参考資料１－２

「次期サイバーセキュリティ戦略」の骨子

１ 策定の趣旨・背景

１．１　サイバー空間がもたらす変革の潮流

・ 民間の主体による自律的なガバナンス（自律・分散・協調）を通じて、急速に拡張・発展したサイバー空間は、場所や時間の制約にとらわれず、国境を越えて、量・質ともに多種多様な情報・データを自由に発信・共有・分析することが可能であり、創意工夫によって人間の活動を拡張させることが可能という特徴

・ このようなサイバー空間は、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でもあり、今後の経済社会の持続的な発展の基盤。また、自由主義、民主主義、文化発展の基盤

・ 現在、このようなサイバー空間における計算機科学の知見の進展や技術・サービスの創出により、これまでの人類社会の認識や概念の根底が揺らいでいるとの指摘もあり、人類が経験してきた狩猟社会、農耕社会、工業社会、情報社会から、経験したことのないパラダイムシフト（Society5.0）が生じつつある状況

・ サイバーセキュリティの在り方についても、このような変革の潮流を俯瞰しながら、検討することが必要

１．２　2015 年戦略策定とそれ以降の状況変化等

・ 2014 年 11 月に制定されたサイバーセキュリティ基本法(以下「基本法」という。)に基づき、2015 年９月に、サイバーセキュリティ戦略本部（以下「本部」という。）における検討を踏まえて、サイバーセキュリティ戦略（以下「2015 年戦略」という。）が閣議決定され、今後３年間に執るべき諸施策の目標や実施方針の明示

・ サイバー空間は、実空間（フィジカル空間）との一体化が加速的に進展[1]し、様々な場面で、あらゆる主体が参加する空間になっており、脅威が深刻化・巧妙化し、実空間での経済的社会的損失のリスクが拡大しており、今後も、指数関数的に拡大していくことが想定

・ 諸外国においては、国家安全保障を重視するという潮流がより鮮明との指摘の一方で、国連サミットで「持続可能な開発目標（SDGｓ）」が採択され、人間の安全保障の理念を反映した動きもみられる状況

・ 経済社会の持続的な発展と人々に豊かさをもたらす社会の実現のため、自律的・持続的に発展するサイバー空間を維持していく必要があり、全ての関係主体が連携・協調してサイバーセキュリティの確保に取り組むことを推進する等「サイバーセキュリティの基本的な在り方」の明確化が必要

・ 具体的には、2020 年東京オリンピック・パラリンピック競技大会（以下「2020 年東京大会」という。）開催等を控えている中、このような「サイバーセキュリティの基

[1] 科学技術イノベーション総合戦略 2017（平成 29 年６月２日閣議決定）、未来投資戦略 2017（平成 29 年６月９日閣議決定）等政府としても、「サイバー空間とフィジカル（実）空間を高度に融合させることにより、経済的発展と社会的課題の解決を両立する社会」（Society5.0）を目指す方針を決定

本的な在り方」に基づき、サイバーセキュリティ対策に万全を期していくことが求められる状況

２ サイバー空間に係る認識

２．１　サイバー空間がもたらす恩恵

・ AI、IoT などのサイバー空間における知見や技術、サービスが社会に定着し、経済社会活動・国民生活の既存構造を覆すイノベーションを牽引しており、サイバー空間と実空間の一体化が進展。こうした技術・サービスは、分野を問わず、あらゆる領域で当然に利用される状況

① サイバー空間におけるサービスの進展と社会への定着

・ サイバー空間におけるサービスの社会への定着が進み、自由な情報の流通にとどまらず、SNS 等による多様なコミュニティの形成、情報共有が進展。経済活動においても、Fintech やシェアリングエコノミー等の新サービスが登場し、イノベーションをけん引

② AI の劇的な進化

・ 深層学習の登場により AI は画像解析精度が飛躍的に向上し、製品の異常検知、ガンの診断、投資判断、翻訳等の性能が高まり、その進化はカンブリア爆発[2]に例えられるほど劇的なものであると評価

③ IoT の進展

・ 端末などのセンサ技術の小型軽量化、低廉化等を背景に、IoT の爆発的な普及が進み、IoT 機器で得られるデータを利活用した新たなビジネスやサービスが創出。サプライチェーン（供給網）の中でのデータ利活用や、「オープンイノベーション[3]」の進展も期待

２．２　サイバー空間がもたらす脅威

・ サイバー空間を前提としたサービスの拡大などサイバー空間と実空間の一体化の進展に伴って、国家の関与が疑われる大規模な事案[4]も含め、脅威は深刻化・巧妙化し、経済的・社会的損失のリスクも指数関数的に拡大

・ IoT、仮想通貨を含む Fintech、重要インフラ、サプライチェーンを狙った攻撃等により、従来の情報漏えいに加えて、直接的な金銭被害、業務・サービス障害による多大な影響など経済社会の持続的発展や国民生活の安全安心等を大きく脅かす事態

