参考資料５

次期サイバーセキュリティ戦略の骨子について

参考資料５－１　「次期サイバーセキュリティ戦略」（骨子）の概要

参考資料５－２　「次期サイバーセキュリティ戦略」の（骨子）

次期サイバーセキュリティ戦略の課題と方向性

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～

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 － DX with Cybersecurity －

- 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。

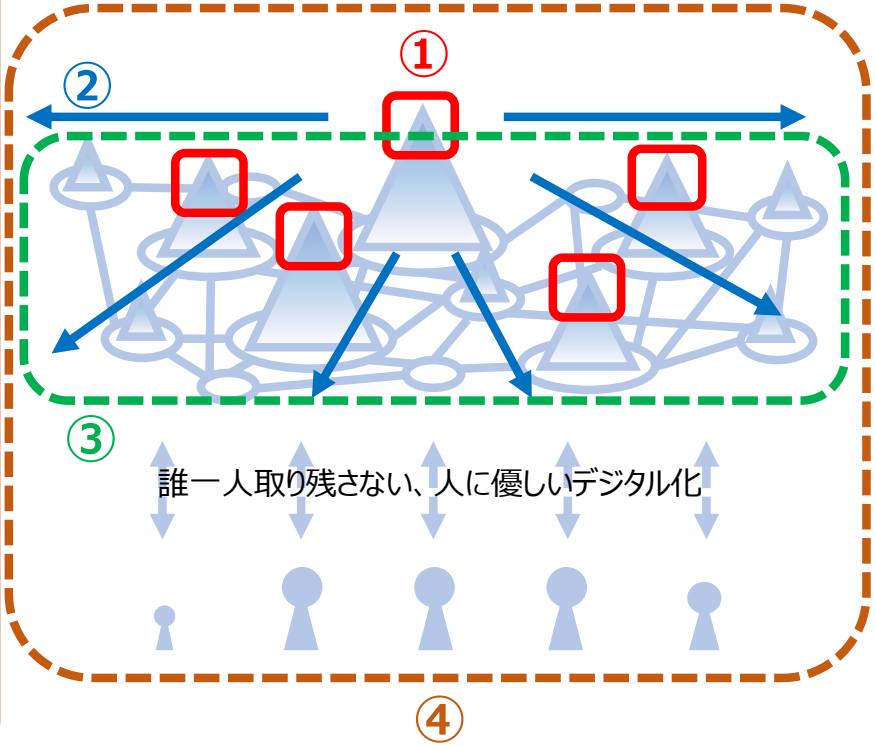
③ サプライチェーン等の信頼性確保に向けた基盤づくり

→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」の普及
- 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 インクルーシブなデジタル／セキュリティ・リテラシーの定着

→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

課題認識と方向性 ー 公共空間化・相互連関・連鎖が進展するサイバー空間の安全・安心確保

- 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。
- サイバー空間とフィジカル空間の垣根を超えて、経済社会活動の相互連関・連鎖が深化。
- サイバー攻撃の組織化・洗練化。

➡ 国が様々な主体と連携しつつ、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。

具体的施策

○ 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

○ 経済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

○ 多様な主体によるシームレスな情報共有体制と東京大会の知見等の活用

○ 大規模サイバー攻撃事態等の対処態勢強化

○ 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

◆安全安心なサイバー空間の利用環境の構築
①サプライチェーン管理
②IoT、5G等新技術・サービス実装への対応

◆新たなサイバーセキュリティの担い手との協調
（クラウドサービス等サイバー空間の技術・サービスを、利用者が安全と安心に利用できる取組）

◆サイバー犯罪対策への対応

◆包括的なサイバー防御の展開
（ナショナルCSIRT機能強化、対処官庁のリソース結集連携による対処能力向上等）

◆サイバー空間の信頼性確保に向けた取組
①国民個人情報や知的財産に関する情報の防護
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、その関与が疑われるサイバー攻撃を行っているとみられている。
- このようなサイバー攻撃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。

⇨ 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。

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

- 国連等における各種活動を通じたサイバー空間における法の支配の推進
- 我が国の基本理念に沿った国際ルール形成

② 我が国の防御力・抑止力・状況把握力の強化

- 防衛省・自衛隊におけるサイバー関連部隊の体制強化、重要技術・産業等のセキュリティ確保、日米連携の強化
- 全国的なネットワーク・技術部隊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

