資料１

次期サイバーセキュリティ戦略（案）について

資料１－１　次期サイバーセキュリティ戦略（案）の概要

資料１－２　次期サイバーセキュリティ戦略（案）

資料１－３　サイバーセキュリティ戦略案の作成に際しての高度情報通信ネットワーク社会推進戦略本部意見

次期サイバーセキュリティ戦略の課題と方向性

資料１－１

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験 テレワーク、オンライン教育等の進展
- 厳しさを増す**安全保障**環境
- **SDGｓ**への デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**に向けた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
  サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
  攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映 **国家間競争**の場に 安全保障上の課題にも
- 不適切な利用は 国家分断、人権の阻害へ
- 官民の取組の 活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

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

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

経済社会の活力の向上及び持続的発展

課題認識と方向性　ー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 ー

- 本年9月には「デジタル庁」の設置が予定。デジタル化が大きく推進される絶好の機会。
  そのためにも、サイバー空間への信頼を醸成し、参加・コミットメントを得ることが重要。
- また、業務、製品・サービス等のデジタル化が進む中、サイバーセキュリティは企業価値に直結する営為に。
  「セキュリティ・バイ・デザイン」の重要性は一層増し、デジタル投資とセキュリティ対策の一体性は高まる。

⇨ デジタル化の進展とあわせて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進。

主な具体的施策

① 経営層の意識改革

→デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化・インセンティブ付けを行い、更なる取組を促進。

② 地域・中小企業におけるDX with Cybersecurityの推進

→地域のコミュニティの推進・発展、中小企業向けサービスの審査登録制度を通じ、デジタル化に当たって直面する知見や人材等の不足に対応。

③ サプライチェーン等の信頼性確保に向けた基盤づくり

→Society5.0に対応したフレームワーク等も踏まえ、各種取組を推進。

- サプライチェーン：　産業界主導のコンソーシアム
- データ流通　　：　データマネジメントの定義、「トラストサービス」によるデータ信頼性確保
- セキュリティ製品・サービス：　第三者検証サービスの普及
- 先端技術　　：　情報収集・蓄積・分析・提供等の共通基盤構築

④ 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

→情報教育推進の中、「デジタル活用支援」と連携して、各種取組を推進。

国民が安全で安心して暮らせるデジタル社会の実現

課題認識と方向性 － 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・安心確保 －

- サイバー空間の**公共空間化**、**相互連関・連鎖の深化**、**サイバー攻撃の組織化・洗練化**。

  国は様々な主体と連携しつつ、①自助・公助による**自律的なリスクマネジメントが講じられる環境づくり**と、②持ち得る手段の全てを活用した**包括的なサイバー防御の展開**等を通じて、**サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築**し、国全体のリスク低減、レジリエンス向上を図る。

主な具体的施策（１）国民・社会を守るためのサイバーセキュリティ環境の提供

① 安全・安心なサイバー空間の利用環境の構築

- サプライチェーン管理のためのガイドライン策定や産業界主導の取組、IoT、5G等の新技術実装に伴う安全確保
- 利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討

② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）

- 政府機関・重要インフラ事業者等向けにクラウド利用の際に考慮すべきセキュリティルール策定
- ISMAPの取組等の民間展開による一定のセキュリティが確保されたクラウド利用の促進
- 信頼性が高く、オープンかつ使いやすい高品質クラウドの整備の推進

③ サイバー犯罪への対策

- サイバー空間を悪用する犯罪者や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の摘発を推進し、実空間と変わらぬ安心・安全を確保
- 警察におけるサイバー事案対処体制の強化

④ 包括的なサイバー防御の展開

- サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化（対処官庁のリソース結集と連携強化、サイバーセキュリティ協議会等の関係機関との連携による官民連携・国際連携強化）
- 包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）

⑤ サイバー空間の信頼性確保に向けた取組

- 個人情報や知的財産を保有する主体への支援
- 経済安保の視点を踏まえたITシステム・サービスの信頼性確保（政府調達、重要なインフラ、国際海底ケーブル等）

国民が安全で安心して暮らせるデジタル社会の実現

主な具体的施策（２）デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

- デジタル庁が策定する国等の情報システム整備方針にサイバーセキュリティの基本的な方針も示し実装を推進。
- 情報と発信者の真正性等を保障する制度を企画立案し、普及を促進。ISMAP制度を運用し、民間利用の推奨。

主な具体的施策（３）経済社会基盤を支える各主体における取組

① 政府機関等

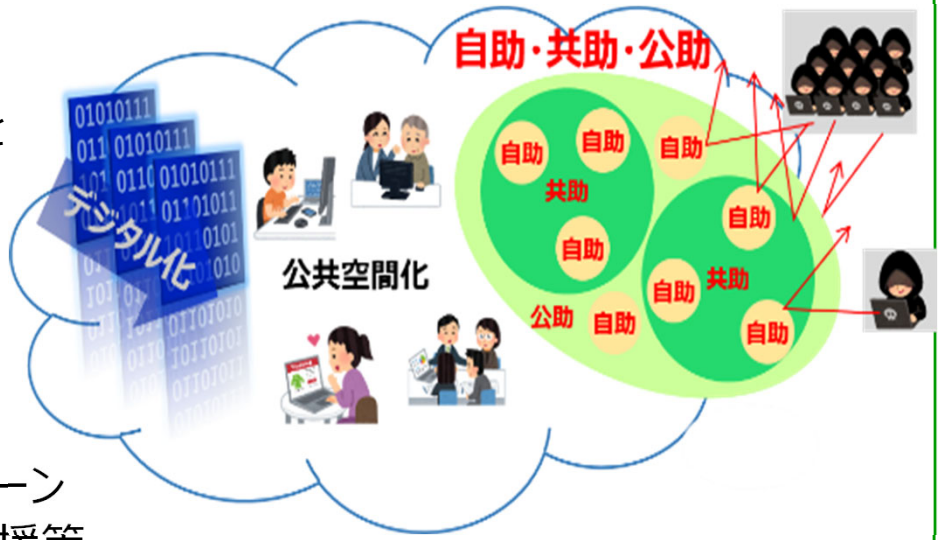
- 政府統一基準群に基づく対策の推進や監査・CSIRT訓練・GSOCによる監視等を通じた政府機関全体としてのセキュリティ水準の向上。
- クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能の強化。

② 重要インフラ

- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」を改定し、環境変化に対応した防護の強化や経営層のリーダーシップを推進。
- 地方公共団体情報システムの標準化や行政手続きのオンライン化等に対応したガイドラインの見直し等の諸制度整備。

③ 大学・教育研究機関等

- リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策を含む、先端情報を保有する大学等への対策強化支援等。



主な具体的施策（４）多様な主体による情報共有・連携と大規模サイバー攻撃事態等への対処体制強化

- 東京大会での対処態勢や運用により得た知見やノウハウを広く全国の事業者等に対する支援として積極活用。
- 平素から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化。

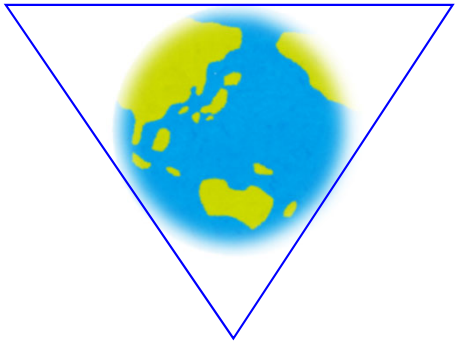
国際社会の平和・安定及び我が国の安全保障への寄与

課題認識と方向性　－ 安全保障の観点からの取組強化 －

- 我が国を取り巻く安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取等を企図したサイバー攻撃を行っているとみられている。
- 一方、同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められており、サイバー事案やサイバー空間に関する国際ルール等をめぐる対立等に対して同盟国・同志国等が連携して対抗している。
- 加えて、安全保障の裾野が経済・技術分野にも一層拡大している中で、サイバー空間に関する技術基盤やデータをめぐる争いに対しても、同盟国・同志国が連携して対抗し、「自由、公正かつ安全なサイバー空間」を確保するため、我が国の基本的な理念に沿った国際ルールを形成していく必要がある。

⇨ サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、以下を一層強化する。

「自由、公正かつ安全なサイバー空間」の確保



国際協力・連携

我が国の防御力・抑止力・状況把握力の向上

国際社会の平和・安定及び我が国の安全保障への寄与

主な具体的施策

① 自由・公正かつ安全なサイバー空間の確保

- サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）
  - 国際法の適用に関する議論・規範の実践の普及、サイバー犯罪に関する条約の普遍化等の推進
- サイバー空間におけるルール形成
  - 信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）や5Gセキュリティ等国際的な取組の進展を踏まえた我が国の基本理念に沿う国際ルールの策定

② 我が国の防御力・抑止力・状況把握力の強化

- サイバー攻撃に対する防御力の向上
  - 防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、自衛隊・米軍のインフラ防護の演習等の実施
  - 先端技術・防衛産業等のセキュリティ確保のための官民連携・情報共有等の強化
- サイバー攻撃に対する抑止力の向上
  - 相手方によるサイバー空間の利用を妨げる能力の活用や外交的手段・刑事訴追等を含めた対応の活用、日米同盟の維持・強化
- サイバー空間の状況把握力の強化
  - 全国的なネットワーク・技術部隊・人的情報を駆使したサイバー攻撃の更なる実態解明の推進

③ 国際協力・連携

- 知見の共有・政策調整
  - 米豪印やASEAN等同志国との省庁横断的・各省庁における国際連携の重層的な枠組みの強化
- サイバー事案等に係る国際連携の強化
  - 国際サイバー演習の主導等による国際的なプレゼンスの向上
- 能力構築支援
  - 「基本方針」*に基づく産学官連携や外交・安全保障を含めたASEANを含むインド太平洋地域における取組強化

*「サイバーセキュリティ分野における開発途上国に対する能力構築支援の基本方針」

横断的施策

DX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

● 上記の推進に向け、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組む。

1．研究開発の推進

産学官エコシステム構築とともに、それを基礎とした実践的な研究開発推進。
中長期的な技術トレンドも視野に対応。

(2)実践的な研究開発の推進

①サプライチェーンリスクへの対応
②国内産業の育成・発展
③攻撃把握・分析・共有基盤
④暗号等の研究の推進

(3)中長期的な技術トレンドを視野に入れた対応

①AI技術の進展
AI for Security
Security for AI

②量子技術の進展
耐量子計算機暗号の検討
量子通信・暗号

(1)国際競争力の強化 産学官エコシステムの構築

・研究・産学官連携振興施策の活用
・研究環境の充実　等

2．人材の確保、育成、活躍促進

「質」・「量」両面での官民の取組を一層継続・深化させつつ、環境変化に対応した取組の重点化。官民を行き来しキャリアを積める環境整備も。

(1)DX with Cybersecurity の推進

・「プラス・セキュリティ」知識を補充できる環境整備
・機能構築・人材流動に関するプラクティス普及　等
(xSIRT、副業・兼業等)

(2)巧妙化・複雑化する脅威への対処

・人材育成プログラムの強化
SecHack365 / CYDER / enPiT
ICSCoE中核人材育成プログラム 等
・人材育成共通基盤の構築
産学への開放
・資格制度活用に向けた取組 等

優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境の整備

(3)政府機関における取組

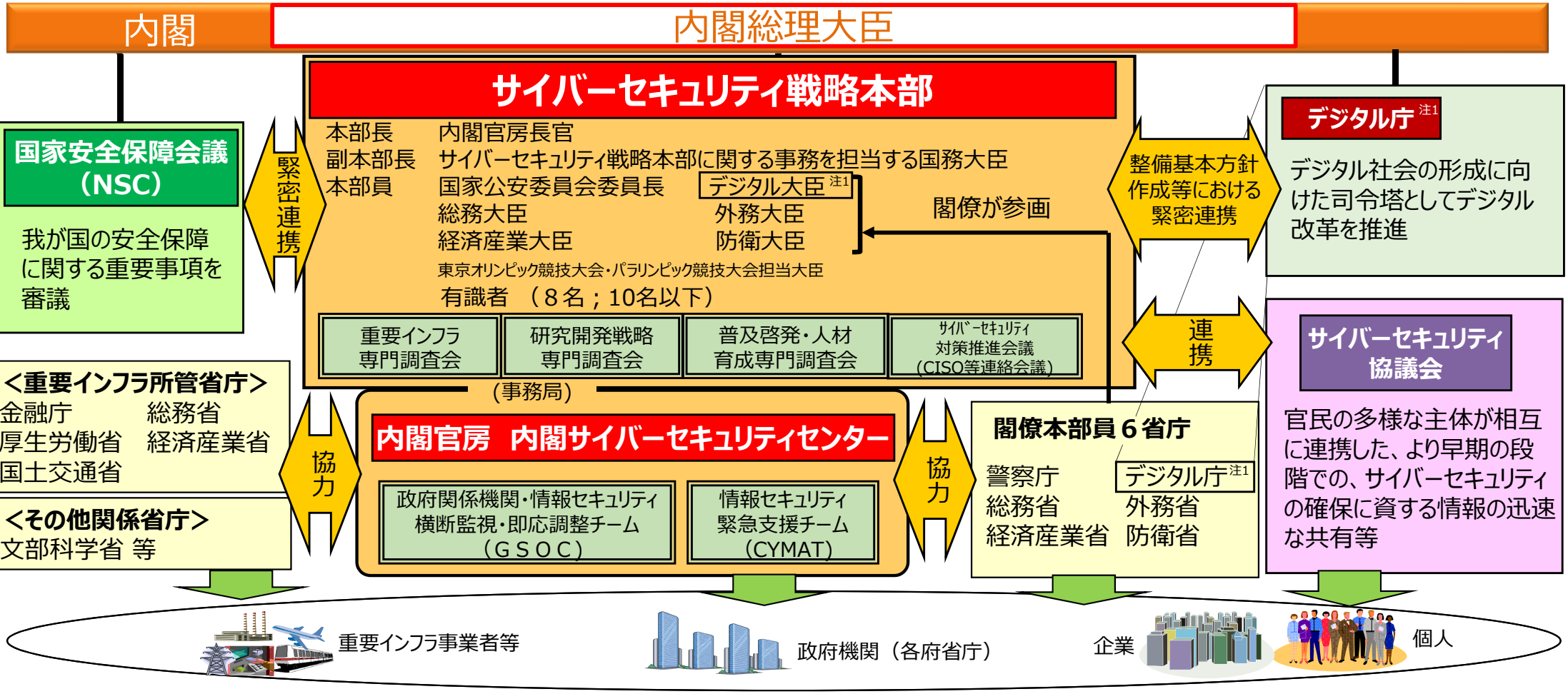
外部高度人材活用の仕組み強化
「デジタル区分」合格者の積極採用、研修の充実・強化　等