・ 今後、サイバー空間における AI やデータ利活用の進展に伴い、サプライチェーン、異業種が協業するオープンイノベーションにおけるリスクが顕在化し、政府機関や重要インフラ事業者以外の事業者、個人においても、サイバーセキュリティに関連する脅威が高まっていくものと想定

---

[2] ５億 4200 万年前から５億 3000 万年前の間に突如として今日見られる動物の「門」が出そろった現象。古代生物学者アンドリュー・パーカーは、「眼の誕生」がその原因だったという説を提唱

[3] 組み合せ全体に貢献する要素をｵｰﾌﾟﾝに集め、全体が提供する価値を向上すること

[4] ランサムウェア（「WannaCry」(2017 年 5 月)、「NotPetya」(同年 6 月)、「Bad Rabbit」(同年 10 月))、平昌五輪に開会式に対するサイバー攻撃が生じたとの報道

① 金銭の窃取・詐取等の損害

・ サイバーセキュリティに関する基本的な対策の不備等により、仮想通貨交換業者等への不正アクセスやビジネスメール詐欺で巨額の金銭的な被害が発生。今後、経済社会におけるサイバー空間への依存度の高まり、基本的な対策の不備が金銭的な損害に直結し、拡大することが想定

② 情報（個人情報、営業秘密・価値あるデータ等）の毀損及び漏えい[5]による競争力低下等

・ 個人情報、営業秘密・価値あるデータ等をはじめとした情報の漏えいは、損害賠償請求の対象となるおそれがあるだけでなく、企業の社会的評価・信頼の低下を招くおそれもあり、競争力の低下に直接つながるもの

③ 業務・機能・サービス障害[6]による経済社会への多大な影響

・ 重要インフラサービス障害（電力、金融、地方自治体等の業務）、IoT 機器（医療機器等）の誤作動などの業務・機能・サービス障害などが生じた場合、その経済社会への影響は大きくなることも想定され、国家安全保障上の問題となることも懸念

３ 目的

３．１　我が国の基本的な立場

・ 自由、公正かつ安全なサイバー空間を堅持するため、国家による統制を強化するアプローチではなく、多様な主体の連携の促進を重視する立場に立つ。このような立場を堅持し、また、悪意ある者の行動を抑制し、国民の安全・権利を保障するため、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を選択肢として保持

（１）基本法の目的

・ 基本法は、経済社会の活力の向上及び持続的発展（以下「経済活力」という。）、国民が安全で安心して暮らせる社会の実現（以下「安全安心」という。）、国際社会の平和・安定及び我が国の安全保障（以下「平和安保」という。）に寄与することを目的[7]

（２）基本的な理念（自由、公正かつ安全なサイバー空間）

・ 基本的な理念として、「自由、公正かつ安全なサイバー空間」を目指すこととし、これを堅持

（３）基本原則

・ サイバーセキュリティに関する施策の立案及び実施にあたって従うべき基本原則については、①情報の自由な流通の確保、②法の支配、③開放性、④自律性、⑤多様な主体の連携の５つの原則を堅持

① 情報の自由な流通の確保

---

[5] 脆弱性を利用した不正アクセスにより、政府機関を含めて広範囲に影響（Apache Struts2、WPA2 等）

[6] 大規模な通信障害により、ネットバンク・証券などを中心に経済的に多大影響

[7] サイバーセキュリティ基本法（抜粋）

第一条　この法律は、（中略）サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

・ サイバー空間においては、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が作られ、維持されるべきという立場を堅持。なお、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は前提[8]

② 法の支配

・ サイバー空間においても、既存の国際法が適用され、国内においては法令を含む各種ルールや規範が及ぶという立場から、自由や民主主義などの普遍的な価値を守るための国際法の適用、規範の形成が不可欠

③ 開放性

・ サイバー空間が持続的に発展し続けるために、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、参加を求める者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[9]

④ 自律性

・ サイバー空間の秩序維持のためには、様々な社会システムがそれぞれの任務・機能に沿って自律的に活動することにより対処する以外にはなく、これを促進していくことが求められる。秩序維持の役割を国家が全て担うとの立場には立たないことを堅持[10]

⑤ 多様な主体の連携

・ 全てのステークホルダーがそれぞれの役割や責務を果たし、努力するだけではなく、適切に連携・協働することが求められる。政府は、適切な連携関係を促す役割を担っており、その役割を適切に果たすことができるように施策を推進[11]

３．２　サイバーセキュリティの基本的な在り方（基本コンセプト）

（１）目指す姿

・ サイバー空間と実空間の一体化が加速的に進展する中、我が国としては、2015 年戦略で「無限の価値を産むフロンティア」とされたサイバー空間が持続的に発展し、新しい価値やサービスが次々と創出されて人々に豊かさをもたらす社会（Society5.0）の実現が必要