- 省庁横断的・各省庁における国際連携のための重層的な枠組みの強化
- ＡＳＥＡＮを含むインド太平洋地域における産官学が連携した能力構築支援

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

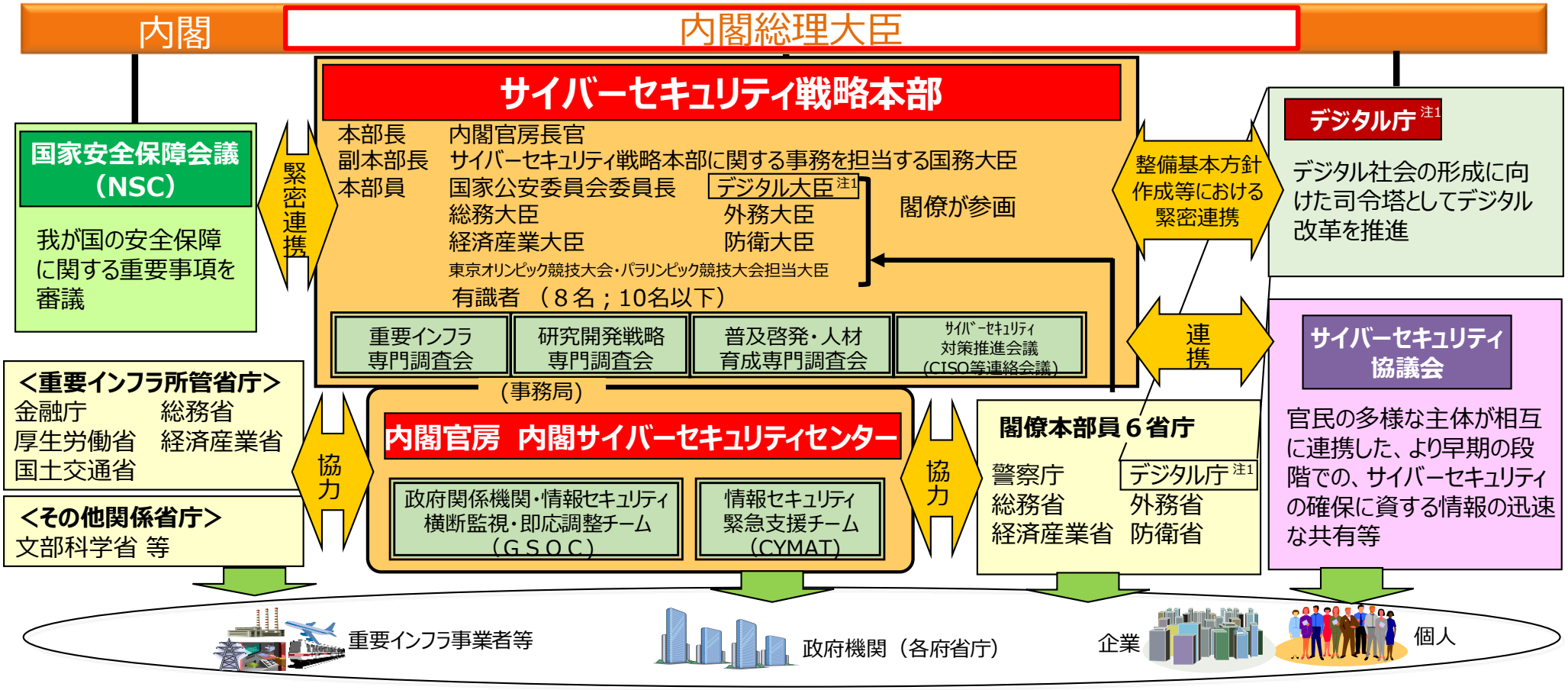
※2021年度前半に「強化方針」を改定

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、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。
- 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強化のための所要の体制を検討。
- 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案等(令和３年２月９日閣議決定)を基に記載。