3．全員参加による協働、普及啓発

デジタル化推進を踏まえ、アクションプランの推進・改善、高齢者への対応を含め見直しの検討。

推進体制

- 我が国のサイバーセキュリティ政策により、自由、公正かつ安全なサイバー空間を確保するためには、政府一体となった推進体制が必要。デジタル庁が司令塔として推進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活用し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・連携強化を図る。
- 各主体に期待される具体的な対策につながるよう、また、国際協調の重要性を認識し、攻撃者に対する抑止の効果や各国政府に対する我が国の立場への理解を訴求するよう、NISCと関係省庁が連携して、本戦略を国内外の関係者に積極的に発信。
- 本部は、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備を行う。
- 年次報告・年次計画は、一体的に検討を行い、前年度の取組実績、評価及び次年度の取組を、戦略の事項に沿って、一連の流れを示すように整理。



（注1）デジタル社会形成基本法（令和３年法律第35号）、デジタル庁設置法（令和３年法律第36号）。（令和３年９月１日施行予定）

「次期サイバーセキュリティ戦略」（案）の構成

中長期的

1　2020年代を迎えた日本をとりまく時代認識

1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、東京大会に向けた取組の活用

2　本戦略における基本的な理念

2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」

2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3　サイバー空間をとりまく課題認識

環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策

＜3つの方向性＞（１）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
（２）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
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展

1．経営層の意識改革

2．地域・中小企業におけるDX with Cybersecurity の推進

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

4．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

国民が安全で安心して暮らせるデジタル社会の実現

1．国民・社会を守るためのサイバーセキュリティ環境の提供

2．デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

3・4・5．経済社会基盤を支える各主体における取組
①(政府機関等)
②(重要インフラ)
③(大学・教育研究機関等)

6．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

7．大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

1．「自由、公正かつ安全なサイバー空間」の確保

2．我が国の防御力・抑止力・状況把握力の強化

3．国際協力・連携

横断的施策

研究開発の推進　人材の確保・育成・活躍促進　全員参加による協働・普及啓発

5　推進体制

「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

「Cybersecurity for All」を踏まえた対応の強化

サイバー空間の課題認識

- あらゆる主体が参画する公共空間化
- サイバー・フィジカルの相互連関・連鎖の深化
- サイバー攻撃の複雑化・巧妙化
- 安全保障上の脅威の増大

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

個人		組織	
DXに向き合う**地方、中小企業、若年層、高齢者等**	目に見えないリスクと向き合う**個人・組織**	サイバー攻撃による**重要インフラ**停止、知財の窃取、金銭被害等の増大	**国家の関与**が疑われる攻撃

DXとサイバーセキュリティの同時推進

○デジタル改革と一体で：経営層の意識改革、地域・中小企業の取組促進
（経営インセンティブ、安価かつ効果的な支援サービス・保険の普及）

○誰も取り残さないリテラシーの向上と定着
（高齢者向けデジタル活用支援講習会との連携、GIGAスクール構想にあわせた普及啓発、サイバー防犯ボランティア）

安全保障の観点からの取組強化

○中露北からの脅威等を踏まえた外交・安全保障上のサイバー分野の優先度向上

○防衛省・自衛隊におけるサイバー防衛能力の抜本的強化

○「妨げる能力」、外交的手段や刑事訴追等を含めた対応、日米同盟の維持・強化

○国際協力・連携

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

○国民・社会を守るためのサイバーセキュリティ環境の提供
（産業横断的なサプライチェーン管理、サイバー犯罪対策、クラウドサービス利用のための対策の多層的な展開、経済安全保障の視点を含むサイバー空間の信頼性確保）

○深刻なサイバー攻撃から国民生活・経済を守る包括的なサイバー防御等の展開
（情報収集から対処調整、政策措置までの一体的推進の総合調整を担うナショナルサートの機能強化、政府機関・重要インフラ等の各主体のセキュリティ対策）

資料１－２

次期サイバーセキュリティ戦略（案）

１　策定の趣旨・背景

2020 年代を迎えた最初の 1 年に、世界はコロナ禍の影響による不連続な変化に直面した。世界各地でロックダウンや外出制限が行われ、人々のくらしや様々な経済活動の基盤となる日常空間は、当たり前に享受できるものではなく、至るところに脆弱な側面を抱えているものであることが浮き彫りとなった。一方で、このような危機への対応を通じ、結果として人々のデジタル技術の活用は加速し、サイバー空間は、我々の生活におけるある種の「公共空間」として、より一層の重みを持つようになってきている。

また、この変化は、長い時間軸でみた大きな潮流を反映したものとも捉えられる。平成の時代を通じたデジタル経済の浸透は留まることなく、令和の時代に入り、デジタル庁を司令塔として、加速していくことが想定される。2020 年代は、2030 年に向けた国際的目標である SDGs[1]への貢献も期待される中、我が国の経済社会が、サイバー空間と実空間が高度に融合した Society5.0[2]の実現へと大きく前進する「Digital Decade」となり得ると考えられる。

一方で、足元では政治・経済・軍事・技術を巡る国家間の競争の顕在化を含む国際社会の変化の加速化・複雑化、情報通信技術の進歩や、複雑な経済社会活動の相互依存関係の深化が進むなど、サイバー空間をとりまく不確実性は絶えず変容し、かつ増大している。

サイバー空間の「自由、公正、安全」が所与のものではなく、むしろその確保が危機に直面している中、我々はサイバーセキュリティに対し、常に変化を重ねていくことこそが確保すべき価値の不変性につながるとする「不易流行」の精神[3]で取り組んでいかなければならない。その礎として、我が国としての戦略があらためて求められている。

１．１　2020 年代を迎えた日本をとりまく時代認識　～「ニューノーマル」とデジタル社会の到来～

（１）デジタル経済の浸透、デジタル改革の推進

インターネットの登場により「サイバー空間」という新たな空間が創出され、平成の時代を通じデジタル経済が大きく進展し、デジタル経済の影響は、人々の生活そのものに波及している。我が国のインターネット利用者は 8 割を超え[4]、インターネットの平均利用時間は 1 日当たり 2 時間を超えた[5]。また、IoT[6]や AI、5G[7]、クラウドサービス等の利

---

[1] Sustainable Development Goals の略。2001 年に策定されたミレニアム開発目標（MDGs）の後継として，2015 年 9 月の国連サミットで加盟国の全会一致で採択された「持続可能な開発のための 2030 アジェンダ」に記載された、2030 年までに持続可能でよりよい世界を目指す国際目標。17 のゴール・169 のターゲットから構成され，地球上の「誰一人取り残さない（leave no one behind）」ことが示されている。

[2] 狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上 5 番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（出典：未来投資戦略 2017（2017 年 6 月 9 日閣議決定））

[3] 熟語の出自は、松尾芭蕉が俳諧の本質を捉えるための理念として提起したものとされる。「不易」は時代の新古を超越して不変なるもの、「流行」はその時々に応じて変化していくものを意味するが、両者は本質的に対立するものではなく、真に「流行」を得ればおのずから「不易」を生じ、また真に「不易」に徹すればそのまま「流行」を生ずるものだと考えられている。（出典：小学館「日本大百科全書（ニッポニカ）」）

[4] 総務省「令和 2 年 通信利用動向調査」（2021 年 6 月 18 日）インターネット利用者の割合は全体の 83.4%。高齢者の利用者の割合も 5 割を超えている。

[5] 総務省情報通信政策研究所「令和元年度 情報通信メディアの利用時間と情報行動に関する調査報告書」（2020 年 9 月 30 日）

[6] Internet of Things の略。

[7] 第 5 世代移動通信システム。2015 年 9 月、ITU において、5G の主要な能力やコンセプトをまとめた「IMT ビジョン勧告

用拡大、テレワークの定着、ICT 教育等の実施など人々の行動が変容しており、サイバー空間はあらゆる人にとって経済社会活動の基盤となりつつある。このような変化の潮流は、確かな推進力として、サイバー空間と実空間が高度に融合した Society5.0 の実現を牽引することが期待される。

一方で、デジタル化の推進に向けては悪用・乱用からの被害防止やリテラシーの涵養、公的機関・民間双方のデジタル化の遅れなど、諸課題への的確な対応が必要となる。このため、2021 年 9 月に設置される「デジタル庁」をデジタル社会の形成に向けた司令塔とし、「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」をビジョンに掲げ、デジタル改革を強力に推進していく[8]こととしている。

（２）SDGs への貢献に対する期待

我が国として強力に推進する Society5.0 の実現を通じて、更なるデータ活用が可能となり、それによって防災や気候変動、環境保護、女性のエンパワーメントなど、SDGs でも重点事項として挙げられている様々な分野において、地球規模課題の解決に寄与することも期待される。

特に、我が国における「2050 年カーボンニュートラル」[9]に伴う「グリーン成長」の実現に向けては、スマートグリッドや製造自動化をはじめ、強靱なデジタルインフラが不可欠であるとされている[10]。

（３）安全保障環境の変化

我が国が享受してきた既存の秩序の不確実性は急速に増している。政治・経済・軍事・技術を巡る国家間の競争の顕在化を含め、国際社会の変化の加速化・複雑化が進展しており、サイバー空間をめぐる情勢が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[11]。

（４）新型コロナウイルスの影響・経験

コロナ禍の影響による不連続な変化に直面し、様々な制約や社会的要請への対応を余儀なくされることを通じ、結果として、「ニューノーマル」とも呼ばれる新しい生活様式が Society5.0 の実現を部分的にも体現することとなった。具体的には、テレワークをはじめとする多様な働き方や ICT 教育、遠隔診療などの取組が、コロナ禍以前と比べて大きく進展することとなった。

（M.2083）」が策定され、その中で、5G の利用シナリオとして、「モバイルブロードバンドの高度化（eMBB：enhanced Mobile BroadBand）」「超高信頼・低遅延通信（URLLC：Ultra Reliable and Low Latency Communications）」「大量のマシーンタイプ通信（mMTC：massive Machine Type Communications）」の 3 つのシナリオが提示されており、主な要求条件として、「最高伝送速度 20Gbps」「1 ミリ秒程度の遅延」「100 万台/㎢の接続機器数」が挙げられている。

[8] 「デジタル社会の実現に向けた改革の基本方針」（2020 年 12 月 25 日閣議決定）

[9] 2020 年 10 月に示された「我が国は、2050 年までに、温室効果ガスの排出を全体としてゼロにする、すなわち 2050 年カーボンニュートラル、脱炭素社会の実現を目指す」との方針。

[10] 「2050 年カーボンニュートラルに伴うグリーン成長戦略」（2020 年 12 月 25 日 成長戦略会議決定）

[11] 想定されるリスクについては、3.2 国際情勢からみたリスクに詳述している。

また、コロナ禍への対応の過程で、「パーソナルデータ」[12]を含む様々なデータを活用した新たなサービスの創出・活用も進展することとなった。

（５）東京大会に向けた取組の活用

2021 年に開催される 2020 年東京オリンピック・パラリンピック競技大会（以下「東京大会」という。）に向けて官民が連携して行ってきた対処態勢の整備やリスクマネジメントの促進等の取組は、コロナ禍という異例の環境下でも行われたことを含め、我が国にとって貴重な経験であると言えよう。こうした経験を、今後、2025 年日本国際博覧会（以下「大阪・関西万博」という。）等の大規模国際イベントを含め、我が国におけるサイバーセキュリティの向上に活用していくこととしている。また、これらの取組から得られた知見、ノウハウは、世界的にみても貴重なものであり、海外に発信・共有していくことで、国際連携への寄与も期待される。

１．２　本戦略の位置づけ

サイバーセキュリティ基本法（以下「基本法」という。）に基づく「サイバーセキュリティ戦略」（以下「戦略」という。）の策定は今回が 3 回目であり、基本法が制定された 2014 年から約 7 年が経過した。

本戦略は、中長期的視点から、先に述べた時代認識に立ち、2020 年代初めの今後 3 年間にとるべき諸施策の目標や実施方針を示すものである。同時に、未曽有のコロナ禍への対応から得られた教訓、デジタル改革、そして東京大会という大規模国際イベントでの対応を通じた経験を踏まえ、我が国としてのサイバーセキュリティに取り組む決意を、あらゆる主体、各国政府、そして攻撃者に対して発信するものである。

２　本戦略における基本的な理念

我が国は、「基本法の目的」や過去 2 回の戦略で示してきた「確保すべきサイバー空間」に関する考え方、「基本原則」といった基本的な立場を堅持する。

２．１　確保すべきサイバー空間

グローバルな拡張・発展を遂げたサイバー空間は、場所や時間にとらわれず、国境を越えて、質・量ともに多種多様な情報・データを自由に生成・共有・分析することが可能な場であり、流通する場である。こうした特徴を持つサイバー空間は、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として、人々に豊かさや多様な価値実現の場をもたらし、今後の経済社会の持続的な発展の基盤となると同時に、自由主義、民主主義、文化発展を支える基盤でもある。

サイバー空間を「自由、公正かつ安全な空間」とすることにより、基本法に掲げた目的に資するべく、国は、これまで 2 度にわたり、我が国のサイバーセキュリティに関する施策についての基本的な計画として、戦略を策定してきた。

