資料１

次期サイバーセキュリティ戦略の検討について

資料１－１　次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）の概要

資料１－２　基本的な時代認識・環境変化、国際情勢から見たリスク/近年の脅威動向

資料１－３　次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）

資料１－１

次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）の概要

次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）

○　現行のサイバーセキュリティ戦略（平成30年7月閣議決定）では、「今後３年間の諸施策の目標及び実施方針を示す」としており、令和３年に計画期間を終えるため、次期のサイバーセキュリティ戦略（次期戦略）の策定に向けた検討を行う必要がある。

○　次期戦略の策定に当たっては、サイバーセキュリティ基本法が定める、①「経済社会の活力の向上及び持続的発展」、②「国民が安全で安心して暮らせる社会の実現」、③「国際社会の平和・安定及び我が国の安全保障」に寄与するものとなるよう、以下の事項を十分に踏まえることが重要である。なお、次期戦略の策定にあたってデジタル改革との緊密な連携を図る。

◆　第一　環境変化や国際情勢等を踏まえ時宜を得た対応方針とすること

○デジタル庁を司令塔として推進する「デジタル改革※」に寄与し、「自由、公正かつ安全なサイバー空間を確保」するため、現行戦略策定後に顕在化した以下の4点を踏まえ、中長期的視点から、時宜を得た対応方針とする。

①　新型コロナウイルス感染症の影響をはじめとする経済社会の環境変化
②　クラウドサービスの利用拡大や５Gの利用開始
③　日本を取り巻く安全保障環境の変化をはじめとする国際情勢
④　サイバーセキュリティに係る近年の脅威の動向

※デジタル改革が目指すビジョン：
　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
（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25日閣議決定）

◆　第二　政府の役割を意識した政策立案の基礎となるものにすること

○サイバー空間は、攻撃者優位ともされる中、各主体が自らの役割を認識し対応するとともに、互いに連携・協働して取り組むことができる環境が重要。

○政府は、全体を俯瞰した上で、特に以下の政府の役割を意識し、今後特に重点的に取り組むべき分野を明確化した政策立案の基礎となるものとする。

①　自律的な取組や多様な主体の緊密連携、組織化・洗練化されたサイバー攻撃に対する公的機関の取組が効率的かつ戦略的に実現できるよう適切な対策を進める（攻撃者との非対称な状況の改善も含む）。

②　2021年に開催される2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けた取組の活用等。

◆　第三　発信力を意識して我が国の考え方を内外に示すものとすること

①　高度化・巧妙化する脅威やサプライチェーンの複雑化など、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発信を行う。

②　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。

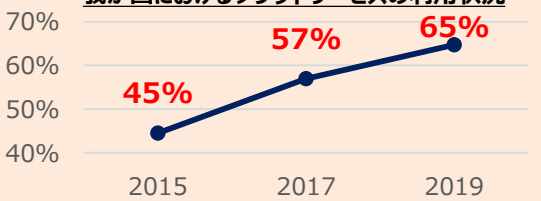
次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）の概要

【基本的な時代認識】

◆ 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～

- 平成の時代を通じ、**デジタル経済が大きく進展**。政府は、「**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、**デジタル庁を司令塔としてデジタル改革を推進。**
- デジタル経済の影響は、**人々の生活そのものに波及**。IoTやAI、5G、クラウドサービス等の利用拡大や人々の行動変容、量子など新技術への期待。サイバー空間と実空間が高度に融合したSociety5.0の実現が期待。

我が国におけるクラウドサービスの利用状況



（データ出所）総務省「情報通信白書」よりNISC作成 ※「一部利用」含む

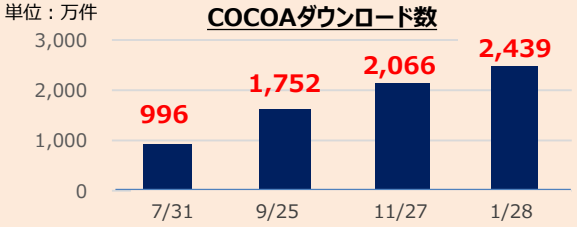
◆ 安全保障環境の変化をはじめとする国際情勢

- Society5.0の実現により、国連が掲げる**SDGsにも貢献することが期待**。
- 他方、**サイバー空間に対する基本的価値・ガバナンスの在り方に対する国家間対立の激化**。