「次期サイバーセキュリティ戦略」（骨子）の概要

中長期的

戦略期間

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、オリンピック・パラリンピックの取組の活用

2　基本的な考え

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

3－1　サイバー空間におけるリスクの増大

・新たな技術革新の浸透と依存度の高まり、クラウドサービス利用拡大と境界型セキュリティの限界、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、リテラシー差異や人材不足・偏在など攻撃者から狙われ得る弱点の顕在化、サイバー空間を巡る国際情勢

3－2　突き付けられている課題と方向性　～Cybersecurity for All～

・デジタル改革を踏まえた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

4　目的達成のための施策

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．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．インクルーシブなデジタル／セキュリティ・リテラシーの定着

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」の堅持

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

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。

参考資料５－２

次期サイバーセキュリティ戦略　骨子

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の策定は今回が3回目であり、基本法が制定された2015年から6年が経過した。この間、サイバー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。

・本戦略は、中長期的視点から、以下のような時代認識に立ち、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、そして本年開催される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。）という世界的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、攻撃者に対して発信するものである。

１．2020年代を迎えた日本をとりまく時代認識

①経済社会の環境変化　～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。

・デジタル経済の影響は、人々の生活そのものに波及。我が国のインターネット利用者は約9割[1]に達し、インターネットの利用時間は2時間を突破[2]。IoTやAI、5G、クラウドサービス等の利用拡大、テレワークの定着、遠隔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に。サイバー空間と実空間が高度に融合したSociety5.0[3]の実現が期待[4]。

・デジタル社会の形成に向けた司令塔として「デジタル庁」を設置することとし、「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」をビジョンに掲げるデジタル改革を推進。

②SDGsへの貢献に対する期待

・Society5.0の実現により、諸課題が解決された豊かな社会を迎えることができ、国連が掲げるSDGsにも貢献することが期待。

・我が国のグリーン成長の実現に向けても、スマートグリッドや製造自動化をはじめ、デジタル技術の活用が重要。

③安全保障環境の変化

---

[1] 総務省「令和元年通信利用動向調査」（令和2年5月29日）インターネット利用者の割合は全体の89.8%。80歳以上でも5割を突破。

[2] 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」（令和2年9月30日）

[3] 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）

[4] 既に「サイバー・フィジカル・スペース」の時代が到来している、との見解もある。

・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・複雑化が進展している。
・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。また、サイバー空間をめぐる情勢は純然たる平時でも有事でも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拡大する中、重大な事態へと急速に発展していくリスクをはらむ。
・また、サイバー空間に関する基本的価値の相違や、国際ルール・技術基盤・データ等をめぐる争いが顕在化している。

④新型コロナウイルスの影響・経験
・「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。テレワークやオンライン教育、遠隔診療などの取組が、コロナ禍への対応を余儀なくされることを通じて、加速的に進みつつある。
・また、この過程で「パーソナルデータ」を活用した新たなサービスの活用も進展。

⑤東京大会に向けた取組の活用
・東京大会に向けて行われた官民の取組を2025年大阪・関西万国博覧会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全体的な能力向上に活用。

２　基本的な考え

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。
・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。
・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、サイバーセキュリティ基本法の目的に資するべく、国は、同法に基づき、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である「サイバーセキュリティ戦略」を策定。
・上記の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、必要性はこれまで以上に増していると認識すべき。

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。

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。
・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。

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。
・また、同様に、サイバー空間では、国連憲章をはじめとした既存の国際法が適用されるべきであり、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。

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。
・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。これには、すべ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。
・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。

⑤多様な主体の連携
・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。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。
・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・外交その他の採り得るすべ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

・デジタル経済の浸透、デジタル改革の推進を通じ、サイバー空間そのものが量的に拡大・質的に進化するとともに、実空間との接点も面的に拡大。さらに、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。また、サイバー空間において提供される多様なサービスは、クラウドの普及やサプライチェーンの複雑化等に伴い、各主体間の相互連関・連鎖の関係がより進展。
・IoT、AI 技術、5G、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や、「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、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」の実現が目指されている。
・一方で、デジタル技術の活用は新たな課題も提示する。不適切に悪意をもって使用されれば、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[5]。従来は想定し得なかったリスクも同様に拡大することも想定され、また、こうした変化は、コロナ禍により不連続な形で進んでおり、予期しない形でリスクが顕在化するおそれがある。このような中で、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、サイバー空間に対する国民の不安感は払拭されていない状況にある。[6]
・こうした中、「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が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、中長期的な視点も同時に意識することが肝要。