[12] 個人の属性情報、移動・行動・購買履歴、ウェアラブル機器から収集された個人情報及び特定の個人を識別できないように加工された人流情報、商品情報等を含む概念。

先に述べた時代認識を踏まえれば、その目的、そしてサイバー空間に対する考え方はいささかも変わるものではない。むしろ、その確保が危機に直面する中で、「自由、公正かつ安全なサイバー空間」を確保する必要性はこれまで以上に増しているとの認識が深められるべきである。

２．２　基本原則

かかる認識の下、我が国は、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については、従来の戦略で掲げた 5 つの原則を堅持し、それに従うものとする。

（１）情報の自由な流通の確保

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（「信頼性のある自由なデータ流通」が確保される世界）が作られ、維持されるべきである[13]。なお、プライバシーへの配慮を含め、情報の自由な流通で他者の権利・利益をみだりに害することがないようにしなければならないことも明確にされるべきである。

（２）法の支配

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。また、同様に、サイバー空間においては、国連憲章をはじ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。

（３）開放性

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、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、サイバー空間は全ての主体に開かれたものであるべきである。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[14]。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。

（４）自律性

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。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。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

[13] 基本法第 1 条において、「情報の自由な流通を確保しつつ」と規定されている。なお、例えば、「G7 首脳コミュニケ」（2021 年 6 月）において、信頼性のある自由なデータ流通（DFFT）ロードマップが承認されるなど、その重要性は国際的にも認識されている。

[14] 高度情報通信ネットワーク社会形成基本法（平成 12 年法律第 144 号）において、「すべての国民が、インターネットその他の高度情報通信ネットワークを用意かつ主体的に利用する機会を有し」と規定されている。

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[15]。

（５）多様な主体の連携

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など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[16]。

国民の自由な経済社会活動を保障し国民の権利や利便性の確保を図ること、また、適時適切な法執行・制度により悪意ある者の行動を抑制することによって国民を保護することこそ、国民から期待されるサイバーセキュリティ政策のあるべき姿である。我が国は、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段を選択肢として保持する点を、これまで以上に明確にする。

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、この空間を取り巻く変化やリスク（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、サイバー空間をとりまく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づけ、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

[15] 基本法第３条第２項において、「サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促す」と規定されている。

[16] 基本法第３条第１項において、「サイバーセキュリティに対する脅威に対して、（中略）多様な主体の連携により、積極的に対応することを旨として、行われなければならない。」と規定されている。

及やサプライチェーン[17]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[18]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、かような状況が、国民に対し、サイバー空間に対する不安感を完全に払拭することを許していないことも事実である[19]。

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性がある。無論、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肝要である。

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つながることを通じ人々は「恩恵」を得ると同時に、そうした情報は今後一層、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。

---

[17] 一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。これらに加えてさらに、IT におけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることがある。

[18] 「国際連合創設 75 周年記念宣言」（2020 年 9 月 29 日）においても、新たな課題として提示されており、デジタルトラストとセキュリティの課題解決が優先事項とされている。

[19] 2020 年 9 月に警察庁が実施したアンケート調査によると、回答者の 75.3%がサイバー犯罪に不安を感じると回答。（出典：「令和２年度サイバーセキュリティ政策会議報告書」（2021 年 3 月 警察庁サイバーセキュリティ政策会議））

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え、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 機器の利用拡大に伴い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[20]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。加えて、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

[20] 境界線（ペリメータ）で内側と外側を遮断して、外部からの攻撃や内部からの情報流出を防止しようとする考え方。境界型セキュリティでは、「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となる。防御対象の中心はネットワーク。

っているとみられている。また、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[21]。

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[22]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[23]、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、

---

[21] 具体的な動向は、3.3 国際社会の平和・安定及び我が国の安全保障への寄与の柱書きに詳述する。

[22] Virtual Private Networkの略。インターネットや多人数が利用する閉域網を介して、暗号化やトラフィック制御技術により、プライベートネットワーク間が、あたかも専用線接続されているかのような状況を実現する技術又はそのための機器。

[23] 例えば、「G7首脳コミュニケ」（2021年6月）においては、「ランサムウェアの犯罪ネットワークによる脅威の高まり」について言及されている。

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、経済社会活動に大きな影響が生じている。

４　目的達成のための施策　～Cybersecurity for All～

本項においては、基本法に掲げた目的を達成するため、前項までの課題認識を踏まえ、今後 3 年間にとるべき諸施策の目標や実施方針を示す。

サイバー空間は、これまで述べたように、空間そのものが量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、セクター、地域等において、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）が到来したと言えよう。今後、サイバー空間とは繋がりのなかった主体も含め、あらゆる主体がサイバー空間に参画することとなる中で、デジタル化の動きと呼応し「誰一人取り残さない」サイバーセキュリティの確保に向けた取組を進める必要がある。この考え方の下、不確実性を増す環境において「自由、公正、かつ安全なサイバー空間」を確保するため、以下の 3 つの方向性に基づき、施策を推進する。

なお、これらは、主として、本項において示す「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」に向けた取組にそれぞれ対応するものであるが、前項までの課題認識を踏まえれば、いずれの目的達成に向けた施策においても意識されるべきである。

＜3 つの方向性＞

（１）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[24]とサイバーセキュリティの同時推進

経済社会のデジタル化をめぐる状況をみれば、コロナ禍を通じて結果としていわゆる「ニューノーマル」の定着が進んだことに加え、デジタル社会の形成に向けた司令塔たる「デジタル庁」が 2021 年 9 月に設置されるなど、いまが、我が国が後れをとったデジタル化の時計の針を大きく進める絶好の機会であることは論を俟たない。

一方で、サイバーセキュリティに対する意識や、サイバー空間を構成する技術基盤やデータ等に対する信頼が醸成されなければ、足元のデジタル化の潮流に対して積極的な参加・コミットメントを得られず、変革を伴わない表層的なデジタル化に留まるおそれがある。裏を返せば、デジタル化に応じたリスクの変容に適切に対処をすることで、サイバーセキュリティに対する意識や信頼の醸成にもつながり得る。

また、経済社会全体のデジタル化だけではなく、個々の企業活動におけるデジタル化に視点を向けても、サイバーセキュリティ確保との強い関係性がみられる。デジタル化進展

[24] 「デジタルトランスフォーメーション」は、一般的に DX と略される。2018 年 9 月「DX レポート」（2018 年 9 月 経済産業省デジタルトランスフォーメーションに向けた研究会）においては、「企業が外部エコシステム（顧客、市場）の破壊的な変化に対応しつつ、内部エコシステム（組織、文化、従業員）の変革を牽引しながら、第 3 のプラットフォーム（クラウド、モビリティ、ビッグデータ／アナリティクス、ソーシャル技術）を利用して、新しい製品やサービス、新しいビジネスモデルを通して、ネットとリアルの両面での顧客エクスペリエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること」という定義が引用されている。

の中で、IT システムやデジタル化への対応能力が、業務、製品・サービス等の有する付加価値の源泉となっていくと想定される中で、サイバーセキュリティの確保は企業価値に直結する営為となると考えられる。加えて、迅速で柔軟な開発・対処の必要性が高まる中で、サイバーセキュリティを業務、製品・サービス等のシステムの企画・設計段階から確保する「セキュリティ・バイ・デザイン」の考え方の重要性は一層重要となり、デジタル投資とセキュリティ対策はより一層、一体性を増すと考えられる。

このように、ミクロ・マクロのいずれの視点においても、デジタル化の進展とあわせてサイバーセキュリティ確保に向けた取組を同時に推進すること（以下「DX with Cybersecurity」という。）が重要であり、あらゆる主体においてこれが意識され、取組が推進されなければならない。足元のデジタル改革では、その基本法たるデジタル社会形成基本法においてサイバーセキュリティの確保が明確に位置づけられるなど、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を同時に推進する素地が整えられたところであり、国として、その前提となる基盤づくりをはじめとして、デジタル化の動きを強力に後押しする。

（２）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

2018 年に策定された従来の戦略では、サイバー空間の持続的な発展に向けて、サービス提供者の「任務保証」、「リスクマネジメント」、「参加・連携・協働」という 3 つの観点から官民の取組を進めることとしてきた。

サイバー空間の脅威の増大、経済社会が抱える脆弱性の顕在化、安全保障環境の変化等、不確実性を増す環境下で、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、それぞれの観点について深化・強化（①任務保証の深化、②「リスクマネジメント」に係る取組強化）し、その環境・原因の改善に正面から取り組んでいくことが求められている。

そうした社会的要請に伴い、サイバー空間に関わるあらゆる主体の役割が増している。自律的な取組（「自助」）や多様な主体の緊密連携（「共助」）の重要性は不変なるものであるが、それらの基盤となる「公助」の役割をはじめとして、各主体の役割や防御すべき対象を不断に検証し、多層的な取組を強化する。その際、自助共助では対応できないような事象に対して、国がインシデント対応とその後の再発防止や改善に向けた政策措置を一体的に推進するための総合的な調整を担う機能として、ナショナルサート（CSIRT/CERT）[25]の枠組みの強化を図りつつ、それが一層果たされるよう、検証による向上・充実強化を図る。

①「任務保証」の深化（エンドユーザへのサービスの確実な提供を意識したサプライチェーン全体の信頼性確保）

[25] 一般的に、CSIRT は Computer Security Incident Response Team の略（シーサート）。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。CERT は Computer Emergency Response Team の略（サート）。コンピュータセキュリティインシデントに対応する活動を行う組織のこと。国際連携の下でサイバー攻撃に対処する際に、我が国においては、政府と民間の専門組織が連携して対応している。本戦略においては、ナショナルサートを、「深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能」と位置づけている（4.2.1(4)に詳述）。

従来の「任務保証」[26]の考え方は、サービス提供者が特に契約関係のあるサービスの直接的な利用者を中心に、遂行すべき業務を「任務」として着実に遂行するための考え方として位置づけられてきた。

近年、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、サイバー空間を通じて提供されるサービスに対する様々なプレーヤーの関与や、クラウドサービス事業者等への依存度の増加により、サービス・業務の責任主体がエンドユーザから見えにくくなっている。また、インシデントが発生した際の影響も広範かつ複雑化し、その波及の予見や解決に向けた困難性も増している。クラウドサービスを例に挙げれば、あるクラウドサービスを利用する事業者のみならず、その利用事業者が提供するサービスを利用するエンドユーザにも影響が及び得る状況となっている。このような状況は、従来、サイバー空間への関与が少なく、デジタル化進展の過程で不可避的にサイバー空間に参加する者にとっては、なおさら深刻である。かかる認識に基づき、サイバー空間を活用して業務・サービスの提供者として携わる者は、提供者と利用者間の一対一の関係だけではなく、サプライチェーン全体を俯瞰し、その信頼性を意識して責任ある行動をとることが求められる。

「任務保証」の考え方の重要性は今後も不変のものとして、更にこれを深化させ、あらゆる組織が、サイバー空間を提供・構成する主体として、自らが遂行すべき業務やサービスからエンドユーザに至るサプライチェーン全体の信頼確保を「任務」と捉えることで、サイバー空間を構成する多様な製品やサービスについて、その安全性・信頼性が確保され、利用者が継続的に安心して利用できる環境をめざす。

② 「リスクマネジメント」に係る取組強化

組織化・洗練化されたサイバー攻撃の脅威の増大等がみられる中で、国として、各国政府・民間等様々なレベルで連携をしつつ、個々の主体による「リスクマネジメント」を補完し、一層実効的に取組を強化する。

具体的には、我が国として、サイバー攻撃に対して能動的に防御するとともに、脅威の趨勢を踏まえ、常に想定されるリスク等の見直しや事後追跡可能性（以下「トレーサビリティ」という。）の確保に努める。

また、国民の個人情報や国際競争力の源泉となる知的財産に関する情報、安全保障に係る情報の窃取のための一つの重要なチャネルとしてサイバー空間が利用されている現状を踏まえ、このようなサイバー攻撃への対処とともに、サイバー空間を構成する技術基盤自体の信頼性の確保に努める。

（３）安全保障の観点からの取組強化

我が国の安全保障を巡る環境は厳しさを増し、サイバー空間が国家間の競争の場の一部ともなっている中で、サイバー空間における攻撃者との非対称な状況を看過してはならない。

[26] 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。

各主体がその姿勢を明確化するとともに、防衛省・自衛隊をはじめとした政府機関等の能力強化により、国家の強靭性を確保するなどして防御力を強化し、攻撃者を特定し責任を負わせるためにサイバー攻撃を検知・調査・分析する能力を引き続き高め、抑止力を強化する。また、サイバー脅威に対しては、同盟国・同志国と連携をして、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる。

加えて、サイバー空間の健全な発展を妨げるような取組に対して、同盟国・同志国や民間団体と連携して対抗し、我が国の安全保障に資する形で、グローバルに「自由、公正かつ安全なサイバー空間」を確保するために、積極的な役割を果たす。

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～

デジタル改革のビジョンである「デジタルの活用により、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、我が国経済社会は、変革を伴うデジタルトランスフォーメーションを遂げることが必要である。

そして、その機会と影響が、あらゆる主体に例外なく及ぶ中で、「DX with Cybersecurity」があらゆる主体において意識され、取組があらゆる面で推進されなければならない。

経済社会のデジタル化を進めていく過程における、経営層の意識改革や、地域・中小企業に対する取組、デジタル時代において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の基盤づくり、経済社会全体でリテラシーを高める取組のいずれにおいても、サイバーセキュリティに関する視点が取り入れられ、施策が推進されることが肝要である。

４．１．１　経営層の意識改革

新型コロナウイルスの影響を経てデジタル化は加速し、今後、企業において、より付加価値の高いデジタルサービス等を生み出す基盤を有しているかが重要な競争力の要素となっていくと想定される。経営層にとって、デジタル化とサイバーセキュリティ対策は、他人事ではなく、同時達成されるべき業務と収益の中核を支える基本的事項となり、両者を理解することが経営の基本的な素養・知識となると想定され、サイバー空間にかかわるリスクの存在はデジタル化に取り組まない言い訳たり得なくなると考えられる。こうした認識に基づき、デジタル化と一体となったサイバーセキュリティの強化に向け、経営層の意識改革や企業の取組を推進していく必要がある。