◆ 新型コロナウイルスの影響・経験

- **テレワークの利用、ICT教育やオンライン診療に係る動きが加速**。パーソナルデータを活用したサービスの進展。

COCOAダウンロード数



（データ出所）厚生労働省HPよりNISC作成

◆ オリンピック・パラリンピックに向けた取組の活用

【環境変化、国際情勢から見たリスク/近年の脅威動向】

◆ 環境変化をとらえたサイバー攻撃の増加

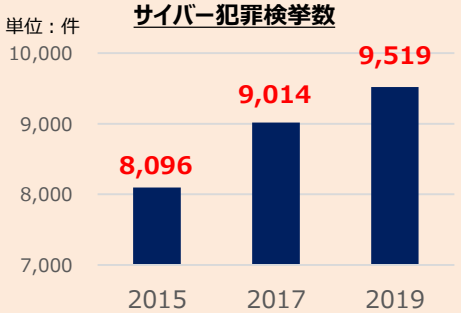
- サイバー犯罪の検挙件数は増加傾向
- テレワーク普及に伴う攻撃・クラウドサービスを標的とする脅威の増加
- 新型コロナウイルス感染拡大に乗じたサイバー攻撃の発生

◆ 従来から見られる攻撃の継続 ／ サプライチェーンリスクの顕在化

◆ サイバー空間を構成する技術基盤や国際ルール、データ覇権を巡る争い

◆ 経済社会全体での人材不足・偏在 ／ リテラシーギャップの顕在化

サイバー犯罪検挙数



※2020年は**9,911件**【暫定値】

（データ出所）警察庁公表資料よりNISC作成

サイバー攻撃についての外務報道官談話

- **米国による北朝鮮のサイバー攻撃に関する発表について（平成29年12月20日）**
- **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（平成30年12月21日）**

次期戦略の検討の基本的な考え方（案）

デジタル改革に寄与するとともに、環境変化や国際情勢等を踏まえ時宜を得た対応方針とすること

各主体が自らの役割を認識し対応するとともに、互いに連携・協働することが重要であり、重点的に取り組む分野を明確化しつつ、政府の役割を意識した政策立案の基礎となるものにすること

発信力を意識して、攻撃者への抑止の効果や各国に対する我が国の立場の理解を訴求するなど、我が国の考え方を内外に示すものとすること

※なお次期戦略の策定にあたってはデジタル庁が司令塔として推進するデジタル改革との緊密な連携を図る。

次期サイバーセキュリティ戦略策定までの主要スケジュール（案）

時期	令和2年度(2020年度)				令和3年度(2021年度)
	12	1	2	3	4～
閣議					★ **閣議** (戦略決定)
CS戦略本部			☆ 本部㉖ (基本的考え方) (2/9)	☆ 本部㉗ (骨子案)	☆ 本部㉘ (パブコメ案) ☆ 本部㉙ (戦略案) IT総合戦略本部及び国家安全保障会議からの意見聴取 パブリックコメント実施

基本的な時代認識・環境変化、国際情勢から見たリスク/近年の脅威動向

基本的な時代認識

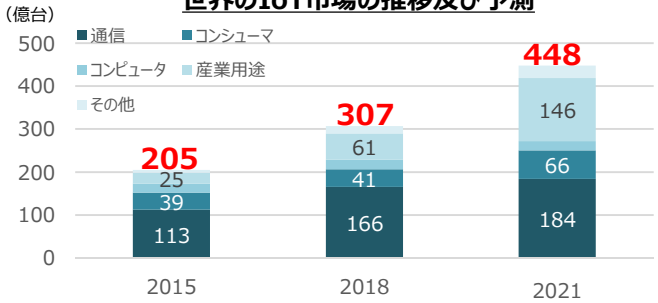
◆ 経済社会の環境変化 ～デジタル経済の浸透、デジタル改革の推進～

➢ 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、**デジタル庁を司令塔としてデジタル改革を推進**。

