資料３

「2020 年及びその後を見据えたサイバーセキュリティの在り方について」の検討状況

資料３－１　サイバーセキュリティ戦略中間レビュー概要

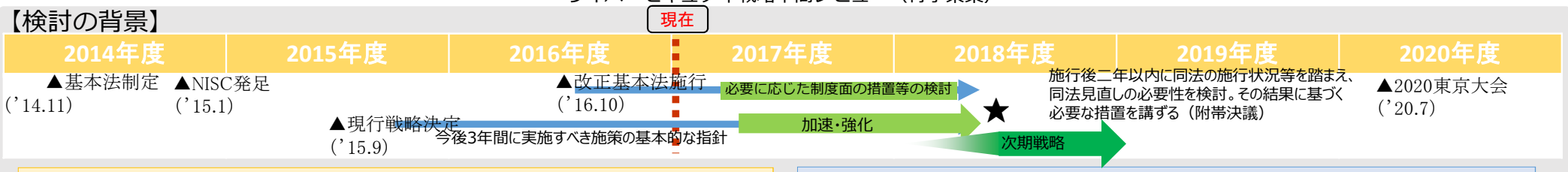
資料３－２　サイバーセキュリティ戦略中間レビュー（骨子素案）

2020年及びその後を見据えたサイバーセキュリティの在り方について

～サイバーセキュリティ戦略中間レビュー（骨子素案）～

資料3－1

【検討の背景】



◆ サイバーセキュリティ戦略の期間（～'18年9月）及び改正基本法の見直し期限（～'18年10月）まで1年余り

◆ 2020年東京ｵﾘﾝﾋﾟｯｸ･ﾊﾟﾗﾘﾝﾋﾟｯｸ競技大会に向けた抜本的対策を見据えた取組の必要（当該取組はその後も見据えたもの）

【脅威の変化】

脅威の一層の複雑化
- 新たな技術（AI,IoT等）の登場
- 攻撃の「サービス化」

防護対象の拡大
- 防護対象の面的増加（マイナンバー、先端保有技術者等）
- 官民におけるデータ利活用の進展

脅威のグローバル化
- IoT機器の指数関数的増大と拡散
- 同時多発的なグローバルなサイバー攻撃等の増加

2020年及びその後に向けて更なる取組が必要

サイバーセキュリティ戦略における基本原則を再確認
- サイバー空間を健全に発展させる役割
  - サイバー空間ガバナンス
  - 安全でクリーンなサイバー空間
- サイバー空間を利用する立場
  - 国民の安全と権利を守るためのサイバー空間の安全の確保

【強化・加速を行う項目の例】

経済社会の活力の向上及び持続的発展

- **ボット（注）撲滅の推進**
  - ✓ IoT機器・システムのセキュリティ対策の実態の把握・確認、是正が必要なものに対する周知・対策、今後製造・輸入される製品・システム等に対する対策等

  （注）ここでは、IoT機器等を外部から遠隔操作するための不正プログラムを指している。
- 安全なＩｏＴシステムの創出による国際競争力の強化（国際標準化）
- セキュリティに係るビジネス環境の整備

国民が安全で安心して暮らせる社会の実現

- **ﾊﾞｰﾁｬﾙ情報連携ｾﾝﾀｰ（仮称）の構築・運用**
  - ✓ 官民が連携し、インシデント情報やその脅威情報を集約・分析し、関係主体と迅速に共有し、対処できる仕組みの強化
- サイバー対処態勢の深刻度判断基準の整備
- 政府機関・独法等における効率的・効果的防護体制の再構築
- 地方公共団体におけるセキュリティ対策向上
- 大学におけるセキュリティ対策の向上支援
- サイバー犯罪・サイバー攻撃対策の強化

国際社会の平和・安定及び我が国の安全保障

- 組織・分野 横断的な取組等による我が国の安全の確保
- 先端技術の防護
- 国際連携の強化（日米、日ASEAN等）
- サイバー犯罪・サイバー攻撃対策の国際的な連携の強化

