次期サイバーセキュリティ戦略の課題と方向性

資料２－１

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**に向けて行ってきた取組

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「デジタル庁」が設置され、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併せて、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 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

→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・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**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全・安心を確保
- 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

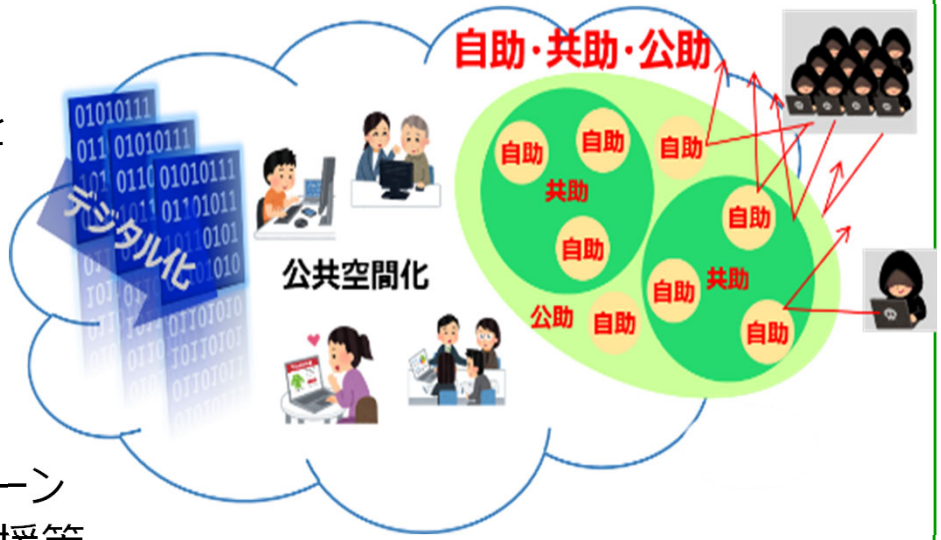
- 政府統一基準群に基づく対策の推進や監査・CSIRT訓練・GSOCによる監視等を通じた政府機関全体としてのセキュリティ水準の向上。
- クラウドサービスの利用拡大を見据えた政府統一基準群の改定・運用やクラウド監視に対応したGSOC機能の強化。

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。

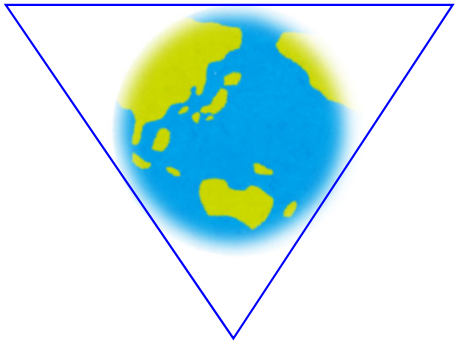
国際社会の平和・安定及び我が国の安全保障への寄与

課題認識と方向性　－ 安全保障の観点からの取組強化 －

- 我が国をとりま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等同志国との府省庁横断的・各府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に係る基本方針」

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、それを基盤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

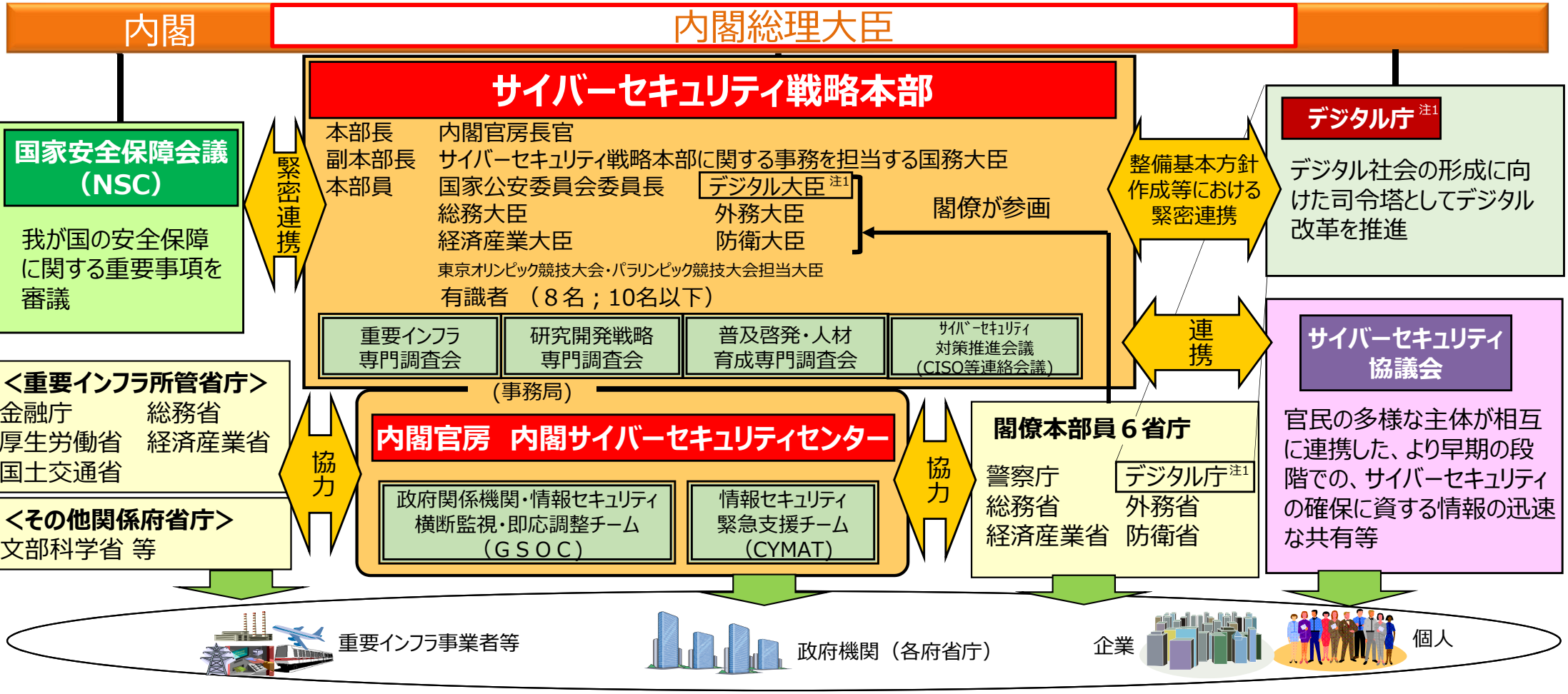
外部高度人材活用の仕組み強化
「デジタル区分」合格者の積極採用、研修の充実・強化　等

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と関係府省庁が連携して、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）

「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）