３．１　サイバー空間におけるリスクの増大

３．１．１　環境変化からみたリスク

・環境変化と表裏一体に、脅威、そして社会全体としての脆弱性も拡大のおそれ。

①脅威の観点

・サイバー空間を通して新たな技術革新の恩恵を得るということは、自らの生命、身体、財産に関わる情報をこれまで以上にサイバー空間に委ねることになり、そうした情報は今後一層、サイバー攻撃の対象となり得ていく。
・また、AI を活用した自動攻撃や人間の制御によらない自律的攻撃など、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。

② 社会全体としての脆弱性の観点

・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り、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が期待される一方、セキュリティに関す

[5] 国連創設 75 周年記念宣言においても、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。
[6] 令和 2 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。

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、新たな脆弱性を生む危険性もはらんでいる。

・一方で、サービス高度化に伴ってデジタルサービス連携の間隙を突いた攻撃がみられるなど、適切なセキュリティ対策がとられなければ、それが即ち脆弱性となり得る。

・また、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 機器の利用拡大により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で、インシデントが発生した際の経済社会活動への影響は、より幅広く、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、リモートワークの拡大などとも相まって、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。

３．１．２　国際情勢からみたリスク

・サイバー空間が国家間の争いの場の一部となっていることを背景とし、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。

・こうしたサイバー攻撃の増大は、経済社会のデジタル化が広範かつ急速に進展する中、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が生じ、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、北朝鮮は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。また、これらの国において、軍をはじめとする各種機関の能力構築が引き続き行われているとみられている[7]。

・加えて、サイバー空間に関する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みられる。

・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

[7] 詳細は、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を参照。

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、脅威に晒される対象の拡大とともに、サイバー攻撃の手段が組織化・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。

３．１．３　近年のサイバー空間における脅威の動向

・かかる傾向は、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。

・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標的とされるケースが増加しており、コロナ禍に乗じたサイバー攻撃やグローバル化に伴う海外拠点を経由した攻撃など、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に大きな影響が生じている。

３．２　突き付けられている課題と方向性　～Cybersecurity for All～

・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、以下の課題認識と方向性の下、施策を推進する。

・これらは、基本法に掲げた目的である「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」を各々対象とするものであるが、前述の現状認識を踏まえれば、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。

（１）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

・現在、デジタル社会形成に関する司令塔として「デジタル庁」の設置が予定されるなど、経済社会全体でデジタル化が大きく推進される絶好の機会。

・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。逆に、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、個々の企業活動をみても、デジタル化進展の中で、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。また、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」の考え方が一層重要となり、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、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。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

・従来のサイバーセキュリティ戦略において、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、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。また、それ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おり、自律的な取組（「自助」）や多様な主体の緊密連携（「共助」）は引き続き重要であるが、その上で、それらの基盤となる「公助」の役割をはじめ、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。あわせて、ナショナルサート（CSIRT/CERT）[8]のミッション（機能）の明確化を図りつつ、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バリューチェーン全体の信頼性確保）

・従来の「任務保証」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。

[8] 2018 年に策定された従来戦略においては、「サイバー攻撃等に対してオールジャパンで力を合わせて対処するための調整役・調整窓口」としている。一般的に、CSIRT は Computer Security Incident Response Team の略、CERT は Computer Emergency Response Team の略である。

・近年、クラウドサービス普及やサプライチェーン複雑化等に伴い、サイバー空間を通じて提供される多様なサービスについて、バリューチェーン上に様々なプレーヤーが参画し、またクラウドサービス事業者等への依存度を増す中で、エンドユーザから見てサービス・業務の責任主体が見えにくくなっている。インシデントが発生した際の影響・波及の予見も難しくなりつつあり、クラウドサービスを例に挙げれば、これを利用する事業者のみならず、その事業者の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その影響はなおさらであることから、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バリューチェーン全体の信頼性を意識して行動することが求められる。
・「任務保証」は今後も重要であり引き続き推し進めるとともに、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バリュー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・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。
・各主体がその姿勢を明確化するとともに、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・外交その他の採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　目的達成のための施策

