暗号に関する研究開発や、その事業化・標準化等に取り組んでいく。

以上のほか、Beyond 5G をはじめとした様々な技術トレンドを中長期的な視点から捉え、国として推進すべき技術課題の検討を不断に行っていく。