・ このような社会の実現に向けて、サイバー空間における安全安心と経済発展を両立させるため、３つの観点（①任務保証、②リスクマネジメント、③参加・連携・協働）から、官民のサイバーセキュリティに関する取組を推進

・ このようなサイバーセキュリティの取組により、持続的に発展するサイバー空間が維持される姿を「サイバーセキュリティエコシステム」と呼称

（２）主な観点

[8] 基本法第１条において、情報の自由な流通の確保について直接規定されている。
[9] 高度情報通信ネットワーク社会形成基本法第３条で「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容易にかつ主体的に利用する機会を有し」と規定している。
[10] 基本法第３条において、「自発的に行うサイバーセキュリティに対する取組が促進される」ことが規定されている。
[11] 基本法第 16 条において、「多様な主体が相互に連携してサイバーセキュリティに関する施策に取り組むことができるよう必要な施策を講ずる」と規定されている。

① 任務保証 -業務・サービスの着実な遂行-（Mission Assurance）

・ 組織が担う任務（業務やサービス等）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し、一部の専門家に依存するのではなく、業務・サービス等の遂行の観点から、その責任を有する者が主体的にサイバーセキュリティ確保に取り組むこと

② リスクマネジメント -不確実性の評価と適切な対応-（Risk Management）

・ 組織が担う任務の内容に応じて、リスク（不確実性の影響[12]）を特定・分析・評価し、リスクを許容し得る程度まで低減する対応をしていくこと

・ 利便性の享受に当たっては、それに伴うリスクが発生するのが一般的であり、リスクの性格や影響の現れ方に応じて適切に対処し、利便性による恩恵と比較してセキュリティリスクを許容し得る程度まで低減していくという課題への対処が必要

③ 参加・連携・協働 -個人・組織による平時からの対策と連携・協働-（Cyber Hygiene）

・ サイバー空間の脅威から生じ得る被害やその拡大を防止するため、個人又は組織各々が、平時から講じる基本的な活動を推進すること

・ 主に、個人又は組織による自身のシステムを守るための常時からの基本的な取組が重要であるが、あらゆる主体にとって脅威が日常化していく中で一般個人等の自助努力による取組のみでは対応が困難であることに留意

・ このため、組織を含む他の主体による積極的なサポートが必要な状況。基本的な活動の中に、サイバー空間に参加する個人又は組織各々が平時から連携・協働し、脅威から対策に至るまで情報共有を行っていくことも含めて、推進していくことが必要

４　目的達成のための施策

４．１ 経済社会の活力の向上及び持続的発展

・ IoT や AI などのサイバー空間における知見や技術・サービスの活用は、企業の生産性、さらには競争力の向上につながるだけでなく、あらゆる産業領域におけるつながりの広がり・深まりによって、ビジネスイノベーションが生ずる可能性（Society 5.0 の実現）

・ 一方、こうしたサイバー空間における技術やサービスの進化と社会的な受容の進展は、サイバーセキュリティのリスクを急速に高めている。このため、サイバー空間におけるビジネスイノベーションと、それを支える基盤としてのサイバーセキュリティの確保は一体的に取り組んでくことが必要

４．１．１ 新たな価値創出を支えるサイバーセキュリティの推進

・ サイバーセキュリティは、我が国の産業全般においてビジネスのイノベーションを実現するための重要な経営問題

[12] 不確実性の影響についてはプラス及びマイナスの両面があることに留意

（１）経営層の意識改革

・ 既存のビジネスの着実な遂行にとどまらず、サイバー空間におけるビジネスイノベーションを巻き起こしていくため、企業は、リスクマネジメントの一環としてサイバーセキュリティに取り組むことが必要

・ 産学官の緊密な連携の下、経営者の役割を明確にし、サプライチェーンを視野に入れた、サイバーセキュリティを確保するための体制を構築していくことが重要

・ このため、経営層への訴求のためのベストプラクティス集の整理や対策状況の見える化等ができるツールの整備及び取組のフォローアップを含め、経営層の意識改革に向けた官民の緊密な連携による取組を推進

（２）サイバーセキュリティに対する投資の推進

・ 企業がサイバーセキュリティに関わる取組を継続的に実施するためには、企業のサイバーセキュリティに関わる取組の情報発信・開示によって市場からの適切な評価が得られるなどにより、サイバーセキュリティに対する投資へのインセンティブが生まれるという好循環が重要。

・ 積極的な情報発信・開示を促すため、国内外のベストプラクティスの共有や、情報発信・開示の状況についての継続的なフォロー等が重要

（３）先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化

・ ビジネスイノベーションを実現するためには、IoT、AI、バーチャルリアリティ、ブロックチェーン、次世代通信技術などの先端技術の利活用が不可欠となる場合が多い。一方、こうした技術の利活用に伴い必要とされるセキュリティニーズを踏まえた具体的な解決策を提供するサイバーセキュリティビジネスの強化が必要。