・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に基づき、今後３年間にとるべき諸施策の目標や実施方針を示す。

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。

・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。

・経営層の意識改革をはじめ、経済社会全体で意識やリテラシーを高める取組とともに、各主体の自律的取組を推進する観点から、地域・中小企業における DX with Cybersecurity の促進や、バリューチェーンの信頼性確保に向けた基盤づくりに取り組む。

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、企業の競争力としてより付加価値の高いデジタルサービスを生み出す基盤を有しているかが重要に。

・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して、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。サイバー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。

・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、デジタル経営に向けた行動指針の実践やツールの活用を通じ、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付されることなどにより、経営層によ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に取り組む。

・また、こうした取組を通して、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経営層が、自社の競争力の源泉たるデジタルサービスに内在するリスクの所在を把握できるよう、「プラス・セキュリティ」知識[9]を補充できる環境整備を推進する。

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

[9] 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人材が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。

・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、リソース（知見・人材）不足に直面。
・「共助」の考え方に基づくコミュニティ活動を全国に展開し、専門家への相談に留まらず、ビジネスマッチングや人材育成・マッチングなど、リソース不足を踏まえた地域による課題解決・付加価値創出の場の形成を促進する。
・また、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・簡易保険を普及させるため、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の審査・登録制度の運営等の取組を推進。
・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。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、設定等の不備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必要な取組を促すこと等を検討する。

４．１．３　バリューチェーンの信頼性確保に向けた基盤づくり

・サイバー空間とフィジカル空間が高度に融合する Society5.0 に向けて、あらゆる主体がバリューチェーン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、このようなバリューチェーンの下で新たに生じる課題への対応が必要に。
・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、バリューチェーンの信頼構築の基盤となる取組を推進。

（１）サプライチェーン

・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の観点では、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、バリューチェーン全体を見渡したリスク管理の重要性は増す。
・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・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、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様々な産業分野の団体等が参加する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ていく。

（２）データ流通

・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）」[10]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。

・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い出しの観点から、データマネジメントに関する定義の明確化（フレームワークの整備等）を進める。

・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。）を実効的なものとする必要。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

・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。また、今後はサプライチェーン・リスクへの懸念もある中、自社製品等の信頼性に対する、第三者による客観的な検証への需要が拡大し、産業として重要になっていくと考えられる。

・こうした観点から、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、一定の基準を満たすセキュリティサービスを審査・登録する取組等を通じ、信頼性確保の基盤づくりや日本発の製品・サービスの育成、海外市場への展開支援に取り組む。また、検証事業者の信頼性の可視化手法の検討に取り組む。

（４）先端技術・イノベーションの社会実装

・デジタル化進展の中で、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必要。

・また、我が国におけるセキュリティ製品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産学の結節点として開放していく。

・加えて、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。

[10] 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）

・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。

４．１．４　インクルーシブなデジタル／セキュリティ・リテラシーの定着

・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」[11]を進める中で、その恩恵を、インクルーシブに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（リテラシー）を身に付けていくことが必須。

・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、マイナンバーの普及やGIGAスクールの推進等が進み、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、能動的に体験を積んでいくことが何よりも重要。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、こうした機会を捉え、デジタル活用支援と連動をしながら、官民で連携して国民への普及啓発活動を実施していく。「GIGAスクール構想」の推進に当たっては、学校における環境整備の支援を行う「ICT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ほか、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。

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

・サイバー空間は、あらゆる主体が参画する公共空間へと進化し、また、各主体の諸活動の相互連関・連鎖がデジタル依存度の上昇と相まって一層深化している。このような現状に鑑み、あらゆる主体が、これまでの「任務保証」という考え方を、提供者と利用者間の一対一の関係のみで捉えるのではなく、サイバー空間全体を俯瞰する視点に立って、責任ある対応を取っていくことが求められる。

・その際、公共空間たるサイバー空間の安全を確保することによって、国民が安心して参画できるデジタル社会を実現できるよう、国は関係主体と連携し、自助及び共助を通じたサイバー空間に対する信頼の醸成と自律的なセキュリティ対策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、国は関係主体と連携し、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、特に防御すべき対象について不断に検証を行い、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、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