デジタル経営の推進に向けては、自律的にデジタルトランスフォーメーションに取り組む企業へと、資金や人材、ビジネス機会が集まるような環境を整備していく観点から、経営者に求められる企業価値向上に向け実践すべき事柄をデジタル経営の指針としてまとめ、その実践を推進することとしている。

また、サイバーセキュリティの強化に向けては、これまで、経営層がリーダーシップを取ってセキュリティ対策を推進していくことの重要性を示したガイドラインの普及啓発を進めてきているところ、引き続き、その実践に向けた事例や手引き等の策定を通じて活用促進に取り組むとともに、必要に応じてその見直しを行っていくこととしている。

これらを踏まえつつ、デジタル化と一体となったサイバーセキュリティ強化に向けた取組状況が、サステナビリティを重視する投資家等のステークホルダーに可視化され、かつそうした取組に対しインセンティブが生まれるよう取り組む。これにより、企業の取組状況が、市場を含む企業内外から持続的な企業価値の向上につながるものとして評価され、更なる取組を促進する機運が形成されることが期待される。具体的には、デジタル経営に向けた行動指針やデジタル化に取り組む先進的な取組企業の選定・公表、デジタル関連投資への税制措置等のデジタル化促進施策においてサイバーセキュリティに係る取組を位置づけるとともに、取組状況を企業内外に可視化するためのツールやガイドラインの活用促進等を推進する。これらを通じ、経営層によるサイバーセキュリティに係るリスク把握や企業情報開示といったプラクティスの普及促進も期待されるところ、企業の取組状況のフォローアップにもあわせて取り組んでいく。

また、こうした一体的な推進策を通して、経営層がデジタル化とあわせてサイバーセキュリティ対策に取り組む上で、自社の競争力の源泉たるデジタルサービス等に内在するリスクの所在を適切に把握できるようにするためには、企業内外の専門家とのコミュニケーションをとることが欠かせない営為となると想定される。このため、経営層に対し、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あ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（以下「『プラス・セキュリティ』知識」という。）を補充できる環境整備を推進する[27]。

４．１．２　地域・中小企業における DX with Cybersecurity の推進

コロナ禍への対応を余儀なくされること等を通じ、ビジネスモデルの変革や働き方・雇用形態のあり方にも変化が及ぶ中で、デジタル化の機会は、地域・中小企業、そしてサイバー空間とは繋がりのなかった業種・業態の企業にも例外なく広がっていくと想定される。

一方で、中小企業がデジタル化と同時にサイバーセキュリティ対策に取り組むに当たっては、セキュリティ専任の人材を配置できないなど、知見や人材等のリソース不足に直面しており、これらの課題への対処が必要である。

このため、「共助」の考え方に基づく、地域のコミュニティづくりにおいて、その機能を引き続き発展させ、専門家への相談に留まらず、ビジネスマッチングや人材の育成・マッチング、地域発のセキュリティソリューションの開発など、リソース不足を踏まえた地域による課題解決・付加価値創出が行われる場の形成を促進するとともに、先進事例の共有を通じて全国への展開に取り組む。

また、中小企業においては、セキュリティに多額の予算を割くことが難しいという課題もあるところ、中小企業が利用しやすい安価かつ効果的なセキュリティサービス・簡易保険の普及など、中小企業向けセキュリティ施策の推進に取り組む。具体的には、中小企業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とも連携しつつ、一定の基準を満たすサービスに商標使用権を付与するための審査・登録、セキュリティ対策の自己宣言等の取組を推進すると

[27] 具体施策については、4.4.2(1)①に詳述する。

ともに、中小企業向け補助金における自己宣言等の要件化等を通じたインセンティブ付けに取り組む。これらの取組を通じ、サイバーセキュリティ強化に向けた取組状況が取引先等に対して可視化されることで、地域・中小企業に取組を広げる契機となることが期待される。

加えて、今後は、中小企業に広くクラウドサービスの利用が普及することも一つの重要な選択肢となると想定される。その利用に当たっては、情報資産が企業外に置かれることに加え、設定の不備等により意図せず流出するリスクも一定程度伴うことから、クラウドサービス利用者が留意すべき事項に関する手引き等の周知に取り組むとともに、クラウドサービス利用時の設定ミスの防止・軽減のため、クラウドサービス事業者に、利用者に対する情報提供やツールの提供等の必要なサポートの提供を促す方策等を検討する。

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

サイバー空間と実空間が高度に融合するSociety5.0の実現に向けて、今後は、あらゆる主体が相互連関・連鎖を自由に形成することで新たな価値を創造することが期待される。一方で、その信頼性を確保する観点から、このように新たに形成される相互連関・連鎖の下で生じる課題に適切に対応していくことが必要となる。

こうした課題への適切な対応を目的として策定された、サイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等も踏まえ、我が国において、新たな価値創出を支えるサプライチェーン等の信頼構築の基盤となる、サイバーセキュリティ確保に向けた取組を推進する。

（１）サプライチェーンの信頼性確保

サプライチェーンの複雑化やデジタルサービスの連携が進む中、より柔軟で動的なサプライチェーンの構成が可能となる一方で、サイバーセキュリティに係る観点では、サイバー攻撃の起点となり得る箇所の拡大や実空間への影響の増大が懸念されるなど、サプライチェーン全体を見渡したリスク管理の重要性は増すと考えられる。

このような認識に立ち、上記フレームワーク等に基づく産業分野別及び産業横断的なガイドライン等の策定や活用促進を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。

また、様々な産業分野の団体等が参加し、サプライチェーン全体でのサイバーセキュリティ対策強化を目的として意識喚起や取組の具体化を行うコンソーシアムの取組を支援する。また、この枠組みの下、一定の基準を満たす中小企業向けサービスの審査・登録や利用推奨、サイバーセキュリティ強化に向けた取組状況の可視化を行うことで、サプライチェーンを通じて地域・中小企業に取組を広げ、サプライチェーン全体の信頼性向上につながることが期待される。

（２）データ流通の信頼性確保

サイバー空間における多様な経済社会活動を進める上で、「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）」[28]の実現に向けたデータガバナンス確保の観点を含め、その価値の源泉となるデータの真正性や流通基盤の信頼性を確保することが重要である。

主体間を流通する中でその属性が絶えず変化するデータの特性を踏まえ、リスクポイントの洗出しの観点から、データマネジメントに関する定義の明確化等を行い、リスクの洗い出しの手順やユースケースの検討等を含むフレームワークの整備を進めるとともに、国境を越えて流通するデータを取り扱う各国等のルール間ギャップの把握等に活用する。

また、送信元のなりすましやデータの改ざん等を防止する仕組み（以下「トラストサービス」という。）については、その利活用に向けて実効的な仕組みとする必要がある。主体・意思、事実・情報、存在・時刻といった要素の真正性・完全性を確保・証明する各種トラストサービスの信頼性に関し、具備すべき要件等の整備・明確化や、その信頼度の評価・情報提供、国際的な連携（諸外国との相互運用性の確認）等の枠組みの整備に取り組む。

（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[29]や OSS[30]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の検討に取り組む。

（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

[28] 安倍総理大臣（当時）による世界経済フォーラム年次総会演説 「『希望が生み出す経済』の新しい時代に向かって（仮訳）」（2019 年 1 月 23 日）

[29] API は Application Programming Interface の略であり、あるソフトウェアが別のソフトウェアに対して公開する、入出力のための仕組みを指す。

[30] OSS は Open Source Software の略であり、利用者の目的を問わずソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称を指す。

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、当該情報を産官学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。

４．１．４　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

サイバー空間の基盤は人々のくらしにとっての基礎的なインフラとなりつつある中、「誰一人取り残さない、人に優しいデジタル化」[31]を進め、その恩恵を享受していくためには、国民一人ひとりが自らの判断で脅威から身を守れるよう、サイバーセキュリティに関する素養・基本的な知識・能力（いわゆるリテラシー）を身に付けていくことが必須である。

一方で、リテラシーは一朝一夕に身に付くものではない。行政のデジタル化、マイナンバーカードの普及や「GIGA スクール構想」[32]の推進等が進み、様々なデジタルサービスに触れる機会が増えていく中、「まずは自分でやってみる」意識を持ち、リテラシーの向上と定着に向けて能動的に体験を積んでいくことが何よりも重要である。この際、情報教育が推進される中で、各種取組が進められるべきである。

国としても、デジタル活用の機会、またそれに応じたデジタル活用支援の取組と連動をしながら、官民で連携して国民への普及啓発活動を実施していく。例えば、高齢者等向けには、携帯電話の販売代理店をはじめ様々な地域の担い手との連携、子供向けには、小中学校とサイバー防犯に係るボランティア等との連携も図りつつ、サイバーセキュリティに関する注意事項の啓発等に取り組む。「GIGA スクール構想」の推進に当たっては、教師の日常的な ICT 活用の支援等を行う支援員等の配置や教職課程における ICT 活用指導力の充実を図るとともに、児童生徒に対し、端末整備にあわせた啓発や、動画教材等を活用した情報モラルに関する教育を推進する。

また、インターネット上の偽情報の流布については、個人の意思決定や社会の合意形成に不適切な影響が与えるおそれがあることから、民間の自主的取組の慫慂を含め、幅広く周知啓発を行う。

---

[31] 「デジタル社会の実現に向けた改革の基本方針」（2020 年 12 月 25 日閣議決定）

[32] 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。

４．２　国民が安全で安心して暮らせるデジタル社会の実現

サイバー空間の公共空間化とサイバー・フィジカルの垣根を越えた相互連関・連鎖の深化を踏まえ、あらゆるサービスの提供主体には、これまでの「任務保証」という考え方を深め、サイバー空間のこのような変容に適合したリスクマネジメントを講ずることが求められる。国は、サイバー空間の安全を確保することによって、サイバー空間に関わるあらゆる国民や主体が、安心してサイバー空間に参画できるよう、サイバー空間全体を俯瞰しつつ、関係主体との連携を通じて、自助・共助による自律的なリスクマネジメントが講じられる環境づくりに努める。また、国民の安全・安心の根幹にかかわる経済社会基盤については、国は、防御すべき対象を不断に検証しつつ、関係主体と連携を図りながら、持ち得る全ての手段を活用して包括的なサイバー防御を講じるとともに、先進的な取組の導入を率先して進めることで社会全体の実装を牽引し、サイバー空間の安全性・信頼性の確保を図る。

これらの取組を通じて、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバー防御体制を構築し、もって、国全体のリスクの低減とレジリエンスの向上を図る。

４．２．１　国民・社会を守るためのサイバーセキュリティ環境の提供

サイバー空間の公共空間化を踏まえ、全ての主体が利便性と安心を感じられる社会を実現するため、国は、関係主体と連携しつつ、サイバー空間を構成する技術基盤やサービスの可視化とインシデント発生時のトレーサビリティの向上に取り組むことで、各主体がニーズに合った適切なリスクマネジメントを選択できるような環境を醸成するとともに、トレーサビリティの確保や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。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。

また、このようなサイバー空間の変容を背景に、インシデントの影響が複雑かつ広範囲に伝播するリスクが顕在化している状況を踏まえ、各サービスの提供主体が、直接の利用者のみならずその先の利用者の存在も見据えつつ、相互連関・連鎖全体を俯瞰してリスクマネジメントの確保に務めることがスタンダードとなるよう、国は関係主体と連携して環境づくりに取り組んでいく。

国民の安全・安心の根幹に関わる経済社会基盤の防護については、これを担う各主体が役割に応じた機密性、可用性、完全性を確実に保証することが基本であるが、前述のサイバー空間の変容に加え、近年の攻撃手法の組織化・洗練化などの脅威に晒されるなど厳しい環境下では、自助、共助の取組だけで対応することは益々困難となっていることから、国が主体的に関係機関とも連携を図りつつ、攻撃者の視点も踏まえ、持ち得る全ての手段を活用して包括的なサイバー防御を講じることによって、国全体のリスクの低減とレジリエンスの向上に精力的に取り組む。

また、国は特に防御すべき対象を不断に検証することも重要である。国家安全保障に関わる情報に加え、特に、国民の個人情報や国際競争力の源泉となる知的財産に関する情報は、国として防護すべき重要な対象であり、サイバー攻撃を通じたこれらの不正な窃取は、国民の安全・安心や公正な経済取引を損なうものであることから、国は経済安全保障の観

点も含め、こうした情報の横断的な防護に向けた対策を強化する。

（１）安全・安心なサイバー空間の利用環境の構築

国はサイバー空間の公共空間化やそのサプライチェーンの深化を踏まえ、各主体の自助及び共助によるリスクマネジメントの向上に資するため、「セキュリティ・バイ・デザイン」の考え方に基づく基盤構築などの指針等を策定するとともに、サイバー空間のトレーサビリティや可視化の向上に官民が一体となって取り組む。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。

① サイバーセキュリティを踏まえたサプライチェーン管理の構築

サプライチェーンに対してリスク管理等の必要な対策に取り組むべく、国はサイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等に基づく産業分野別・産業横断的なガイドライン等の策定を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。

また、国は中小企業、海外拠点、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、サプライチェーン内での情報共有や報告、適切な公表等を推進する産業界主導の取組を支援する。

更に、国は機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素における信頼の確保を図るための仕組みを構築するとともに、これら構成要素の信頼が、サプライチェーン上において連続的に確保されるよう、トレーサビリティの確保と信頼を毀損する攻撃に対する検知・防御の仕組みの構築を推進する。