- 高度人材、経営層との橋渡し人材等幅広い階層における人材育成・確保の継続的な促進
- 研究開発等の推進
- 普及啓発

- **2020年東京ｵﾘﾝﾋﾟｯｸ･ﾊﾟﾗﾘﾝﾋﾟｯｸ大会に向けた体制の整備**
  - ✓ サイバーセキュリティ対処調整センターの構築、セキュリティ調整センター（仮称）との緊密な連携・調整
  - ✓ セキュリティ情報センターの構築
  - ✓ リスクマネジメントの促進

（参考）サイバーセキュリティ戦略

1 サイバー空間に係る認識
2 目的
3 基本原則
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
- 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
- 研究開発の推進、人材の育成・確保

5 推進体制

【スケジュール】

2017年4月18日　戦略本部（第12回）　骨子素案の決定
本年夏頃　戦略本部　方針の決定
} この間、有識者会合の開催（随時）

～2018年6月　可能な施策から段階的に実施（必要な制度面の見直しも含め、1年以内の実施）

資料３－２

サイバーセキュリティ戦略中間レビュー（骨子素案）

１．総論

サイバー空間は、様々な役割を担う多様な主体による連携のもと自律的なガバナンスの基により発展してきた。情報の自由な流通が確保されることで、民間企業を中心とした新たな創意と発想による無限の価値を産みだす場となり、人類に対して計り知れない恩恵をもたらしてきた。このように発展を続けるサイバー空間の中で流通する情報量は爆発的に増加している中、近年のサイバー攻撃の激化などサイバー空間における脅威がますます高まる状況にあることから、その対応も従来の離散的なものからサイバー空間における全体的な状況を踏まえたものとする必要が生じている。また、サイバー空間を構成するネットワーク、コンピュータ等の技術革新に加え、ＩｏＴ、人工知能（ＡＩ）、ブロックチェーンなどの新しい技術は社会経済に対する影響の度合いを急速に増しており、サイバー空間における関係主体の概念にも影響を及ぼす可能性も生じているが、このような急速な技術革新に適時適切に対応する必要がある。また、サイバー空間の関係主体は通信サービスを提供する事業者、サイバー空間上で様々なコンテンツやサービスを提供する事業者などの技術を有する者だけでなく、一般企業、個人にも拡大し、その数がさらに増加・拡散するとともに、官民におけるデータの活用がより一層進展することも想定される。今後、サイバー空間が一層発展することが期待されるなか、引き続き、国としても情報の自由な流通の確保など従来の基本原則を維持し、グローバルなサイバー空間の健全な発展に向けて、これらの政策を強化・加速するため、以下の方針に基づく取組を進めることとする。

＜我が国が立脚する基本原則の実現へ向けた方針＞

（１）サイバー空間を健全に発展させる役割を担う立場

ア．サイバー空間ガバナンス

サイバー空間が民間部門が主体となって構築・運用している空間であり、新しいサービス・技術が次々と産み出される場であることを踏まえ、我が国の立場・地位の保持も念頭に置いて、新たな技術・サービスに技術的・経済的に門戸を開放し、特定の関係主体に偏らないよう配慮しつつ、その自律的な発展を支持する。

イ．安全でクリーンなサイバー空間

国民の活動の場、経済活動の場として必要であるサイバー空間の健全な発展を確保するため、セキュリティ・バイ・デザインのより一層の推進を図りつつ、安全でクリーンなサイバー空間の実現を目指す。

ウ．多様な関係主体による連携と役割分担

多様な役割を有する者（マルチステークホルダー）が連携しつつ、適切な役割分担を行いながら自発的・主導的に取り組むことを促す。その際、国は枠組みを整備し、取組を活性化・発展させる結節点の機能を果たす。

エ．グローバルな連携

サイバー空間においては国境を意識することなく活動できるという長所を損なうことなく、そのセキュリティを確保することが重要であるため、上記の方針に基づく取組を進める上で国外の多様な関係者とも連携する。