・サイバー空間が、あまねく主体が参画する公共空間に進化していることを踏まえ、その安全を確保し、全ての主体が利便性と安心を感じられる社会を実現しなければなら

[11] 「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）

ない。このため、国は関係主体と連携しつつ、サイバー空間を構成する財・サービスや主体間の関係性及びその潜在するリスクを把握可能とするトレーサビリティ（追跡可能性）や可視化を高める取組を進め、各々の主体が自らのニーズに合ったリスクマネジメントを適切に選択できる環境を醸成する。さらに、サイバー犯罪の温床となっている要素・環境の改善を図るためにも、トレーサビリティを確保するとともに、サイバー犯罪に関する警察への通報・相談を促進する。

・また、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・連鎖の深化に伴い、インシデントの影響が広範囲に伝播し、想定以上の被害が生じうることから、これらへの責任ある対応が不可欠となる。このため、国は関係主体と連携しつつ、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、バリューチェーン全体を俯瞰した安全・安心の確保に務めることがスタンダードとなるような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ることから、国が様々な主体と連携を図り、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、特に防御すべき対象を不断に検証することも重要。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、経済安全保障の観点も含めた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

・ 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、セキュリティ・バイ・デザインに基づく基盤構築などの指針等を策定するとともに、通信の秘密やプライバシーに留意しつつ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ことで、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。

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バリューチェーンの観点からのリスク管理等の必要な対策に取り組むべく、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。

・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。

・機器、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、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、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。

・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。

・自動運転、ドローン、工場の自動化、スマートシティ、暗号資産、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・行動規範を策定し、脆弱性対策への体制を整備する。

（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ている実態を踏まえ、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。具体的には、クラウドサービスをはじめ、サイバー空間を構成する技術やサービスについても、その設計、開発及び運用のライフサイクルのそれぞれの過程でサイバーセキュリティを担保することにより、利用者が自らニーズに合ったサービスを適切に選択し、安心を確保できる取組を強化する。

・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りつつあり、利用者が安心して情報資産を委ねる環境づくりを推進するため、政府情報システムのためのセキュリティ評価制度（ISMAP）等の取組を活用してクラウドサービスの安全性の可視化に取り組むとともに、クラウドサービス等のセキュリティが適切に確保されるよう、グローバルな連携を進める。

・なお、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、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。

（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、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。
・さらに、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。

（４）包括的なサイバー防御の展開

・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実効的な防御を行えるよう、国が持ち得る全ての能力と手段を活用し、網羅的な対処を講じる。
・具体的には、以下を実施する。

① オールジャパンで力を合わせて対処するため、外部との連携・調整、情報収集・分析、調査、注意喚起の実施、対策・対応の立案等のそれぞれの活動が包括的、有機的に機能し、国全体として網羅的かつ積極的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の機能強化、対処官庁のリソース結集と連携による対処能力の向上、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との連携を推進する。

② 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 」に係る諸施策、技術検証、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と連携して検討する。

（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、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。その際、このような情報の窃取は、あらゆるチャネルを通じて行われる傾向があることから、全体像を踏まえつつ、効果的な対策を講ずる。

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

・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。
・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、大学等における情報共有を促す取組を強化する。

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

・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や情報を扱う IT システム・サービスについて、サプライチェーン・リスクも勘案し、その安全性・信頼性を確保するための対策を推進する。
・国際海底ケーブル等のインフラ防護を強化する。
・IT 機器やサービスの安全性・信頼性の可視化を促すための基準作りや評価の取組を国際連携も念頭に置きながら推進。特に、我が国の IT 機器の安全性・信頼性の技術検証のための基準策定に着手するとともに、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。

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（整備方針）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。

・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。

・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情報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 GSOC 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。セキュリティは、社会全体のデジタル化の車の両輪として、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。

・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おり、「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り、これに対応したシステムの設計、運用・監視、監査等やそれを担う体制・人材の在り方を検討する。

・複雑化・巧妙化しているサイバー攻撃は、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。企業規模等に応じた実効性を見極めつつ、このような新たな脅威に対処した効果的な情報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・デフォルトに対応したセキュリティ対策として、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、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や GSOC 等の在り方を検討する。