・ このため、大企業のみならずベンチャー企業を含め、先進技術による新たな価値創造に向けたチャレンジを支えられるよう、先端技術の利用に伴うリスクの明確化、ガイドラインの策定や研究開発に関する機動的な取組、セキュリティ技術・サービスの供給者とのマッチングに係る仕組みの構築等の検討を行う。

４．１．２ 多様なつながりから価値を生み出すサプライチェーンの実現

・ Society5.0 の実現に向けて、サイバー空間と実空間の一体化が加速的に進展する中で、多様な規模・業種の企業、個人等が、実空間に留まらず、サイバー空間でも、これまで以上に、広く多様な形でつながり、そのつながりにより価値が創造されていくことを想定

・ 一方、このような社会では、従来のサプライチェーンを超えた多様かつ流動的な形態を見せることになり、サプライチェーンのつながりの端で起こったサイバーセキュリティの問題が、サプライチェーン、さらには、経済社会全体に広く波及する

おそれがあり、サプライチェーンへの攻撃の脅威が高まっている。Society5.0 におけるサプライチェーン全体を俯瞰した取組を推進することが不可欠

（１）セキュリティ対策指針の策定

・ Society5.0 のさまざまなつながりにおけるセキュリティ上の脅威を明確化し、事業者がリスクと対策コストのバランスを意識でき、また、海外におけるルール化の動きも反映した形で、運用レベルでの対策が実施できるような対策指針を策定し、産業分野毎に展開する

（２）サプライチェーンにおける機器・サービスのセキュリティを確認できる仕組の構築

・ 信頼の創出（セキュリティ要件を満たす機器・サービス等の生成、認証など）、信頼の証明（対象機器・サービス等が正常に生成されたものであることを確認するためのトラストリストの作成など）、信頼のチェーンの維持と構築（トレーサビリティの確保と、信頼のチェーンに対する攻撃・防御）の仕組を、対策指針を踏まえつつ構築

（３）中小企業の取組の促進

・ サプライチェーンのうち、中小企業は、セキュリティのための投資が難しいという事情がある一方、中小企業が踏み台となって自社のみならず取引先までサイバー攻撃の影響が拡大することへの懸念

・ このため、中小企業の事情を踏まえた促進策や、リスク評価ツールの検討、具体的なセキュリティ対策のベストプラクティスの検討を進めることが必要

４．１．３ 安全な IoT システムの構築

・ IoT はさまざまなモノ（機器）が連接することによって、新たな価値を創造する一方、セキュリティレベルや物理的安全性等の安全基準が異なるさまざまなモノがつながることは新たな脅威を生む可能性

・ また、さまざまなモノがつながるインフラとしてのサイバー空間に悪影響を及ぼしうる脆弱なモノ（機器）の対策は喫緊の課題

（１）IoT システムにおけるセキュリティの体系の整備と国際標準化

・ 2016 年８月に示した安全な IoT システムを実現するために求められるセキュリティに関する基本的な要素[13]に基づき、関係主体間の相互信頼に基づく連携と各主体の自律的な対策実施による協働を促すための基盤として、基本理念等に関する共通認識の醸成や各主体の取組の見える化などが重要

・ また、IoT システムにおける価値創造の仕組をグローバルな規模で展開するため、安全な IoT システムを実現するために求められるセキュリティに関する基本的な要素の国際標準化に向けた取組の推進

（２）脆弱性対策に係る体制の整備

・ IoT 機器を踏み台としたサイバー攻撃等の深刻化に対応するため、適切な官民

[13] 「安全な IoT システムのセキュリティに関する一般的枠組」（平成 28 年８月）

（企業だけでなく、一般国民も含む）及び民間企業相互間の役割分担の下、対策を推進することが重要

- IoT が関わるサイバー攻撃やその対象となる IoT 機器の実態を把握するために取り組むとともに、IoT の利用者等に対する注意喚起等の対策を実施
- 安全な IoT システムの構築に向けて、設計・製造段階、販売段階、設置段階、運用・保守段階、利用段階においてそれぞれの主体が必要な対策を実施。さらに、諸外国の動向を注視し、必要な国際連携を推進

４．２　国民が安全で安心して暮らせる社会の実現

- 近年、サイバー攻撃が複雑化・巧妙化し、深刻化している一方で、行政機関や企業が提供するサービスが情報通信技術の活用を前提としたものとなっていく状況の中、国民が安全で安心して暮らせる社会を実現するためには、関係する様々な主体が連携し、多層的なサイバーセキュリティを確保することが必要
- 政府機関や重要インフラ事業者等が提供する業務やサービスは、円滑な社会経済活動及び国民生活を支える基盤であり、これらの業務やサービスが安全かつ持続的に提供されるよう、任務保証の考え方に基づく取組を推進
- 2020 年東京大会等の国際的・国民的なビッグイベントを円滑に実施できるよう、各関係主体がそれぞれの役割を着実に果たし、皆で協力し合って対応していくことが必要