➢ **デジタル経済の影響**は、**人々の生活そのものに波及**。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変容、量子など新技術への期待。その先にはサイバー空間と実空間が高度に融合したSociety5.0の実現が期待。

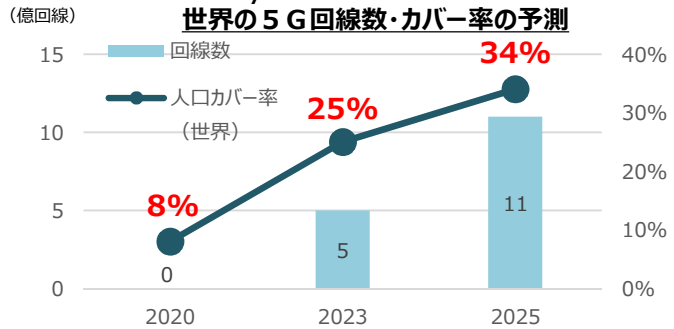
AI,IoT等を活用している企業の割合 25%(2019年度) → 34%(2020年度)
（資本金100億円以上）
（データ出所）DBJ「全国設備投資計画調査（大企業）」

世界のIoT市場の推移及び予測



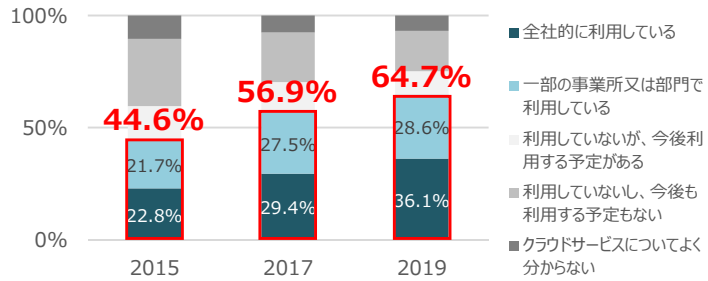
（データ出所）IHS TechnologyよりNISC作成

世界の５Ｇ回線数・カバー率の予測



（データ出所）GSMAよりNISC作成

我が国におけるクラウドサービスの利用状況



（データ出所）総務省「情報通信白書」よりNISC作成

◆ SDGｓへの貢献への期待

➢ 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**。

◆ 安全保障環境の変化、地政学的課題

➢ **サイバー空間に対する基本的価値・ガバナンスの在り方に対する国家間対立の激化**。

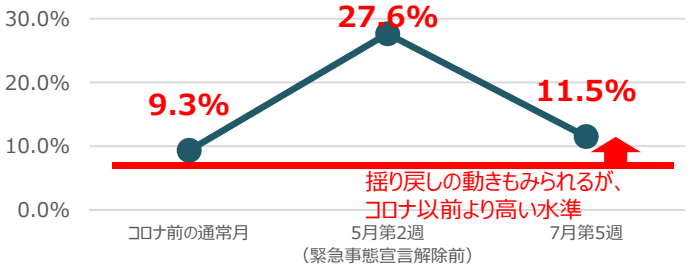
◆ オリンピック・パラリンピックに向けた取組

➢ 2021年に開催される**2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けた取組を活用**

◆ 新型コロナウイルスの影響・経験

➢ 新型コロナウイルスの感染拡大に伴い、**テレワークの利用、ICT教育やオンライン診療に係る動きが加速**。パーソナルデータを活用したサービスの活用も進展。

週1日以上在宅勤務の割合



（データ出所）JILPTリサーチアイ第47回（周燕飛氏執筆）よりNISC作成

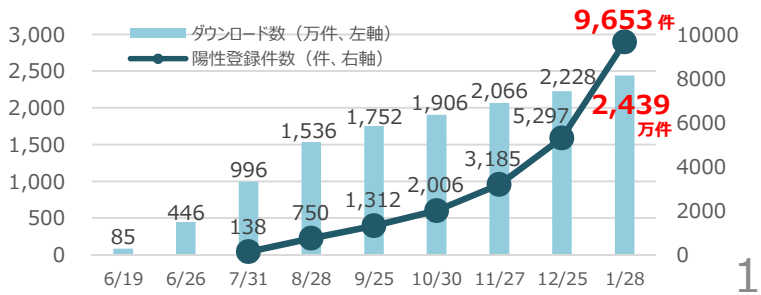
GIGAスクール構想

○2020年度補正予算で約2,000億円を措置し、学校における環境整備の支援を行うGIGAスクールサポーターの配置や、2023年度に達成するとされている端末整備の前倒しを支援。
※小5・6、中1に加え、残りの中2・3、小1～4全てを措置。