・第 4 期 GSOC（令和 3 年度～6 年度）を着実に運用する。

・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。

・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。

・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。

・平成 26 年に公布・施行されたサイバーセキュリティ基本法では、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」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、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、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、経営層のリーダ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」（以下「ガイドライン」という。）に基づくセキュリティ対策が着実に実施されるよう、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、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」（令和２年 12 月閣議決定）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、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。

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、多様なシステムを有するという利用実態を踏まえ、その自律的な対策とともに、連携協力体制の構築や情報共有等の積極的な支援が重要である。

・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。

・先端的な技術情報等を保有する大学等については、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、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。

・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、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に関する全体的な能力の底上げを進める。また、東京大会の運用で得られた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。

（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、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。

・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に関する全体的な能力の底上げを進める。

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増々進展し、インシデントの影響が広範囲に伝播するおそれがあることなどを踏まえ、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。

・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。

・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。

・また、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純然たる平時でも有事でも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[12]、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

[12] 警察庁警備局　治安の回顧と展望（令和 2 年 12 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）。　なお、サイバー空間における脅威の概況 2021（公安調査庁）において、中国について、軍・情報機関によるサイバー攻撃への関与が指摘されているとしている。

するため[13]、北朝鮮は政治目標の達成や外貨獲得のため[14]、サイバー攻撃等を行っているとみられている。加えて、これらの国において、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[15]。

・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[16]。

・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・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、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。

（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）

・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、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

---

13 警察庁警備局　治安の回顧と展望（令和 2 年 12 月）、米国国防省サイバー戦略（2018 年 9 月）。なお、サイバー空間における脅威の概況 2021（公安調査庁）において、ロシアについて、軍・情報機関によるサイバー攻撃への関与が指摘されているとしている。

14 警察庁警備局　治安の回顧と展望（令和 2 年 12 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中間報告書（2019 年 9 月）。なお、サイバー空間における脅威の概況 2021（公安調査庁）において、北朝鮮について、サイバー攻撃を用いた不正な金銭獲得・諜報・破壊活動への軍の関与が指摘されているとしている。

15 令和 2 年版防衛白書

16 令和 2 年版防衛白書

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」[17]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・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[18]。

・他方、既存の秩序とは相容れない恐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、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（以下「防衛大綱」という。）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

・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、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。

---

17 「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。

18 G7 伊勢志摩首脳宣言（平成 28 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。

・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。

・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

・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[19]ことを踏まえ、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り、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、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[20]。例えば、2021 年 4 月に警察において書類送致した事件[21]の捜査等を通じて、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た。

・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。

・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とから、偶発、不必要な衝突を防ぐため、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。

（３）サイバー空間の状況把握力の強化

・状況把握力は、防御力ひいては抑止力の基盤である。

・攻撃者を特定し、責任を負わせるため、サイバー攻撃を検知・調査・分析する能力を引き続き向上させ、関係機関の全国的なネットワーク、技術部隊も駆使しなが

[19] 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）

[20] 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。

[21] 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。本件は、捜査等を通じて、約 200 の国内企業等に対する一連のサイバー攻撃が Tick と呼ばれるサイバー攻撃集団によって実行され、当該 Tick の背景組織として、山東省青島市を拠点とする人民解放軍第 61419 部隊が関与していた可能性が高いと評価するに至った。

らサイバー攻撃の更なる実態解明を推進する。
・国家の関与が疑われるサイバー攻撃等に対応するため、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。

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。

（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２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）」の実現に向けサイバーセキュリティ分野における米豪印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[22]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

・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、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、「インフラシステム海外展開戦略 2025」[23]の下、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。

[22] IoC (Indicator of Compromise)。サイバー攻撃の痕跡を表す情報
[23] 経協インフラ戦略会議決定（令和 2 年 12 月）

・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。
・また、能力構築支援の基本方針である「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（基本方針）」[24]については、産官学連携や外交・安全保障を含めた取組の強化を念頭に、新たなサイバーセキュリティ戦略策定とともに更新する。