４．２．１ 国民・社会を守るための取組

- 政府機関、地方公共団体、サイバー関連事業者、重要インフラ事業者等、教育研究機関、国民一人一人が自主的にセキュリティの意識を向上させ、主体的に取り組む努力が不可欠
- サイバー犯罪が深刻な社会問題となっている中、関係機関・団体と連携し、積極的な対応を推進し、引き続き、犯罪対策を強化

（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る「積極的サイバー防御（仮称）」を推進（攻撃情報の共有・活用の促進、攻撃誘因技術の活用、ボットネット対策等）
- 国民が仮想通貨取引や自動走行車等を安全に利用できるよう、事業者等と連携し、対応を推進するとともに、全体の基盤となる信頼できる情報インフラの整備を促進

（２）サイバー犯罪への対策

- 深刻な社会問題となっているサイバー犯罪への対策として、広報啓発活動に加え、関係主体の連携強化、人材育成、情報共有、訓練等の拡充を推進し、情報収集・分析機能及び緊急対処態勢を強化するとともに、情報技術の解析の体制を強化

４．２．２　2020 年東京大会とその後を見据えた取組

・ オリンピック競技大会・パラリンピック競技大会は、開催国が国の威信をかけて実施する世界最大のスポーツイベントであり、世界中の注目が集まり、サイバー攻撃のターゲットとなる恐れ
・ 過去大会において多くのサイバー攻撃があり、被害があったとされている
・ 2020 年東京大会も、過去大会以上のサイバー攻撃が予想されることから、2015 年戦略、「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の準備及び運営に関する施策の推進を図るための基本方針」及び「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セキュリティ基本戦略（Ver.1）」に基づき、内閣サイバーセキュリティセンター（以下「NISC」という。）、関係府省庁、東京都、大会組織委員会等が連携して 2020 年東京大会に向けた取組を実施中
・ 整備した仕組み、その運用経験及びノウハウはレガシーとして、以降の我が国のサイバーセキュリティの確保のために活用

（１）2020 年東京大会に向けた態勢の整備

・ 2020 年東京大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象として、リスク評価に基づく対策の促進
・ サイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センター（政府オリンピック・パラリンピック CSIRT）の運用（2018 年度末を目途）に向けた構築の推進

（２）未来につながる成果の継承

・ 2020 年東京大会に向けて整備した仕組み、運用経験、ノウハウをレガシーとして、2020 年東京大会以降の我が国のサイバーセキュリティの確保のために活用
・ サイバーセキュリティ対処調整センターは、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、調整窓口となる組織として活用し、リスクマネジメントの手法は、全国の事業者等に適用できるように共有・普及促進

４．２．３　官民一体となった重要インフラの防護

・ 官民一体となって重要インフラを重点的に防護していくため、任務保証[14]の考え方に基づき、重要インフラサービスを安全かつ持続的に提供できるよう、第４次行動計画に基づいた取組を推進。必要に応じて見直しを実施。
・ 重要インフラの防護範囲について、社会的情勢に鑑み、必要に応じて対象を拡大し、面としての防護を強化
・ 重要インフラのセキュリティを更に高めるため、安全等を維持する観点から、安全基準等を策定するための指針を浸透させる取組を行うとともに、データの管理の状況に関する調査や国際動向も踏まえた望ましいデータ管理の在り方を含め安全

[14] 「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」では「機能保証」としていたが、趣旨は「重要インフラ事業者等が果たすべき役割を確実に遂行することが重要」ということであり、ここで言う「任務保証」と同じ趣旨である。

基準等を改善する取組を継続的に推進。また、官民の枠を超えた関係者間での演習・訓練を引き続き実施

（１）サイバー攻撃発生時における関係主体の冷静かつ適切な対応を促進する取組

・ 重要インフラ事業者等の関係主体間において認識の共有を図り、迅速な対応要否等の判断を行い、様々な関係主体の冷静な対処に資するものとして、重要インフラサービス障害等に係る深刻度評価基準を策定し、適時見直しを実施

・ 重要インフラ事業者等が事前のセキュリティ対策を講ずるだけではなく、事業継続計画（BCP）及びコンティンジェンシープランを策定することが重要であり、こうしたリスクマネジメントの活動全体が継続的かつ有効に機能するよう取組を推進

（２）地方公共団体のセキュリティ強化・充実

・ 地方公共団体のセキュリティに関するガイドラインの更新、事務用のネットワークのセキュリティレベルの確保、セキュリティ人材及び体制の確保・充実を支援する等の取組を推進