（２）サイバー空間を利用する立場

国は、国民の安全と権利を守るため、サイバー空間の安全の確保を図る。その実現の際、（１）で述べた視点も踏まえ、国から付加価値を付与するスタイルでの官民連携を重視することとし、（１）と（２）のバランスをとりながら以下の取組を進める。

ア．サイバー犯罪・サイバー攻撃対策

サイバー空間における脅威は深刻化している中、社会情勢等の変化に的確に対応しつつ、これらの脅威先制的かつ能動的に対処するため、情報収集、官民連携、態勢の強化等を通じてサイバー犯罪・サイバー攻撃への対処能力・捜査能力を向上させる。

イ．重要インフラ及び政府機関防護のための対策

重要インフラ及び政府機関の機能・サービスを保証するための対策を推進することとし、サイバーセキュリティ基本法の理念に基づき、各主体の自主的・積極的な取組を基本とする。

ウ．我が国の安全の確保

自由な、公正かつ安全なサイバー空間を希求する立場から国際協調主義に基づく「積極的平和主義」をもって国際社会の平和と安定を実現することにより、我が国の安全保障を確保する。

２．現状認識

平成２６年１１月に制定されたサイバーセキュリティ基本法に基づき、平成２７年９月に閣議決定されたサイバーセキュリティ戦略により様々な政策を推進してきているが、平成２８年１０月、国の行政機関に加えて、独立行政法人や戦略本部が指定する法人について監視、分析、原因究明調査等を行うことを旨とする改正法が施行された。

この基本法の改正に当たっては、施行後２年以内にその内容を見直し、必要な処置を行う旨の附帯決議がなされている。また戦略は決定後１年半が経過し、総論で述べた技術変革等に伴う社会・経済に生じている様々な変化に対応し、２０２０年東京オリンピック・パラリンピック競技大会（「２０２０東京大会」）に向けた体制・

対応等の準備を加速・強化する必要がある。更に、平成２８年１２月に施行された官民データ活用推進基本法に基づき、官民データの活用がより一層進むことが想定され、情報の円滑な流通の確保を図る上で、データを安心・安全に活用する観点を踏まえた対策を講じることも必要となっている。このため、現状の戦略における取組について、戦略の見直しを待たずしてさらに迅速に対応できる体制の整備等を行いつつ取り組む必要がある。

３．各論（今後の諸施策の推進方針）

（１）これまでの進捗状況

戦略に基づき、サイバーセキュリティ基本法の改正、第４次重要インフラ行動計画策定、ＧＳＯＣの機能強化及び独法・指定法人への段階的拡張、政府セキュリティ人材確保（専任審議官設置等）、サイバーセキュリティ人材育成プログラムの改定等を実施し、各取組とも一定の進展があったところであるが、現状認識を踏まえて、以下の取組については加速・強化を行う必要がある。

（２）今後の政策推進強化方針

①　横断的項目

（ア）（バーチャル）サイバー情報連携センター（仮称）の構築・運用

サイバー空間を安全に利用でき、また安全に発展させるよう、サイバーインシデント情報やその脅威情報を分析し、民間等の関係主体と共有することで着実にそのインシデント等への対応に繋がる仕組みの構築を進める。

この仕組みの構築に当たっては、官民の役割分担・責任関係の明確化、官民での連携を行うことにより、民間企業等の利用者にとって検知、判断、決定・行動をより容易に行うことが可能となり、提供者と受領者が互いに価値を見いだせる仕組み（自動化等を含む。）とする。なお、その際、業界毎の情報共有体制を推進しつつ、その状況を踏まえるものとする。

また、内閣サイバーセキュリティセンターが官民連携の活性化を進める結節点として機能するよう、専門機関の活用等による体制の抜本的強化を図ることとする。

その際、制度的枠組の構築を含めた環境整備を併せて行う。

（イ）ボット撲滅の推進

サイバー環境をよりクリーンなものに保つため、国内外の官民が連携して、意図せずに悪意あるＩＣＴ利用に加担するセキュリティ対策が不十分な機器・システム等を是正するための対策を講じる。