② IoT や 5G 等の新たな技術やサービスの実装における安全・安心の確保

IoT が急速に普及する中、安全・安心な IoT 環境を実現していくため、国はサイバー攻撃に悪用されるおそれのある機器を特定し注意喚起を進めていくとともに、「セキュリティ・バイ・デザイン」の考え方に基づいて、安全な IoT システムを実現するための協働活動や指針策定、情報共有、国際標準化の推進、脆弱性対策への体制整備を実施する。また、IoT 機器・システムの活用に当たっては、セーフティの観点からの対策とサイバーセキュリティ対策を組み合わせることが求められるところ、国はそのようなセキュリティとセーフティの融合に対応したフレームワークの活用を推進する。

また、国は全国及びローカル 5G のネットワークのサイバーセキュリティを確保するための仕組みの整備や、サイバーセキュリティを確保した 5G システムの開発供給・導入を促進する。

更に、国は自動運転、ドローン、工場の自動化、スマートシティ[33]、暗号資産[34]、宇宙産業等の新規分野に関するサイバーセキュリティの対策指針・行動規範の策定等を通じて、安心・安全を確保する。

③ 利用者保護の観点からの安全・安心の確保

[33] ICT 等の新技術や官民各種のデータを活用した市民一人一人に寄り添ったサービスの提供や、各種分野におけるマネジメント(計画、整備、管理・運営等)の高度化等により、都市や地域が抱える諸課題の解決を行い、また新たな価値を創出し続ける、持続可能な都市や地域であり、Society 5.0 の先行的な実現の場。

[34] 法定通貨や法定通貨建ての資産ではなく、不特定の者に対する代価の弁済や不特定の者を相手方とした法定通貨との交換等に使用でき、電子的に記録され移転することが可能なもの。

利用者が安心して通信サービスを利用してサイバー空間において活動できるようにする観点から、必要に応じて関係法令に関する整理を行いながら、安全かつ信頼性の高い通信ネットワークを確保するための方策を検討する。

また、多数の公的機関、企業及び国民が利用するサービスについては、その社会的基盤（プラットフォーム）としての役割に鑑み、国はより一層のサプライチェーン管理を含めたサイバーセキュリティ対策を促進する。

（２）新たなサイバーセキュリティの担い手との協調

サイバー空間が、日進月歩に変化する技術やサービスの実装により間断なく高度化し、サービス提供者の主体が変わりうる実態を踏まえ、国は常にサイバー空間に登場する新たな技術やサービスを把握し、これらによるサイバー空間の各主体への相互影響度やその深刻度の分析を行い、それぞれの主体においてサイバーセキュリティへの確保に責任ある対応を果たせるような環境づくりを行う。

特に、クラウドサービスは、サイバー空間において欠かせないインフラとなっているが、例えばサービスの設定不備等によって、利用者にとって意図しないインシデントが発生し、場合によっては当該インシデントを認識することも難しく、さらには自分の力だけでは正常化できないような事態も発生している。また、クラウドサービスは、これを利用する多数の間で同様のインシデントが同時多発的に発生するという問題もある。このため、利用者が安心してクラウドサービスに情報資産を委ねることができるよう国は、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進するとともに、政府機関や重要インフラ事業者等の利用者がクラウドサービスを利用する情報システムの設計及び開発の過程において考慮すべきサイバーセキュリティのルールを利用者、クラウドサービス事業者、システム受託事業者等の関係者と連携しながら策定する。これによって、クラウドサービスの利用者側が、自らのリスクマネジメント指針に合致した適切なクラウドサービスを選択し、セキュリティに関するポリシーや責任分界を正しく理解することを可能とするほか、提供者との間で認識のずれが生じた場合にも適切に課題を処理できるような関係を構築していく。並行して、国は政府情報システムのためのセキュリティ評価制度（ISMAP[35]）等の取組を活用したクラウドサービスの安全性の可視化の取組を政府機関等から民間にも広く展開し、一定のセキュリティが確保されたクラウドサービスの利用拡大を促進する。クラウドサービスは外国企業により提供されているものも多いことから、グローバルな連携も進める。

これらの対策を多層的に展開し、必要に応じてパッケージ化することも検討したうえで、中小企業や地方における利用者のサイバーセキュリティの確保も促し、日本社会全体における安心安全なクラウドサービス利用環境を構築する。

（３）サイバー犯罪への対策

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、国はサイバー空間を悪用する犯罪者や、トレー

[35] Information system Security Management and Assessment Program の略。政府情報システムのためのセキュリティ評価制度（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。

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、暗号資産、ダークウェブ、SNS 等を悪用した犯罪や、高度な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とともに、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。

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、被害の未然防止、人材育成等の観点から、官民が連携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。

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など、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、攻撃者との非対称な状況を生んでいる環境・原因を改善するため、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国際連携等必要な取組を推進する。また、通信履歴等に関するログの保存の在り方については、関係のガイドラインを踏まえ、関係事業者における適切な取組を推進する。

これら取組を効果的に実施していくため、警察組織内にサイバー部門の司令塔を担う機能と、専門の実働部隊を創設することを検討するなど、対処能力の強化を図る。

（４）包括的なサイバー防御の展開

重要インフラの機能停止、国民情報や知的財産の窃取、金銭窃取など国民の安全・安心の根幹を揺るがすような深刻なサイバー攻撃に対しては、サイバー空間の相互連関・連鎖の深化と相俟って、個々の主体による自助・共助の取組だけでは対応に限界があり、また、その影響の全体像を把握することも困難となるなど、実効的な防御を講じることが難しい状況となっている。

このため、国は、このような深刻なサイバー攻撃に対して、オールジャパンで力を合わせて、適宜適切な情報把握・分析から事案対処までに至るインシデント対応及びその後の再発防止や改善に向けたルール作り等の政策措置の展開を一体的に推進する包括的なサイバー防御策について、関係主体との連携も図りつつ、持ち得る全ての能力と手段を活用して展開する。

① 包括的なサイバー防御の総合的な調整を担うナショナルサート機能等の強化

国は、深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能としてのナショナルサート（CSIRT/CERT）の枠組みを強化する。具体的には、対処官庁のリソース結集と連携強化を通じて対処能力の向上と対処に係る一体性・連動性を図るとともに、サイバー関連事業者との連携強化

によって組織・分野横断的に影響が波及しうる事案の情報収集や初動を含めた対処調整の迅速化を図る。また、サイバーセキュリティ協議会[36]やサイバーセキュリティ対処調整センター[37]、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間や海外関係機関との連携を一層推進することで、官民間・国際間での情報共有と対処調整の円滑化を図る。さらに、発生した事案等から得られた課題や気づきを踏まえ、国は、官民を含む関係者と総合的な調整を行い、適時に制度化など必要な政策の立案・措置を講じていく。

これらの取組により、官民を含む関係者からの適宜迅速な情報収集と被害の全体像の迅速な把握力を強化するとともに、国の防御に関する情報発信の訴求力と網羅性の向上、攻撃の特性や深刻度、個々の分野の事情に応じた系統的できめ細かい対応、防御の実効性向上に資する経営から現場レベルまでの様々なニーズに応じた適時な注意喚起や情報提供、サイバー攻撃の無害化等を模索するグローバルなオペレーションへの協力、さらに、円滑な総合調整による迅速な政策立案等の更なる推進を図り、国全体の包括的な防御力を向上する。

② 包括的なサイバー防御を着実に実施していくための環境整備

国は深刻なサイバー攻撃への対処を実効たらしめる脆弱性対策等の「積極的サイバー防御」[38]に係る諸施策、IT システムやサービスの信頼性・安全性を確認するための技術検証体制の整備、情報共有・報告・被害公表の的確な推進、制御システムのインシデント原因究明機能の整備等について関係省庁間で連携して検討する。

（５）サイバー空間の信頼性確保に向けた取組

現在認知されているサイバー攻撃の多くが国民の個人情報や国際競争力の源泉となる知的財産に関する情報を目的としていることを踏まえ、国は経済安全保障の観点も含めた横断的な防護対策を講じる。

また、我が国の国民生活や経済社会活動の根幹を支える基盤において実装されている IT システムに起因するインシデントが、それら基盤の機能停止に直結するリスクを踏まえ、国は経済安全保障の観点から、任務及び機能の自律性の毀損につながるおそれのあるサイバー空間の脆弱性を把握し、その信頼性確保に向けた対応を検討する。

① 国民の個人情報や国際競争力の源泉となる知的財産に関する情報を保有する主体を支援する取組

国はサイバー攻撃等から個人情報を保護する有効な安全管理措置について、適時適切に情報提供を行い、対策の徹底を図る。

また、国は国民の個人情報や国際競争力の源泉となる知的財産に関する情報を保有または管理する主体である民間企業、大学等におけるセキュリティ対策に資する情報共有を促す取組を強化する。

---

[36] 2018 年 12 月に成立したサイバーセキュリティ基本法の一部を改正する法律（2018 年法律第 91 号）に基づき、2019 年 4 月 1 日に、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うために組織されたもの。本協議会は、官民又は業界を問わず多様な主体が連携し、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を防ぎ、また、被害の拡大を防ぐことなどを目的としている。

[37] 東京大会のサイバーセキュリティに係る脅威・事案情報を収集し、関係機関等に提供するとともに、関係機関等における事案対処に対する支援調整を行う組織。2019 年 4 月 1 日に設置。

[38] サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じていく取組のこと。

② 経済安全保障の視点を踏まえたITシステム・サービスの信頼性確保

国は我が国の国民生活や経済社会活動に大きな影響のある重要なインフラにおいて実装されるITシステム・サービスや、その業務提携や委託契約の態様について、サプライチェーン・リスクを含む様々なリスク・シナリオも勘案し、その安全性・信頼性を確保するための制度的検討を含む対策を推進する。また、それに必要となる新たな技術開発を推進する。

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。

また、国はIT機器やサービスに係る国際標準の策定や、安全性・信頼性の可視化を促すための基準作り・評価の取組についても国際連携も念頭に置きながら推進する。特に、政府情報システムの調達に係るサプライチェーンも含めた信頼性確保の取組強化やセキュリティ評価制度（ISMAP）の活用を進めるとともに、ITシステム・サービスの信頼性に関する技術面での検証能力の構築やそのための基準策定に着手することで制度面・技術面の双方から信頼性の底上げを図る。

４．２．２　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

「誰一人取り残さない、人に優しいデジタル化」の実現のためには、国民目線に立った利便性向上の徹底とサイバーセキュリティの確保の両立が必要である。このため、デジタル庁が策定する国、地方公共団体、準公共部門等の情報システムの整備及び管理の基本的な方針（以下「整備方針」という。）において、サイバーセキュリティについても基本的な方針を示し、その実装を推進する。

また、デジタル庁は、データの安全・安心な利活用の観点から、マイナンバーや法人番号など個人・法人を一意に特定し識別するID制度や電子署名、商業登記電子証明書など情報とその発信者の真正性等を保証する制度の企画立案を関係省庁と共管し、利用者視点で改革し、普及を推進する。

更に、国はクラウド・バイ・デフォルトの実現を支えるISMAP制度を運用し、運用状況等を踏まえて制度の継続的な見直しを行うとともに、民間における利用も推奨する。

４．２．３　経済社会基盤を支える各主体における取組①（政府機関等）

各政府機関においては、統一的な基準を踏まえたセキュリティ対策が講じられるとともに、当該基準に基づいた監査やCSIRT訓練・研修等、GSOC[39]による不正な通信の監視等の取組を通じて、政府機関全体としての対策の水準の向上を推進している。各政府機関は、社会全体のデジタル化と一体としてサイバーセキュリティ対策を進め、情報システムの開発・構築段階も含めたあらゆるフェーズでの対策を強化していく。

特に、各府省庁が共通で利用する重要なシステムについては、デジタル庁が自ら又は各府省と共同で整備・運用し、セキュリティも含めて安定的・継続的な稼働を確保する。

[39] 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GSOCシステムを運用する体制のこと。2008年4月から運用を開始した政府機関等に対する監視体制（第一GSOC）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）がある。

加えて、コロナ禍を契機としたテレワークやクラウドの浸透によって、新たなセキュリティリスクが顕在化していることから、国は「新たな生活様式」を安全・安心に実現できる対策を講じる。特に従来の「境界型セキュリティ」だけでは対処できないことも現実となりつつあることから、国はこうした状況に対応したシステムの設計、運用・監視、インシデント対応、監査等やそれを担う体制・人材の在り方を検討する。

また、複雑化・巧妙化しているサイバー攻撃に鑑みれば、近年は、対策が手薄になりがちな海外拠点や中小企業等を含めた委託先を狙う等サプライチェーン全体を俯瞰したセキュリティ対策の必要性が増している。そのため、企業規模等に応じた実効性を見極めつつ、国はこのような新たな脅威に対し効果的なセキュリティ対策を進めていく。

具体的には、「クラウド・バイ・デフォルト原則」[40]に対応したセキュリティ対策として、国はクラウドサービスの利用拡大を見据えた政府統一基準群[41]の改定と運用やクラウド監視に対応した GSOC 機能強化の検討を実施する。

また、国は第 4 期 GSOC（2021 年度～2024 年度）を着実に運用するとともに、従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討と政府統一基準群の改定を行い、可能なところから率先して導入を進め、政府機関等における実装の拡大を進めていく。併せて、GSOC 等の在り方も検討する。

国は行政分野におけるサプライチェーン・リスクや IoT 機器・サービス（制御システムの IoT 化も含む）への対応を強化する。

国は情報システムの設計・開発段階から講じておくべきセキュリティ対策（認証機能、クラウドサービス等における初期設定、脆弱性対応等）を実施する。

国はセキュリティ監査や CSIRT 訓練・研修等を通じて政府機関等におけるサイバーセキュリティ対応水準を維持・向上する。

４．２．４　経済社会基盤を支える各主体における取組②（重要インフラ）

我が国の経済や社会は、様々な重要インフラサービスの継続的な提供に依存しているが、重要インフラ間の相互依存性の高まりやサプライチェーンの複雑化・グローバル化を踏まえると、安全で安心な社会の実現には、脅威が年々高まっている重要インフラのサイバーセキュリティを確保し、強靭性を高めることが不可欠である。