（３）制御系システムのセキュリティ対策

・ 制御系システムのインシデントや脅威情報に関する情報収集・分析・展開等を実施

・ 重要インフラ事業者等の経営層に対して、サイバーセキュリティに関する意識を高めるよう働きかけを実施

４．２．４　政府機関等におけるセキュリティ強化・充実

・ サイバー攻撃は複雑・巧妙化しており、その脅威は深刻化

・ 2020 年東京大会をはじめとした国際的イベントの開催を控え、さらにサイバー攻撃のターゲットとなることも予想

・ 行政サービスの円滑な遂行は極めて重要な責務であり、セキュリティ関連投資の充実とともに、早急に対策を強化することが重要

（１）情報システムのセキュリティ対策の高度化・可視化

・ 攻撃側が優位である現状の改善を目指し、マルウェア等による攻撃からの保護能力を強化するため、マルウェアが動作するエンドポイントにおける挙動の監視・検知、情報システムのリアルタイム管理、全政府機関におけるデータ保護による情報漏えいの防止、検知した挙動情報の活用による検知能力の更なる向上等を推進

・ 予防・検知・復旧の各段階におけるセキュリティ施策を多層的に展開するとともに、政府機関等の横断的な監視を行う GSOC[15] と効果的かつ効率的に連携しつつ、情報システムにおけるセキュリティ対策の高度化及び可視化の推進

（２）クラウド化の推進によるセキュリティ施策の集約等

・ 各府省庁において情報の特性に応じて適切な情報システムの形態を選択する

[15] Government Security Operation Coordination team の略。政府機関情報セキュリティ横断監視・即応チーム

とともに、政府全体としてセキュリティ施策を効率的・効果的に実施できるよう、システムの構築と運用の集約及びセキュリティ水準向上の利点を活かすことができるクラウド化（政府共通プラットフォームの移行を含む）を推進

・ 政府機関のインターネット接続口の集約を推進し、GSOC による境界監視の効率化を検討

（３）先端技術の活用による先取り対応への挑戦

・ 近年、普及してきた情報システムの基盤の中には、サイバー攻撃による高い耐性を有するものがある。このような、新しい設計思想の下で誕生した情報技術を、政府機関等における活用の可能性を検討し、ベストプラクティスの蓄積を図り、防御側優位への転換を図る

（４）監査結果の活用

・ 本部が実施する監査の結果を、当該機関だけではなく政府機関等全体に活用するなど監査結果の活用を推進することで、サイバーセキュリティ対策の水準の更なる向上を推進

・ 本部が実施する監査において、（１）で対策を進めることとしている情報システムのリアルタイム管理で得られる情報も活用し、監査を効果的・効率的に実施するよう検討

４．２．５　大学等における安全・安心な教育・研究環境の確保

・ 多様な構成員、多岐に渡る情報資産、多様なシステムの利用実態等を有する大学等における安全・安心な教育・研究環境を確保するため、サイバーセキュリティ対策の推進が重要

・ サイバーセキュリティ対策を経営上の重要課題と位置づけ、組織的・計画的に取り組むことが必要

（１）大学等の多様性を踏まえた対策の推進

・ 教育・研究等の多様性を踏まえつつ、計画等に基づくマネジメント面及び技術面における自律的・組織的な取組を推進

・ 情報システムの防御力及びインシデント対処能力の向上とフォローアップを推進

・ 情報セキュリティリスクの把握とリスク等に応じた重点的な対策を推進

（２）大学等の連携協力による取組の推進

・ 学術情報ネットワークにおけるサイバー攻撃検知など、大学等の連携協力によるインシデント対応の体制構築や、共通課題の検討、知見の共有等の場を形成するなど、情報共有体制の構築を推進

４．２．６　従来の枠を超えた情報共有・連携体制の構築

・ 他の組織との連携を重視する認識が官民ともに着実に広がり、幅広い主体が情報

共有に参加

- サイバー空間と密接に関連する分野が一層増加する中、情報共有の裾野は更に広がり続けることが予想されるため、国は、関係者との緊密な連携の下、新たな役割を果たしていくことが必要

（１）多様な主体の情報共有・連携の推進

- 情報共有に取り組む主体の増加に伴い、情報の集約・分析や関係者との迅速な調整を担う役割の重要性が増している一方、積極的な情報共有が阻害されるといった課題も顕在化
- 専門機関を含む官民の多様な主体が安心して相互にセキュリティ対策に資する情報の共有を図るための体制を、国が各主体の自主性を重んじた上で形成することで、官民横断的、業界横断的な情報の共有・連携を推進
- 官民で複数組織されている各情報共有体制の特色や役割を踏まえ、連携や統合を検討