オンライン診療

○2020年4月より、厚生労働省が、「医師の判断の下、初診から電話や情報通信機器を用いた診療により診断や処方をして差し支えない」とする時限的・特例的措置を実施。

新型コロナに係る接触確認アプリ(COCOA)のダウンロード数等推移

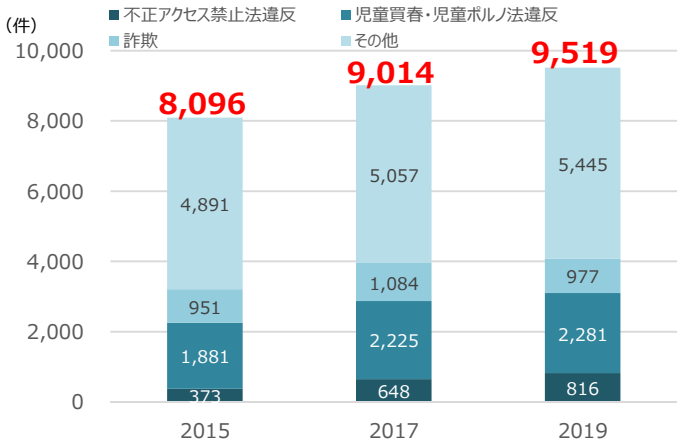


（データ出所）厚生労働省HPよりNISC作成

環境変化、国際情勢から見たリスク ／ 近年の脅威動向①

◆ 環境変化をとらえたサイバー攻撃の増加

➢ サイバー犯罪の検挙件数は増加傾向。
2019年中の検挙件数は過去最多。
（2020年中は9,911件【暫定値】）



（データ出所）警察庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について」並びに「令和2年の犯罪情勢【暫定値】」よりNISC作成

➢ テレワークの普及に伴うサイバー攻撃の増加。

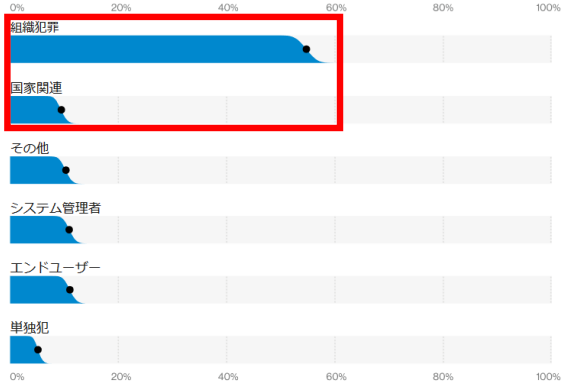
リモートデスクトップを狙ったブルートフォース攻撃の件数(米)
2020/3/9 約20万件 ⇒ 2020/4/9 約138万件
(約6.9倍) （データ出所）Kaspersky

➢ クラウドサービスを標的とした脅威の増加。

クラウド脅威の合計と外部クラウド脅威：
2020年1月～4月にかけて**約7.3倍** （データ出所）McAfee Labs

◆ サイバー攻撃の組織化 国家の関与が疑われるサイバー攻撃

世界における漏洩/侵害でよく見られる攻撃者の種類



（データ出所）Verizon「データ漏洩/侵害報告書2020」

選挙に関連するサイバー攻撃事例

◆香港（2018年10月）
中国のサイバー情報窃取を行う者が、マルウェア（EVILNEST）により選挙中に香港の組織を攻撃対象とした。

◆米国（2018年11月）
イランを支援する攻撃者とのつながりが疑われるアカウントのネットワークの一部に、米共和党の候補者を装った多数のツイッターアカウントが確認された。