４．４　横断的施策

・基本法に掲げた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。

４．４．１　研究開発の推進

・中長期的観点から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に取り組むとともに、それを基礎とした実践的な研究開発を推進しつつ、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、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で、デジタル技術の活用進展と相まって重要な研究分野となっている。
・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及び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む。
・関係府省における研究及び産学官連携振興施策の活用を促進するとともに、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。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。

（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、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。
  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
  ② 国内産業の育成・発展に向けた支援策の推進
  ③ 攻撃把握・分析・共有基盤の強化
  ④ 暗号等の研究の推進
・戦略期間において、関係府省の取組を推進するとともに、（１）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。

[24] サイバーセキュリティ戦略本部報告（平成28年10月）

（３）中長期的な技術トレンドを視野に入れた対応

・「Beyond 5G」[25]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り、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。

① AI 技術の進展を見据えた対応

・AI を活用したサイバーセキュリティ対策（AI for Security）の取組と AI を使ったサイバー攻撃に対処する観点

・AI そのものを守るセキュリティ（Security for AI）の取組

② 量子技術の進展を見据えた対応

・耐量子計算機暗号に関する検討

・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

４．４．２　人材の確保、育成、活躍促進

・人材の不足感に関する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。

・また、サイバーセキュリティに係る人材が、男女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。

・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む。

（１）”DX with Cybersecurity”の推進

・企業・組織内でのデジタル化推進に伴う人材の需要と人材の供給が車の両輪として好循環を生み出すことが重要。

・また、そのためには、経営者及び DX 推進者において、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前提となるところ、意識改革に取り組みつつ、以下の取組を推進。

① 「プラス・セキュリティ」知識の補充

・経営層や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。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。

・こうした取組の一環として研修・セミナー等の人材育成プログラムを社会的に広く普及させていくため、国や関係機関・団体で需要を喚起する普及啓発を行

[25] 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。

うことに加え、国による先導的・基盤的なプログラム提供だけでなく、需要者からみて一定の質が確保・期待される仕組みを通じて、人材育成プログラムに係る需要と供給を相応させ市場の形成・発展を目指していくほか、地域におけるコミュニティ形成を通じた「共助」の取組や、人材育成基盤・環境の民間提供等を重点的に進めていく。

②IT・セキュリティ人材が活躍できる環境の構築

・今後、DX に伴い、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との連携などが増加する中で、新たな開発・監視・対処のプラクティスが必要となり、セキュリティ・バイ・デザインの重要性も増すと考えられる。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を行っていく。

・また、人材の活躍の場という観点では、兼業・副業といった雇用形態の活用や行政でのデジタル改革業務の機会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、業務や製品・サービス等のデジタル化に応じた企業・組織内での適切な開発・監視・対処機能構築のプラクティス実践が図られるとともに、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環境整備が必要。このため、新たな時代に応じたプラクティス実践の事例を、先進事例として積極的に共有するとともに、実践に当たって参考となるノウハウやネットワークを提供することを通じ、展開を図る。

（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。

・このため、これらの脅威動向に対応し、実践的な対処能力を持つ人材育成プログラムを強化しコンテンツの開発・改善を行うとともに、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、産学に開放する。

・また、こうした人材の活躍促進の観点から、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もあわせて重要である。

（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が重要。この方針[26]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、素養を有する人材がより確保しやすくなる仕組みの早期導入、研修の充実・強化等に向けた方策を新たに示し、取組を推進。

[26] 「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）

・また、各府省庁の人材確保・育成計画に基づき、「サイバーセキュリティ・情報化審議官」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、毎年度計画の見直しを行い、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、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、様々なリスクに対処できることが不可欠。素養・基本的な知識（リテラシー）を身に付けると同時に、自らの判断で脅威から身を守れるよう、行動強化につながる普及啓発・情報発信が重要。
・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。
・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を推進。今後、デジタル改革推進により、サイバー空間に参加する層が広がる中で、当該アクションプランプランを推進しつつ継続的な改善に取り組むとともに、状況を踏まえた見直しを検討する。
・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に伴い、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。

５．推進体制

・これまで述べてきた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。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、NISC 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。
・危機管理対応についても一層の強化を図ることが必要。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。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、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。
・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、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。
・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、経費の見積もり方針を定め、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。

・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。年次計画と年次報告は一体的に検討を行い、本戦略に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。