（２）情報共有・連携の新たな段階へ

- 国は多様な主体と連携し、積極的に情報提供に協力する者ほど恩恵を享受できる情報共有体制を構築することで、セキュリティを高めるためには双方向の情報共有が不可欠である、との認識を社会に広く醸成
- 他者からの協力を得るためには、自らが保有する情報を共有する行為が重要であることを明確にし、国も率先して自ら保有している情報を適切に提供
- 処理の自動化を推進するなどして適切かつ迅速な分析や各主体が真に必要とする情報の共有を実現していくとともに、我が国の情報共有の仕組みを発展させつつ、戦略的に国際社会へ発信
- 官民や業界といった従来の枠を超えて、各主体が共存・発展していくことのできる関係を構築できるよう、国は関係者と連携し、積極的に環境整備

４．３　国際社会の平和・安定及び我が国の安全保障

- 自由、公正かつ安全なサイバー空間の堅持のため、国際場裡における我が国の立場の発信、既存の枠組みを活用した我が国の安全を確保するための取組、国際連携の推進

４．３．１　「自由、公正かつ安全なサイバー空間」の堅持

- グローバル規模で自由、公正かつ安全なサイバー空間を実現するための、国際場裡におけるその理念の発信、サイバー空間における法の支配の推進

（１）「自由、公正かつ安全なサイバー空間」の理念の発信

- 国家による統制を強化するアプローチではなく、関係主体が連携・協働してサイバーセキュリティの確保に取り組む日本型のアプローチの発信、同盟国・有志国、民間団体等の多様な主体と連携した対応

（２）サイバー空間における法の支配の推進

- サイバー空間においても既存の国際法が適用されるという立場から、サイバー

空間における国際法の適用、規範の形成・普遍化についての議論への積極的関与。国際捜査共助や情報交換等、サイバー犯罪対策に係る国際連携の推進

４．３．２　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国家の強靭性を確保することにより国家を防御する力、サイバー攻撃を抑止する力、サイバー空間の状況を把握する力の強化

（１）国家の強靭性の確保

①　任務保証

・ 我が国の安全保障に関係する政府機関の任務遂行を保証するため、また、国民や社会に不可欠なサービスを提供するための、政府機関、重要インフラ及び重要サイバー関連事業者におけるサイバーセキュリティの確保の推進

・ 防衛省・自衛隊が保有するネットワーク・インフラの防護の継続的強化

②　我が国の先端技術・防衛関連技術の防護

・ 宇宙関連技術、原子力関連技術、セキュリティ技術、防衛装備品に関する技術等、我が国の安全保障上重要な技術を扱う事業者及び関係省庁における対策の強化。国立研究開発法人や先端的な技術情報を保有する大学、企業等における対策の促進

③　サイバー空間を悪用したテロ組織の活動への対策

・ サイバー空間におけるテロ組織の活動に関する情報の収集・分析の強化その他の必要な措置の実施。

（２）サイバー攻撃に対する抑止力の向上

①　対応措置

・ 我が国の安全保障を脅かすようなサイバー空間における脅威について、悪意ある者の行動を抑止し、国民の安全・権利を保障するため、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を選択肢として保持。内閣官房を中心とした関係省庁の連携体制の強化、有志国と連携した対応

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の、各国との連絡体制の構築、国家間の信頼の醸成

（３）サイバー状況把握（CSA[16]）の強化

①　対処機関の能力向上

・ 対処機関の情報収集・分析能力の質的・量的向上。高度な分析能力を有する人材の育成・確保、サイバー攻撃を検知・調査等するための技術の開発・導入・習得、カウンターサイバーインテリジェンスに係る取組の推進

②　サイバー攻撃対処能力向上のための脅威情報連携

・ 有志国とのサイバー脅威情報の共有の推進。また、攻撃情報、インテリジェンス、周辺情報について、内閣官房を中心とした政府内の脅威情報共有・連携体

[16] Cyber Situational Awareness の略

制の強化、官民における脅威情報共有の推進とそのための環境整備

４．３．３ 国際協力・連携

・ 世界各国との政府・民間様々なレベルでの多層的な協力・連携の実施による国際社会の平和・安定及び我が国の安全保障の実現

（１）知見の共有

・ 二国間のサイバー協議や国際会議を通じた、互いのサイバーセキュリティ政策や戦略、体制等に係る情報交換、戦略的パートナー国との二国間の協力・連携の強化

（２）事故対応等に係る国際連携の強化

・ サイバー攻撃情報や脆弱性情報を平素から共有し、事故発生時に連携対処するための CERT 間連携の強化。国際サイバー演習への参加や共同訓練等を通じた連携対処能力の向上。事故発生時の適切な国際連携による対処