◆欧州（2019年）
選挙関連機関及びメディアに対するスピアフィッシング攻撃が確認された。

（データ出所）ファイアアイ

◆ サイバー空間を構成する技術基盤や国際ルール、データ覇権を巡る争い

例 新たなインターネットプロトコル(New IP)に係る議論

○2018年 ファーウェイを中心に、ITU-T次会期（2021～2024年）における新たな検討課題として、「New IP」に係る議論開始を提案。

○2020年12月 SG13・SG11会合において、日米欧等の反対により、次会期の新規設置検討課題として提案しないこととなった。

（注）報道情報等を基にNISC作成

◆ サプライチェーン複雑化

主要通信機器の世界シェア

サーバー(2019年)	
デル【米国】	17.4%
HPE/New H3C【米国/中国】	15.4%
インスパー【中国】	8.7%
レノボ【中国】	6.4%
ファーウェイ【中国】	5.2%
その他	46.8%

（データ出所）IDC

移動通信インフラ(2019年)	
エリクソン【スウェーデン】	29.0%
ファーウェイ【中国】	26.0%
ノキア【フィンランド】	23.9%
ZTE【中国】	12.0%
サムスン【韓国】	5.0%
その他	4.1%

（データ出所）Informa

◆ 新型コロナウイルス感染拡大に乗じたサイバー攻撃の発生（Emotet）

例 保健所等の専門機関を装った偽メール

2020年1月29日、保健所等の専門機関を装って新型コロナウイルス感染症に関する偽の情報を載せたメールが発見された。偽メールは、「通知」という件名で、送信元として「○○保健所福祉室」という実在する保健所の名称を使用し、文面には「新型コロナウイルス関連肺炎については、中国武漢市を中心に患者が報告され、国内でも○○県で患者が報告されている」等と書かれており、添付のWordファイルを開くとマルウエア**Emotet**に感染するもの。

（注）報道情報等を基にNISC作成

◆ 従来から見られる攻撃の継続／サプライチェーンリスクの顕在化

情報セキュリティ10大脅威の変遷（組織）

2021年の順位	2018年の順位
1位 ランサムウェアによる被害	2位
2位 標的型攻撃による機密情報の窃取	1位
3位 テレワーク等のニューノーマルな働き方を狙った攻撃	ランキングなし
4位 サプライチェーンの弱点を悪用した攻撃	ランキングなし
5位 ビジネスメール詐欺による金銭被害	ランキングなし

（データ出所）IPA「情報セキュリティ10大脅威」よりNISC作成

◆ 経済社会全体での人材不足・偏在／リテラシーギャップの顕在化

➢ 人材不足感が大きく、IT企業に偏在。

セキュリティ対策に従事する人材の不足感
86% (米16%)
（データ出所）NRIセキュア「企業における情報セキュリティ実態調査」

情報処理・通信に携わる人材がIT企業に所属している割合
72% (米35%)
（データ出所）IPA「IT人材白書2017」

➢ サイバー空間拡大の中、リテラシー浸透が急務。

インターネットの利用時に不安を感じる人の割合
71%
（データ出所）総務省「通信利用動向調査」

インターネットや情報に関する倫理教育を受けたことがある割合
18%
（データ出所）IPA「情報セキュリティに対する意識調査」

近年の脅威動向②

近年の主なサイバー攻撃事案

○…国内　□…海外

○ 暗号資産が不正に送信されたとみられる事案（2018年１月）

国内仮想通貨交換業者から**約580億円相当**の暗号資産（NEM）が**不正に送信**されたとみられる事案が発生した。

○ 2020年東京大会のチケット抽選に関するフィッシング（2019年７月）

2020年東京大会の**チケット抽選に関係があると見せかけた偽のショートメッセージサービス（SMS）**が、スマートフォン利用者に送られているとの報道。
誘導先のサイトで米Appleのギフト券の番号を入力させて窃取する仕組み

○三菱電機への不正アクセスによる個人情報・企業機密等の漏えい（2020年1月）

三菱電機は、同社のネットワークが第三者による不正アクセスを受け、個人情報や企業機密が外部に流出した可能性があると公表
流出した可能性のある情報に、防衛省の「注意情報」が含まれていたと判明