基本法では、重要インフラ事業者の責務を明確に定めるとともに、国は、重要インフラ事業者等のサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他自主的な取組の促進その他必要な施策を講ずるよう規定されている。

こうしたことを踏まえ、重要インフラに関わる各主体がそれぞれの責務を認識し、官民が一体となって堅牢な重要インフラの実現に向けた取組を推進する。

（１）官民連携に基づく重要インフラ防護の推進

国民生活及び社会経済活動の基盤である重要インフラサービスの安全かつ持続的な提供のため、重要インフラ防護に責任を有する国と自主的な取組を進める事業者等との共通

40　クラウドサービスの利用を第一候補とした、政府情報システムにおけるクラウド・バイ・デフォルトの基本的な考え方を整理したもの。

41　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。

の行動計画を官民で共有し、これを重要インフラ防護に係る基本的な枠組みとして引き続き推進する。

重要インフラを取り巻く脅威は年々高度化・巧妙化しているが、その一方で、重要インフラ分野ごとにシステムの利用形態が異なることから、各組織における脅威の差異が拡大してきている。このことを踏まえ、重要インフラ防護のよりどころとなる現行の「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」[42]を基本としつつ、重要インフラ分野が全体として今後の脅威の動向、システム、資産を取り巻く環境変化に柔軟に対応できるようにするため、国は行動計画を積極的に改定し、官民連携に基づく重要インフラ防護の一層の強化を図る。

重要インフラサービスの安全かつ持続的な提供において、デジタル技術は大きな役割を果たすものであり、サイバーセキュリティの確保は経営の根幹に関わるものである。この認識の下、ビジネスとセキュリティのバランスが取れ、先進的でセキュリティ対策が適切に講じられた重要インフラサービスの実現を確実なものとするため、国は各組織が先行事例で得られた教訓を有効に生かせるよう、重要インフラ事業者等による情報収集を円滑にするための横断的な情報共有体制の一層の充実を図るとともに、セキュリティ対策は組織一丸となって取り組むことが重要であることから、国は経営層のリーダーシップが遺憾なく発揮できる体制の構築を図っていく。

（２）地方公共団体に対する支援

地方公共団体は、個人情報等の多数の機微な情報を保有し、国民生活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セキュリティが確保されるよう、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。

「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」[43]に基づくセキュリティ対策が着実に実施されるよう、国は人材の確保・育成及び体制の充実並びに必要な予算を確保するための取組を支援する。

地方公共団体情報システムの標準化、行政手続のオンライン化、「クラウド・バイ・デフォルト原則」等を受けたクラウド化、働き方改革や業務継続のためのテレワークの導入等、新たな時代の要請に柔軟に対応できるよう、国は同ガイドラインの継続的な見直し等、必要な諸制度の整備を推進する。

地方におけるデジタル改革（デジタル・ガバメントの実現）を促進するため、国は、「デジタル社会の実現に向けた改革の基本方針」[44]を踏まえ、整備方針において、地方公共団体のセキュリティについての方針を規定する。

国民生活・国民の個人情報に密接にかかわるマイナンバーについて、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。

---

[42] 重要インフラ防護に係る基本的な枠組みとして、重要インフラ防護に責任を有する政府と自主的な取り組みを進める重要インフラ事業者等との共通の行動計画を策定し、これを推進してきた。昨今のサイバー攻撃による急速な脅威の高まりや、東京大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第 3 次行動計画を見直したもの。

[43] 2020 年 12 月に総務省において改定。各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。

[44] 2020 年 12 月 25 日閣議決定。「デジタル社会の将来像」、「IT 基本法の見直しの考え方」、「デジタル庁（仮称）設置の考え方」等について、デジタル・ガバメント閣僚会議の下で開催されたデジタル改革関連法案ワーキンググループにおける議論も踏まえ、政府としての方針を示すもの。

４．２．５　経済社会基盤を支える各主体における取組③（大学・教育研究機関等）

大学・大学共同利用機関等（以下「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や、多様なシステムを有するという実態を踏まえ、その自律的な対策はもちろん、連携協力体制の構築や情報共有等において、国の積極的な支援が重要である。

そのため、国は大学等に対して、サイバーセキュリティに関するガイドライン等の策定・普及、リスクマネジメントや事案対応に関する研修や訓練・演習の実施、事案発生時の初動対応への支援や、情報共有等の大学等の連携協力による取組を推進する。

また、先端的な技術情報等を保有する大学等については、国は組織全体に共通して実施するセキュリティ対策のみならず、当該技術情報等を高度サイバー攻撃から保護するために必要な技術的対策や、サプライチェーン・リスクへの対策を強化できるよう取組を支援する。

４．２．６　多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

サイバー空間におけるリスクの高まりを踏まえ、国は、リスクへの感度とレジリエンスを高め、実効性かつ即応性のあるサイバー攻撃対処に資する、時間的・地理的・分野的にシームレスな情報共有・連携を推進し、平時から大規模サイバー攻撃事態等に対する即応力を確保する。

また、新たな攻撃にも国全体として網羅的な対処が可能となるよう、国はナショナルサート（CSIRT/CERT）の枠組み整備の一環として、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見、ノウハウを活かすことで、大阪・関西万博をはじめとする大規模国際イベント時だけではなく、平時における我が国のサイバーセキュリティ全体の底上げを進める。また、国は東京大会での運用で得られた知見、ノウハウを適切な形で国際的にも共有していく。

（１）分野・課題ごとに応じた情報共有・連携の推進

サイバー空間における各主体の有機的な連携による多層的なサイバー防御体制の構築を図る観点から、各主体との緊密な連携の下、国は ISAC を含む既存の情報共有における取組を充実・強化するほか、情報共有に関する新たな枠組みの構築・活性化を支援する。

（２）包括的なサイバー防御に資する情報共有・連携体制の整備

サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備の一環として、国はサイバーセキュリティ協議会やサイバーセキュリティ対処調整センターをはじめとした情報共有体制間の連携を進め、外部との連携や調整の在り方について具体的に検討する。

また、国は東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見やノウハウを、東京大会の運営を支える事業者等にとどまらず、広く全国の事業者等におけるサイバーセキュリティ対策への支援等として積極的に活用することで、大阪・関西万博をはじめとする大規模国際イベント時から、平時に至る我が

国のサイバーセキュリティ全体の底上げを進める。

４．２．７　大規模サイバー攻撃事態等への対処態勢の強化

サイバー空間と実空間の一体化がますます進展し、インシデントの影響が広範囲に伝播するおそれやこれを考慮した被害予測等を踏まえ、国は平時から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化する。

また、国は分野や地域のコミュニティを活用してサイバー攻撃への対処態勢の強化に努めるとともに、官民連携により情報収集・分析・共有機能を強化する。

更に、国及び各主体は官民連携の取組等を通じてセキュリティ人材を育成及び活用することで、大規模サイバー攻撃事態等への対処を強化する。

４．３　国際社会の平和・安定及び我が国の安全保障への寄与

我が国を取り巻く安全保障環境は、厳しさを増しており、我が国が享受してきた既存の秩序についても、不確実性が急速に増している。政治・経済・軍事・技術を巡る国家間の競争の顕在化を含め、国際社会の変化の加速化・複雑化が進展している。

サイバー空間についても、地政学的緊張も反映しつつ、平素からこうした国家間の競争の場となっている。高度なサイバー能力を有する軍等が他国の重要インフラへのサイバー攻撃を行ったとされている事例も指摘される等、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おり、社会のデジタル化が広範かつ急速に進展する中、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。また、サイバー空間を利用した影響工作や、主体、被害等の把握が困難なサイバー攻撃等は、ときに軍事活動と複合的に組み合わされることにより、武力攻撃に至らない形での現状変更の試みに利用されうる。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[45]。加えて、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・増強が引き続き行われているとみられている[46]。一方、同盟国である米国や基本的価値観を共有する同志国においても、サイバー脅威に対応するため、サイバー軍の能力構築が加速されるとともに、サイバー攻撃対処能力の強化が進められている[47]。

こうした中で、各国において同盟国・同志国との協力・連携を強化する重要性が認識されており、特に、国家の関与が疑われるサイバー事案やサイバー空間に関する国際ルール等をめぐる対立に対して同盟国・同志国等が連携して対抗している。2021 年 3 月に行われた日米安全保障協議委員会（以下「日米『2+2』」という。）及び日米外相会談においては、この分野を一層強化していくことの重要性が確認された。加えて、近年、安全保障の裾野が経済・

45　中国、ロシア及び北朝鮮によるサイバー攻撃等については「G7 首脳コミュニケ」（2021 年 6 月）、「G7 外相コミュニケ」（2021 年 5 月）、「国連安全保障理事会北朝鮮制裁委員会専門家パネルによる最終報告書」（2021 年 3 月）、米国国家サイバー戦略（2018 年 9 月）、米国国防省サイバー戦略（2018 年 9 月）を参照。
なお、公安調査庁「サイバー空間における脅威の概況 2021」及び警察庁警備局「治安の回顧と展望」（2020 年 12 月）において、個別事案に係る米国等の発表に触れつつ、中国、ロシア及び北朝鮮の軍・情報機関等の関与が指摘されているとしている。また、中国に関しては、注釈 53 も参照。

46　防衛省「令和 2 年版防衛白書」（2020 年 7 月 14 日閣議報告）

47　防衛省「令和 2 年版防衛白書」（2020 年 7 月 14 日閣議報告）

技術分野にも一層拡大している中で、技術基盤やデータをめぐる争いについても、同様に同盟国・同志国等と連携して対抗している。

このような中で、「自由、公正かつ安全なサイバー空間」を確保し、国際社会の平和・安定及び我が国の安全保障に寄与することの重要性は一層高まっている。サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を一層強化する。

４．３．１　「自由、公正かつ安全なサイバー空間」の確保

グローバル規模で「自由、公正かつ安全なサイバー空間」を確保するため、国際場裡において我が国の基本的な理念を発信していく。また、サイバー空間における法の支配の推進及びこのような我が国の基本的な理念に沿った国際ルール形成のため、引き続き、同盟国・同志国と連携し、積極的な役割を果たしていく。

（１）サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）

国際社会の平和と安定及び我が国の安全保障のため、サイバー空間における法の支配を推進することが重要である。

グローバル規模で「自由、公正かつ安全なサイバー空間」を確保するため、引き続き国際場裡においてその理念を発信し、サイバー空間における法の支配の推進のため積極的な役割を果たしていく。特に、コロナ禍において医療機関へのサイバー攻撃が多くの国で見られ、こうした攻撃を抑止し、また、重要インフラを防護するためにもサイバー空間において法の支配を推進することが一層の重要課題となっている。国連等においては、サイバー空間においても既存の国際法の適用を前提とし、サイバー空間における規範などの実践にも積極的に取り組んでいく立場から、国際法の適用に関する我が国の見解を積極的に発信し、「自由、公正かつ安全なサイバー空間」の確保のため同盟国・同志国と連携していく。そのような活動を通じ、我が国の安全保障及び日米同盟全体の抑止力向上の取組に資するよう、国内外における国際法の適用に関する議論・規範の実践の普及に取り組んでいく。

サイバー犯罪対策については、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とともに、国連における新条約策定に関する議論に十分関与することを通じ、サイバー空間における法の支配及び一層の国際連携を推進する。

（２）サイバー空間におけるルール形成

G20 大阪首脳宣言においてデジタル経済における「信頼性のある自由なデータ流通(Data Free Flow with Trust: DFFT)」を促進する必要性が確認されたこと、「プラハ提案」[48]において 5G セキュリティにおけるトラストの重要性が言及されたこと等に見られるように同盟国・同志国等と連携した国際的な取組に向けた動きが進展している。また、我が国が目指す「自由、公正かつ安全なサイバー空間」の秩序形成に向けては、インターネット・

[48] 「プラハ提案」とは、プラハ 5G セキュリティ会議における議長声明（2019 年 5 月）を指す。

ガバナンス・フォーラム等インターネット・ガバナンスに関するマルチステークホルダー・アプローチでの枠組みも発展してきている[49]。

他方、既存の秩序とは相容れないおそれのある提案が行われていること等も踏まえ、引き続き国際社会に対して我が国の基本理念を発信し、我が国の基本理念に沿う新たな国際ルールの策定に積極的に貢献するとともに、こうした国際社会の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国際ルールの変更を目指す取組については、同盟国・同志国や民間団体等と連携して対抗する。

４．３．２　我が国の防御力・抑止力・状況把握力の強化

我が国を取り巻く安全保障環境が厳しさを増している中、政府機関、重要インフラ事業者、先端技術を有する企業・学術機関等への攻撃や、民主主義の根幹を揺るがしかねない事例も発生している。さらに、それらの中には国家の関与が疑われる事案も存在する。

以上を踏まえ、サイバー攻撃から我が国の安全保障上の利益を守るため、サイバー攻撃に対する国家の強靱性を確保し、サイバー攻撃から国家を防御する力（防御力）、サイバー攻撃を抑止する力（抑止力）、サイバー空間の状況を把握する力（状況把握力）をそれぞれ高めつつ、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。

これら安全保障に係る取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は内閣サイバーセキュリティセンターを中心として官民を問わず全ての関係機関・主体、抑止は対応措置を担う省庁、状況把握は情報収集・調査を担う機関が、平素から緊密に連携して進める。また必要な場合には、国家安全保障会議で議論・決定を行う。

また、こうした政府全体の安全保障に係る取組の中で、防衛省・自衛隊は、「平成 31 年度以降に係る防衛計画の大綱」に基づき、各種の取組を進め、サイバー防衛に関する能力を抜本的に強化する。

（１）サイバー攻撃に対する防御力の向上

① 任務保証

政府機関は、国民生活や経済社会を守り、支える任務を有しており、その機能停止は、安全保障上の重大な懸念事項である。政府機関の任務遂行は、重要インフラその他のシステムを担う事業者のサービスに依存している。また、これら事業者自身も、国民や社会に不可欠なサービスを提供するという重要な任務を有している。