（３）能力構築支援

・ 日本を含む世界全体へのサイバー攻撃によるリスク低減のための、開発途上国における能力構築支援の積極的な実施

４．４ 横断的施策

４．４．１ 研究開発の推進

・ 様々な技術・サービスの戦略的な組み合わせ（インテグレーション）によって実現されるサイバー空間におけるイノベーションを支えるため、情報通信技術の利活用の動向とそれに対するサイバー攻撃の脅威を踏まえた、実践的なサイバーセキュリティの研究開発が必要。併せて、中長期的な技術・社会の非連続的進化を視野に入れた対応も必要

（１）実践的な研究開発の推進

・ インテグレーションの安全確保に必要となるセキュリティ技術の研究開発の推進

・ 先端的な情報通信技術に対応したセキュリティ技術の研究開発の推進

・ 深刻な悪影響を及ぼす可能性のある技術的課題に関する研究・検証体制の構築

（２）研究開発環境の整備

・ 研究人材の育成、高度技術を生かしたセキュリティ製品やサービスの開発や提供ができる人材の育成

・ 研究開発資金の戦略的・集中的投資

・ 法律や規格・慣行、マネジメントなど、研究開発を行う際の課題となっている制度等に関わる検討の推進

（３）国内外への積極的な発信

・ 我が国の研究開発の取組を国内外に積極的に発信

４．４．２ 人材育成・確保

・ 将来の社会の劇的な変化（パラダイムシフト）を見据えた、産学官の協働による需要（雇用）と供給（教育）の好循環の形成

（１）戦略マネジメント層の育成

・ 事業そのものの戦略企画・マネジメントの役割を担う人材層を想定

・ 経営層の方針を踏まえつつ、自社の事業に必要なサイバーセキュリティ対策を定義し、社内外の実務者・専門家を活用・指揮しつつ、対策やインシデント対応を実践

（２）実務者・専門家層の育成

・ 戦略マネジメント層の指揮の下、その人材層の期待に応えつつ、セキュリティ技術の進化を意識し、中長期にわたって活躍できる実務者・専門家の育成

・ 高度技術を生かしたセキュリティ製品やサービスの開発や提供ができる人材の育成

（３）人材育成基盤の整備、国際連携の推進

・ 中長期的な情報通信技術の進化を見据え、応用分野であるサイバーセキュリティの土台となる基礎原理の理解を促し、論理的思考力や概念的思考力の育成を充実。また、人材育成における国際連携の推進

４．４．３ 全員参加による協働

・ 国民一人一人が、サイバー空間につながる（参加する）ことによって得られる恩恵だけでなくリスクを認識し、そのリスクに対して適切に対処すること（リスクマネジメント）が必要

・ それを支えるものとして、関係者の役割を明確化し、協働を促進

（１）政府による取組

・ NISC が中核的役割を担いつつ、戦略的な情報発信、相談対応等に向けた産学官の連携体制の強化、サイバーセキュリティ月間を実施

・ 国民向け教材の作成・普及や、学校教育を通じた最低限、国民が知っておかなければならない情報モラル教育の一部としてのサイバーセキュリティ教育の推進

（２）関係団体等の連携

・ 地域、企業、学校など様々なコミュニティにおける取組の促進（例えば、地域（ボランティア活動）、企業（社員から家族へ）、学校（友人から友人へ））

（３）安全・安心な利用環境の確保

・ 国民に PC,スマホ等を提供する者（供給者）が、適切にサイバーセキュリティの取組を実施するとともに、国民への説明責任や社会貢献などの社会的責任を果たしていくことを期待

５ 推進体制

- NISC は、本部の事務局として、本戦略に基づく諸施策が着実に実践されるよう、各府省庁間の総合調整、産学官連携の促進等の要となる主導的役割を担う。また、危機管理対応についても一層の強化を図る。
- とりわけ、2020 年東京大会を控える中、産学官民の参加・連携・協働の枠組みを構築し、サイバーセキュリティの確保に向けた取組の着実な履行が重要
- サイバーセキュリティ政策は、経済発展及び危機管理・安全保障の観点から極めて重要であり、政策をより一層強力に推進するため、本部は、戦略で示された方向性に基づき各省庁の施策が効果的に実施されるよう、経費の見積もり方針を定め、政府全体としての最適な予算の確保と執行
- サイバーセキュリティの確保は、我が国の危機管理、安全保障上においても重要な課題であることから、本部は、必要に応じて、重大テロ対策本部や安全保障会議と緊密な連携により対応
- 本部が方向性を示し、それを踏まえ、政府機関がそれぞれの機能を果たし、政府一体となったサイバーセキュリティ対策を推進。３年間の戦略期間内各年度の年次計画を作成するとともに、その施策の進展を振り返り、年次報告として取りまとめ
- サイバー空間に係る情勢や技術前提が非連続的に変化することもあり得るため、必要が生じた場合には、計画期間に縛られることなく、機動的な見直しを実施