○NTTコミュニケーションズへのBYOD端末等を通じた不正アクセス事案（2020年5月）

NTTコミュニケーションズは、同社の設備が攻撃者からの不正アクセスを受け、社内に保存されていたファイルが閲覧され、一部の情報が外部に流出した可能性を公表
調査の結果、**当初は海外拠点への攻撃及び侵入を起点とした不正アクセス**が明らかになったが、その後**社内のBYOD端末による不正アクセス**も発覚

○□ ホンダへのサイバー攻撃（2020年6月）

本多技研工業は、**各国の拠点のコンピュータがダウンし、工場からの出荷が停止**したことを公表。その原因は、**ランサムウェア**を使った攻撃によるものとみられている。

○ ドコモ口座をはじめとした電子決済サービスを利用した口座振替による不正出金事案（2020年９月）

「ドコモ口座」をはじめとした電子決済サービス、ゆうちょ銀行の「mijica」及びSBI証券において、不正アクセスにより、**不正送金や顧客資産の流出が発生したことが、相次いで発覚**

○ 慶応義塾大学への不正アクセスによる個人情報漏えい（2020年10月）

慶応義塾大学は、湘南藤沢キャンパスのネットワークシステム、授業支援システム等に対する不正アクセスにより、**利用者の個人情報が漏えいした可能性がある**と公表

○ カプコンへのサイバー攻撃による個人情報の流出（2020年10-11月）

カプコンは、サイバー犯罪グループからランサムウェアによる不正アクセス攻撃を受け、社外の**個人情報約39万件が流出した可能性がある**と公表

□SolarWinds社製品へのサイバー攻撃（2020年12月）

米SolarWinds社は、同社のソフトウェア（orion platform）の脆弱性を悪用した、同ソフトウェアを利用しているシステムへのサイバー攻撃を認識したと公表

資料１－３

次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方（案）

令和　　年　　月　　日
サイバーセキュリティ戦略本部決定

現行のサイバーセキュリティ戦略（平成 30 年７月 27 日閣議決定。以下「現行戦略」という。）において、「今後３年間の諸施策の目標及び実施方針を示す」とされており、令和３年に計画期間を終えるため、次期のサイバーセキュリティ戦略（以下「次期戦略」という。）の策定に向けた検討を行う必要がある。

次期戦略の策定に当たっては、サイバーセキュリティ基本法（平成 26 年法律第 104 号）が定める「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」及び「国際社会の平和・安定及び我が国の安全保障」に寄与するものとなるよう、以下の事項を十分に踏まえることが重要である。

第一　環境変化や国際情勢等を踏まえ時宜を得た対応方針とすること

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、デジタル庁を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、自由、公正かつ安全なサイバー空間を確保していくため、現戦略策定後に顕在化した、新型コロナウイルス感染症の影響をはじめとする経済社会の環境変化、クラウドサービスの利用拡大や５G の利用開始、日本を取り巻く安全保障環境の変化をはじめとする国際情勢及びサイバーセキュリティに係る近年の脅威の動向を踏まえ、中長期的視点から、時宜を得た対応方針とすること。

第二　政府の役割を意識した政策立案の基礎となるものにすること

サイバー空間においては、関連技術の進展が早く、攻撃者優位ともされる中で、それぞれの主体が自らの役割を認識し対応するとともに、互いに連携・協働して取り組むことができる環境が重要。政府としては、社会全体を俯瞰した上で、攻撃者との非対称な状況の改善も含め、自律的な取組や多様な主体の緊密連携、組織化・洗練化されたサイバー攻撃に対する公的機関の取組が効率的かつ戦略的に実現できるよう適切な対策を進めるなど政府の役割を意識した政策立案の基礎となるものにすること。その際、併せて、2021 年に開催される 2020 年東京オリンピック競技大会・東京パラリンピック競技大会に向けた取組の活用等を含め、今後特に重点的に取り組むべき分野を明確化して推進すること。

第三　発信力を意識して我が国の考え方を内外に示すものとすること

ますます高度化・巧妙化する脅威やサプライチェーンの複雑化など、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発信を行うこと。併せて、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こと。

なお、次期戦略の策定にあたってデジタル庁が司令塔として推進するデジタル改革との緊密な連携を図る。次期戦略に基づいて計画した取組について、その計画期間内において定期的に実績を評価し、その後の取組に反映する進め方についても併せて検討することが重要である。