任務保証の観点から政府機関及び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の推進が引き続き必要である。政府においては、安全保障上重要な情報を取り扱うネットワークについて、リスクの低減を含めた一層の防護を推進する。さらに、自衛隊及び米軍の活動が依拠する重要インフラ及びサービスの防護のため、自衛隊及び米軍による共同演習等を着実に実施していく。防衛省・自衛隊においては、サイバー関連部隊の体制強化等、サイバー防衛能力の抜本的強化を図る。

---

[49] G7 伊勢志摩首脳宣言（2016 年 5 月 27 日）において「我々は、政府、民間部門、市民社会、技術コミュニティ及び国際機関による十分かつ積極的な参加を含むインターネット・ガバナンスに関するマルチステークホルダー・アプローチを促進することにコミットする」としている。

② 我が国の先端技術・防衛関連技術の防護

我が国の安全保障上重要な情報等が狙われている中で、宇宙関連技術、原子力関連技術、その他先端技術等我が国の安全保障に関連する技術等につき、リスク低減を含めた一層の防護が必要である。特に防衛産業については、新たな情報セキュリティ基準の策定や官民連携の一層の強化等によりセキュリティ確保の取組を進めていく。また、国の安全保障を支える重要インフラ事業者や先端技術・防衛関連技術産業、研究機関といった関係事業者と国の一層の情報や脅威認識の共有及び連携を図る。

③ サイバー空間を悪用したテロ組織の活動への対策

サイバー空間は、個人や団体が自由に情報をやり取りし、自らの考えを述べる場を提供するものであり、民主主義を支えているものの一つである。他方、テロ組織が、過激思想の伝播や示威行為、組織への勧誘活用、活動資金の獲得等の悪意ある目的でサイバー空間を利用することは防止しなければならない。このため、表現の自由を含む基本的人権を保障しつつ、サイバー空間を悪用したテロ組織の活動への対策に必要な措置を引き続き国際社会と連携して実施する。

（２）サイバー攻撃に対する抑止力の向上

①　実効的な抑止のための対応

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[50]。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、被害者である国家は、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、一定の場合には、サイバー攻撃が国際法上の武力の行使又は武力攻撃となり得る[51]。

これらを踏まえ、我が国は、悪意ある主体の行動を抑止し、国民の安全・権利を保障するため、国家の関与が疑われるものも含め、サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる。この点に関し、2019 年の日米「2+2」において、一定の場合には、サイバー攻撃が日米安全保障条約第 5 条の規定の適用上武力攻撃を構成し得ることを確認したところである。また、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力も活用していくとともに、サイバー攻撃に関する非難等の外交的手段や刑事訴追等の手段も含め、然るべく対応していく[52]。刑事訴追等の例としては、2021 年 4 月に警察において書類送致した事件[53]への捜査等が挙げられる。この捜査等を通じ、国内企業等への攻撃を実行したサイバー攻撃集団の背景組織として、中国人民解放軍が関与している可能性が高いと評価するに至っ

[50] 2015 年国連第 4 会期政府専門家会合報告書において、サイバー空間に対する国連憲章全体を含む既存の国際法が適用されることが確認され、2021 年国連オープンエンド作業部会報告書においても同趣旨を再確認した。

[51] G7 伊勢志摩サミット　サイバーに関する G7 の原則と行動（2016 年 5 月）

[52] これまで同盟国・同志国と連携して、2017 年にも「ワナクライ」事案の背後に、北朝鮮の関与があったことを非難する外務報道官談話を発出し、2018 年には中国を拠点とする APT10 といわれるグループによるサイバー攻撃について非難する旨の外務報道官談話を発出している。

[53] 2021 年 4 月に警視庁が中国共産党員の男を被疑者として、東京地方検察庁に書類送致した事件。本件に関し、2021 年 4 月 20 日の内閣官房長官記者会見では、「本件捜査を通じて、契約された日本のレンタルサーバーが、JAXA 等に対するサイバー攻撃に悪用されたこと、またその攻撃には中国人民解放軍 61419 部隊を背景に持つ「Tick」と呼ばれるサイバー攻撃集団が関与した可能性が高いことが判明したとも承知をしております。」としている。

たところであり、今後も警察組織内に設置される実働部隊をはじめとした捜査機関による厳正な取締りを進めていく。

また、サイバー攻撃は、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ことから、平時・大規模サイバー攻撃事態・武力攻撃という事態のエスカレーションにもシームレスに移行することで、迅速に事態に対処するとともに、2021 年 3 月の日米「2+2」の成果を踏まえ、引き続き日米同盟の抑止力を維持・強化していく。

②信頼醸成措置

サイバー攻撃を発端とした不測の事態の発生や悪化を防止するため、国家間の信頼を醸成する。サイバー空間は匿名性、隠密性が高く、意図せず国家間の緊張が高まり、事態が悪化するリスクがある。このように、偶発的又は不必要な衝突を防ぐため、国境を越える事案が発生した場合に備え、信頼醸成措置として国際的な連絡体制を平素から構築することが重要である。

また、二国間・多国間の協議における情報交換、政策対話等を積極的に行うことを通じ、透明性を高め、国家間の信頼を醸成する必要がある。各国と協力し、サイバー空間の問題を調整するメカニズムを活用する。

（３）サイバー空間の状況把握力の強化

① 関係機関の能力向上

状況把握力は、防御力ひいては抑止力の基盤である。深刻化するサイバー攻撃やサイバー空間を利用した影響工作の脅威を抑止していくためには、対応力の強化に加え、攻撃者を特定し、責任を負わせるために、サイバー攻撃等を検知・調査・分析する十分な能力が求められる。このため、関係機関におけるこうした能力を質的・量的に引き続き向上させ、関係機関の全国的なネットワーク・技術部隊・人的情報も駆使しながらサイバー攻撃等の更なる実態解明を推進する。

加えて、高度な分析能力を有する人材の育成・確保、サイバー攻撃等を検知・調査・分析等するための技術の開発・活用等あらゆる有効な手段について幅広く検討を進める。また、カウンターサイバーインテリジェンス[54]に係る取組を進める。

② 脅威情報連携

国家の関与が疑われるサイバー攻撃、非政府組織による攻撃等多様な脅威に的確に対処し、抑止するため、政府内関係省庁及び同盟国・同志国との情報共有を推進する。また、内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。

４．３．３　国際協力・連携

サイバー空間においては事象の影響が容易に国境を超え、他国で生じたサイバー事案は我が国にも容易に影響を及ぼす可能性があることから、各国政府・民間等様々なレベルで重層的に協力・連携することが重要である。このため、知見の共有・政策調整、サイバー事案等に係る国際連携及び能力構築支援を推進する。

[54] 情報通信技術を用いた外国の諜報活動に対抗する情報防衛活動

（１）知見の共有・政策調整

国際ルールや技術基盤をめぐる争いが顕在化する中、米国その他同志国等とのサイバー協議に見られるハイレベルでの省庁横断的な二国間協議及び多国間協議のほか、内閣官房や各府省庁のそれぞれのカウンターパートにおいて平素から実務的な国際連携を実施する重層的な枠組みを強化し、同盟国・同志国との連携を強化する。「自由で開かれたインド太平洋（Free and Open Indo-Pacific: FOIP）」の実現に向けた、サイバーセキュリティ分野における米豪印やASEAN[55]等との協力についても積極的に推進する。

また、民間における情報共有に係る国際連携も拡大するとともに、国際場裡で我が国の立場を主張できる官民の人材を確保し、他国への人材派遣や国際会議への参加等を通じて育成する。加えて、我が国のサイバーセキュリティ政策等に関する国際的な情報発信も強化し、東京大会における我が国の経験等も他国に共有し国際貢献を果たす。

（２）サイバー事案等に係る国際連携の強化

サイバー事案への迅速な対応や被害の拡大防止のため、サイバー攻撃関連情報（脆弱性情報やIoC[56]情報など）に関する平素からの国際的な情報共有を引き続き強化し、他国と共同した情報発信を検討する。CERT間連携や国際サイバー演習への参加のみならず、我が国が国際サイバー演習等を主導して連携対処のための信頼関係を構築するとともに、情報のハブとなり、サイバーコミュニティにおける国際的なプレゼンスの向上を図る。

（３）能力構築支援

国際的な相互依存関係が進む現在、我が国の平和と安全は我が国一国のみでは確保できない。我が国の安全保障の確保に寄与するためには、全世界的に連携してサイバーセキュリティ上の脆弱性を低減し、撲滅を目指していくことが肝要である。このような観点から、世界各国におけるサイバーセキュリティの能力構築を支援することは、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定を確保し、当該国の健全なサイバー空間の利用の進展を促すのみならず、サイバー空間全体の確保と直結しており、ひいては我が国を含む世界全体の安全保障環境の向上に資する。

能力構築支援については、他国においても様々な支援が実施されている中、我が国の基本的な理念の下、産官学連携や外交・安全保障を含めた取組の強化を示す能力構築支援の基本方針[57]に基づき、求められる支援を、同志国、世界銀行等の国際機関、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な支援を実施していく。

このようなサイバーセキュリティの確保によりSDGsの達成を促進するほか、サイバーハイジーンの確保につなげていく。また、人材育成やサイバー演習のみならず、国際法理の理解・実践、政策形成、技術基準策定や5G、IoTといった次世代のサイバー環境を形成する分野においても、能力構築支援を実施していく。加えて、海外へのサイバーセキュリ

[55] 東南アジア諸国連合（Association of South‐East Asian Nations）
[56] IoC (Indicator of Compromise)。サイバー攻撃の痕跡を表す情報
[57] （策定後記入）

ティに係るビジネス展開を後押ししていく[58]。

こうした取組に加え、特にASEANを含むインド太平洋地域については、能力構築支援を中心としたこれまでの成果と経験、また、その地政学的な重要性を踏まえ、サイバー分野における外交・安全保障を含めた連携の抜本的な強化を図る。

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、その特質から、脅威に関する情報やユーザー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礎となる研究開発の国際競争力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、研究開発の推進にはIT関連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、様々な分野からを含む研究人口の流入により、世界的に論文投稿数が急成長するなど若く伸びており、国際共著・産学官連携論文などコラボレーションが活発な研究分野となっている。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。

我が国でも研究者が増えている一方、経済社会のデジタル化により社会的要請が更に高まっており、我が国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。

---

[58] 「インフラシステム海外展開戦略2025」（2020年12月経協インフラ戦略会議決定）

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取り巻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。

戦略期間において、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」[59]をはじめとするネットワーク技術の高度化など、IT 関連技術の進展に応じ、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、

[59] 5G の特徴的機能の更なる高度化、持続可能で新たな価値の創造に資する機能の付加を指す。

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。

４．４．２　人材の確保、育成、活躍促進

サイバー攻撃が複雑化・巧妙化する中、企業が事業継続を確固なものとしつつ、新たな価値を創出していくためには、サイバーセキュリティ確保に向けた人材の育成・確保が不可欠である。我が国におけるサイバーセキュリティ人材の不足が指摘されて久しいが、一方で、実務者層・技術者層の育成に向けては、資格・試験や演習、学び直しの促進等の官民の取組も進展している。こうした現状認識やデジタル化に向けた取組の広がりを踏まえれば、「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要である。

また、デジタル化がそれに応じた脅威への対処とあわせて推進されていくためには、サイバーセキュリティに係る人材が、男女等を問わず多様な視点や優れた発想で幅広く活躍できる環境をつくり、次代を担う優秀な人材を引きつけられる好循環を生むことが重要である。このため、環境変化に対応して以下の政策目的に適った取組の重点化を図るとともに、優秀な人材が民間、自治体、政府を行き来しながらキャリアを積める環境整備に取り組んでいく。

（１）「DX with Cybersecurity」に必要な人材に係る環境整備

デジタル化の進展とあわせてサイバーセキュリティ確保に向けた取組を同時に推進すること（DX with Cybersecurity）が社会全体で実現されるためには、企業・組織内でのデジタル化進展に伴い新たに必要となるセキュリティを含む人材・仕事の需要の増加と、若年層や社会的要請に応じた人材流入や適切なマッチング等による人材・仕事の供給の増加が、双方とも連関して好循環を形成することが重要である。

実務者層・技術者層向けの人材育成プログラムの「質」・「量」の確保はもちろん、企業・組織内での機能構築、人材の流動性・マッチングの観点から、セキュリティ人材が活躍できるような環境整備が図られなければ、悪循環に陥り、経済社会のデジタル化推進は不確実性をはらむものとなり得る。

加えて、そのためには、経営層はもちろん、企業・組織内でデジタルトランスフォーメーションを推進したり関与したりする様々な者において、デジタル化とサイバーセキュリティ対策は他人事ではなく、同時達成されるべき、業務と収益の中核を支える基本的事項として認識されることがその前提となる。経営層の意識改革に取り組みつつ、必要な素養や基本的知識が補充できる環境整備が重要となる。

① 「プラス・セキュリティ」知識を補充できる環境整備

経営層や、特に企業・組織内でDXを推進するマネジメントに関わる人材層をはじめとして、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様々な人材に対して「プラス・セキュリティ」知識が補充され、内外のセキュリティ専門人材との協働等が円滑に行われることが、社会全体で「DX with Cybersecurity」を推進していく上で非常に重要である。同時に、経営層の方針を踏まえた対策を立案し実務者・技術者を指導できる人材の確保に向けた取組も重要であり、これらの取組により「戦略マネジメント層」の充実を図る。

しかしながら、ITリテラシーや「プラス・セキュリティ」知識に係る研修・セミナー等の人材育成プログラムは、社会的に必ずしも普及していないと考えられる。このため、環境整備の一環として、人材育成プログラムの需要と供給に係る対応を双方行い、市場の形成・発展を目指していく。

需要に係る観点からは、「DX with Cybersecurity」に取り組む様々な企業・組織内において、これまで専門知識や業務経験を必ずしも有していない人材（経営層を含む）が、今後デジタル化に様々に関わるためにITリテラシーや「プラス・セキュリティ」知識を補充しなければならない必要性は増しており、潜在的な大きな需要が存在すると考えられる。このため、様々な企業・組織において、人材育成プログラムを受講する呼びかけ等が行われることや、職員研修等の機会が提供されることが重要であり、こうした需要の顕在化につながる取組を企業・組織等に促す普及啓発を、国や関係機関・団体が先導して行う。

また、国や人材育成プログラム等を提供する関係機関・企業・教育機関等が、先導的・基盤的なプログラム提供を図ることに加え、趣旨に適うプログラムを一覧化したポータルサイト等を通じて官民の取組の積極的な発信を行うなど、企業・組織の需要者からみて供給側の一定の質が確保・期待される仕組みの構築を図る。これとあわせ、対策推進に向けた専門人材との協働等に資するよう、法令への理解を深めるツール等の活用促進を図る。

② 企業・組織内での機能構築、人材の流動性・マッチングに関する取組

今後、業務等のデジタル化、製品等のネットワーク接続、デジタルサービスの開発や他のサービスとの連携などが増加する中で、迅速で柔軟な開発・対処、新たなリスクに対応した監視・対処のプラクティスが必要となる。特に、前者の実践に当たっては「セキュリティ・バイ・デザイン」の考え方の重要性も一層増し、企画部門や開発運用部門と企業・組織内のセキュリティ機能との連携・協働が一層重要となると考えられる。一方で、こうした機能の構築や普及に向けては、必ずしも参照できる導入事例や人材の蓄積が十分とは言えないのも事実である。

また、人材の活躍の場という観点では、コロナ禍への対応の結果として雇用環境の変化や労働時間管理のあり方の明確化等を踏まえ、兼業・副業といった柔軟な雇用形態の活用の機会が今後増していくと考えられる。また、デジタル改革の動きを踏まえ、国の機関のみならず、地方自治体を含め、行政分野における業務改革を含むデジタル化関連業務における人材需要が今後増していくと考えられる。社会全体で「DX with Cybersecurity」を推進していくためには、働き方や雇用形態の多様化、デジタル改革の推進を機会としてIT・セキュリティ人材の流動性・マッチング機会の促進が図られるための環境整備が必要である。

したがって、これらの動向や人材の偏在等を考慮しつつ、企業・組織内での機能構築やIT・セキュリティ人材の確保・育成に関するプラクティス実践の促進に向け、人材ニーズに係る実態把握とあわせ、実際のインシデントを踏まえた普及啓発や、参考となる手引き資料の活用促進、人材の活躍等の先進事例の収集・整備、ポータルサイト等を通じた積極的な発信、学び直しの機会の提供に取り組む。

また、特に地域・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ころ、地域における「共助」の取組や、産業界と教育機関との連携促進・エコシステム構築を通じ、プラクティスの実践に当たって参考となるノウハウやネットワークの提供を行う。

（２）巧妙化・複雑化する脅威への対処

巧妙化・複雑化したサイバー攻撃の増大、サプライチェーンの複雑化・グローバル化に伴うリスクの増大、制御系システムを対象とする攻撃等もみられる中で、実践的な対処能力を持つ人材育成の重要性は一層増している。

実務者層・技術者層の育成に向けては、資格制度の整備・改善、若年層向けのプログラムや制御系システムに携わる実務者を対象とするプログラムの実施、演習環境の提供、学び直しの促進など、官民で取組の推進が行われてきているところ、近年の脅威動向に対応するとともに、男女や学歴等によらない多様な視点や優れた発想を取り入れつつ、これら実践的な対処能力を持つ人材の育成に向けた取組を一層強化し、コンテンツの開発・改善を図っていく。

また、社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、教育機関・教育事業者による演習事業実施が可能となるよう、講師の質の担保等に留意しつつ、産学に開放する。

なお、こうした人材の活躍促進やマッチング促進の観点から、多様な人材の活躍等の先進事例の発信、プログラムに参加した修了生同士のコミュニティ形成や交流の促進、資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進にもあわせて取り組む。

（３）政府機関における取組

IT・セキュリティ人材の活躍促進の観点からも、優秀な人材が、各府省庁、地方公共団体、民間企業、独立行政法人を行き来しながらキャリアを積める環境の整備が重要である[60]。この考え方を踏まえ、外部の高度専門人材を活用する仕組みの強化や、新たに創設される国家公務員採用試験「デジタル区分」合格者の積極的な採用、デジタル化の進展を踏まえた研修の充実・強化等に向けた方針に基づき、政府機関全体で取組を強化していく。

また、当該方針に基づき各府省庁において人材確保・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、定員の増加による体制整備、研修や演習の実施、適切な処遇の確保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。

特に、高度なサイバー犯罪や安全保障への対応等を行うため、外部の高度専門人材を活用するだけでなく、政府機関等内部においても独自に高度専門人材を育成・確保する。

４．４．３　全員参加による協働、普及啓発

サイバー空間と実空間の一体化の進展、サイバー攻撃の巧妙化・複雑化の中で、実空間における防犯対策や交通安全対策と同様に、サイバー空間における公衆衛生活動として、国民一人ひとりがサイバーセキュリティに対する意識・理解を醸成し、基本的な取組を平時から行い、様々なリスクに対処できることが不可欠である。リテラシーを身に付け、自らの判断で脅威から身を守れるよう、官民が一体となって行動強化につなげるための普及啓発・情報発信に取り組むことが重要である。

また、様々な関係者がお互いの役割分担の下で連携・協働することが何より重要である。国は、地域、企業、学校など様々なコミュニティの自主的な活動を尊重しつつ、各々の関係者が、お互いの役割分担の下で、連携・協働をできるような仕組みを構築し、その仕組みを下支えしていく役割を担う。

こうした認識の下で、普及啓発に向け産学官民の関係者が円滑かつ効果的に活動できるよう、「全員参加による協働」に向けた具体的なアクションプランを策定し、地域・中小・若年層を重点対象として、取組推進を行ってきた。本戦略では「Cybersecurity for All」という考え方を示しているが、これは「全員」が自らの役割を主体的に自覚しサイバーセキュリティに取り組む、という考え方を含んでいる。今後、デジタル改革の推進により、サイバー空間に参加する層が広がることが予想される中で、当該アクションプランを着実に推進することはもちろん、取組状況をフォローアップし、継続的な改善に

[60] 「デジタル社会の実現に向けた改革の基本方針」（2020 年 12 月 25 日閣議決定）にも示されている。

取り組んでいくことが求められる。また、高齢者への対応を含め、当該アクションプランの見直しを検討する。

加えて、特に、テレワークの増加やクラウドサービスの普及等の近年の人々の行動や企業活動の変化に応じて、ガイドラインや様々な解説資料等の整備が進められている。これらも含め、情報発信・普及啓発のあり方（コンテンツ）についても、必要な対応を実施する。

５　推進体制

本戦略においては、政府において進められているデジタル改革と一体となったサイバーセキュリティの確保が求められている[61]。また、サイバーセキュリティの確保を通じて、我が国の安全保障を万全のものとする[62]ことは、従来からの我が国政府の方針である。

我が国のサイバーセキュリティ政策により、「自由、公正かつ安全なサイバー空間」を確保するためには、政府一体となった推進体制が必要である。サイバーセキュリティ戦略本部（以下「本部」という。）は、本戦略に基づく取組が、デジタル庁が司令塔として推進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・連携強化を図る。その中で、内閣サイバーセキュリティセンターは、本部の事務局として、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担う。

本部は、新たに設置されるデジタル庁と、整備基本方針作成等における緊密連携を図る[63]。また、危機管理対応についても一層の強化を図ることが必要である。本部は、必要に応じて、重大テロ対策本部など危機管理体制と情報共有・連携する。さらに、安全保障にかかわる問題については、国家安全保障会議との緊密な連携により対応し、内閣官房国家安全保障局による全体取りまとめの下、関係省庁が連携して対応する。

本部は、変化するサイバーセキュリティリスクに対応して各主体に期待される具体的な対策につながるよう、また、国際協調の重要性を認識し、攻撃者に対する抑止の効果や各国政府に対する我が国の立場への理解を訴求するよう、各府省庁と連携して、本戦略を国内外の関係者に積極的に発信する。

また、本部は、本戦略で示された方向性に基づき、各府省庁の施策が着実かつ効果的に実施されるよう、経費の見積り方針を定め、政府としての必要な予算の確保と執行を図る。さらに、情報収集・分析機能に加え、サイバー攻撃の速やかな検知・分析・判断・対処を一体的サイクルとして行う機能の強化のため、所要の体制について検討する。本部は、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備を行う。

今後、本部は、本戦略を的確に実施するため、3 年間の計画期間内において、各年度の年次計画を作成するとともに、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。年次計画と年次報告は一体的に検討を行い、本戦略に

---

61 「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）

62 「国家安全保障戦略」（2013 年 12 月 17 日閣議決定・国家安全保障会議決定）は、「情報の自由な流通による経済社会やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠」としている。

63 デジタル庁設置法（令和 3 年法律第 36 号）附則第 43 条により、サイバーセキュリティ戦略本部員にデジタル大臣が加えられた。

基づく前年度の取組実績、評価及び次年度の取組を、本戦略の事項に沿って、報告と計画について一連の流れを示すように整理する。

資料１－３

サイバーセキュリティ戦略の案の作成に際しての
高度情報通信ネットワーク社会推進戦略本部意見

令和 3 年 6 月 30 日
高度情報通信ネットワーク社会推進戦略本部

１．デジタル庁の設置及びデジタル社会形成基本法の施行

令和 3 年 5 月 12 日に、デジタル庁設置及びデジタル社会形成基本法（以下、「新基本法」という。）制定等を柱とするデジタル改革に関する法律が可決・成立し、これに伴い高度情報通信ネットワーク社会形成基本法（以下、「IT 基本法」という。）は廃止されることとなった。

IT 基本法では、高度情報通信ネットワークの安全性及び信頼性の確保等により国民が高度情報通信ネットワークを安心して利用できるようにすることを掲げていたのに対し、新基本法では、情報通信ネットワークの安全性及び信頼性の確保に加え、情報の漏えい・滅失・毀損の防止、情報の安全管理によるサイバーセキュリティの確保のほか、情報通信技術を用いた犯罪の防止、情報通信技術を用いた本人確認の信頼性の確保、情報の改変の防止、高度情報通信ネットワークの災害対策など、クラウドをベースとしたデジタル社会の基盤となるシステム全体の安全性・信頼性確保を強力に推進することとなった。

また、「サイバーセキュリティ戦略本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ高度情報通信ネットワーク社会推進戦略本部の意見を聴かなければならない」とされている規定は廃止され、9 月 1 日のデジタル庁設置以降、デジタル大臣は、サイバーセキュリティ戦略本部の本部員に位置付けられ、サイバーセキュリティ戦略の案の作成及び実施に直接取り組むこととされている。

このように、デジタル庁が推進するデジタル改革において、サイバーセキュリティの確保は最重要課題の一つと認識しており、サイバーセキュリティ戦略本部とデジタル庁は、サイバーセキュリティの確保を含むデジタル改革に一体となって取り組む必要があると考える。

２．サイバーセキュリティ戦略の案について

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」等の目標設定、基本的な理念

における「情報の自由な流通の確保」をはじめとする 5 つの基本原則、デジタル技術とデジタルサービスの発展に伴うサイバー空間の量的・質的拡大といった現状認識とこれらが同時かつ相互影響的に進展するという将来予想はいずれも的確なものと考える。

なかでも、サイバー空間を巡る国際的な脅威が増大し、サイバー攻撃の手段が組織化・洗練化し、またゼロデイ攻撃が深刻化する中、「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の危機意識は強く同意するところである。

これに対し「Cybersecurity for All」の理念のもと講じようとしている各施策はいずれも重要な施策である。その際、この理念は、あらゆる国民、セクター、地域等サイバー空間に参画する「全員」が自らの役割を主体的に自覚し、サイバーセキュリティに取り組むという考えに基づくものであることをしっかり説明することが重要と考える。加えて、重要なのはスピード感をもって各施策を着実に実行し、その実施状況をモニタリングすることである。本案に明記されている通り、デジタル社会の形成に向けた司令塔たるデジタル庁が 9 月 1 日に設置されるなど、今が、我が国が後れを取ったデジタル化の時計の針を大きく進める絶好の機会であり、この機にあらゆる施策を一気呵成に推し進める必要があると考える。

３．デジタル庁が推進するデジタル改革と一体となったサイバーセキュリティの確保

デジタル庁では、社会のデジタル化を強力に進めるために、以下の取組をはじめ、デジタル改革と一体となったサイバーセキュリティの確保を、サイバーセキュリティ戦略本部と緊密に連携しつつ、推進することとしている。

（１）国等の情報システムの整備及び管理の基本的な方針（整備方針）において、内閣サイバーセキュリティセンターと緊密に連携してサイバーセキュリティについても基本的な方針を示し、その実装を推進する。
（２）デジタル庁が統括・監理する政府情報システムのセキュリティをゼロ・トラストの考え方に基づき強化するため、常時診断・対応型セキュリティアーキテクチャの実装等に取り組むとともに、クラウド・バイ・デフォルトを推進するために ISMAP 制度を活用し、その運用状況を踏まえた継続的な見直しに貢献する。
（３）政府情報システムを①デジタル庁システム、②デジタル庁・各府省共同プロジェクト型システム、③各府省システムの区分に分類し直した

上で、これらシステムに関する事業を統括・監理する。その際、デジタル庁にセキュリティ専門チームを置き、デジタル庁が整備・運用するシステムの検証・監査を実施する。

（４）セキュリティ専門チームの人材確保に努めるとともに、優秀な人材が、政府機関と民間企業を行き来しながらキャリアを積める環境の整備に努める。また、国家公務員採用試験に新たに創設される「デジタル区分」合格者の積極的な採用等ＩＴ・セキュリティ人材の確保に努める。

以上を踏まえた上で、閣サ第 483 号により意見聴取のあったサイバーセキュリティ戦略の案については異存ない。