そのため、現状において大規模なサイバー攻撃に利用される可能性のあるＩｏＴ機器・システムについての実態の把握・確認、すでに攻撃を受けて是正が必要なものに対する周知と対策の働きかけ、今後製造・輸入される製品・システム等に対して講じるべきセキュリティ対策等の取組を進める。

（ウ）２０２０年東京大会に向けた体制の整備

「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）」に基づき以下の取組を推進する。

ａ．サイバーセキュリティ対処調整センター（オリンピック・パラリンピック CSIRT）の構築

セキュリティ調整センター（仮称）との緊密な連携・調整のもと、物理的な対策と連動しつつ、政府機関、重要サービス事業者等に対するサイバーセキュリティに係る脅威・事案情報の収集・提供及び対処支援の総合調整を行う中核的組織としてサイバーセキュリティ対処調整センターを構築する。その際、制度的枠組の検討を併せて行う。また、同センターを中核とする対処体制のため、要員の計画的訓練を図る。

ｂ．セキュリティ情報センターの構築

平成２９年７月を目途に警察庁に設置することとされているセキュリティ情報センターにおいて、国の関係機関の協力を得て、サイバーセキュリティに係るものを含む２０２０年東京大会の安全に係る情報を集約し、大会の安全に対する脅威及びリスクの分析・評価を行い、関係機関等に対し必要な情報を随時提供する。

ｃ．リスクマネジメントの促進

２０２０東京大会の円滑な運営のため、リスクの明確化、第三者による監査の支援等を通じた重要サービス事業者等におけるリスクマネジメントを促進するとともに、横断的に国としても戦略的リスク評価（２０１８年度までに全分野において実施）を行い、これに基づくマネジメントを強力に進める。その際、サイバー空間における事象が物理空間に影響し得ることを念頭に、各重要サービスを構成する業務、経営資源及び情報システム・制御システムの鳥瞰図的な把握、安全の観点からの整理が必要であることに留意する。

②　個別的・基盤的項目

（ア）経済社会の活力の向上及び持続的発展

ａ．安全なＩｏＴシステムの創出による国際競争力の強化

ＩｏＴシステムに関係する分野に共通する用語を定義した上で、その設計、開発、運用に係る概念を国際的に共通化する取組を国際標準化として進めるとともに、この標準に基づく安全、高品質を訴求できるＩｏＴシステムを実現することで、世界的な市場シェアの獲得を目指す。

ｂ．人材育成・確保の継続的な促進

ＩｏＴ、ＡＩ、ビッグデータなど、ＩＴの利活用により新しい価値を創造するためのビジネス・イノベーションと一体となったサイバーセキュリティ人材育成の取組も進めるため、引き続き産業界と連携し、サイバーセキュリティを経営問題としてとらえ、経営層の意識改革、「橋渡し人材層」

の育成、様々な役割を担う人材がチームとなって対応できるような人材育成を推進するとともに、中小企業のサイバーセキュリティに引き続き取り組む。また、政府機関における人材確保・育成に引き続き取り組む。加えて、各種人材育成・確保プログラム施策の有機的な連携により効果的かつ効率的な施策の実施を推進する。

c．セキュリティに係るビジネス環境の整備

我が国の政府機関や企業等のサイバーセキュリティの確保に向けて、サイバーセキュリティに係る投資を促進することで、セキュリティ産業における継続的な需要喚起を促す。

（イ）国民が安全で安心して暮らせる社会の実現

a．サイバー対処態勢の整備

事象を評価する既存の国際的な基準等を参考としたリスクベースによる重要インフラサービス障害等の深刻度の判断基準、事業継続計画（ＢＣＰ）及びコンティンジェンシープランの整備、情報セキュリティ対策に係る安全基準の継続的改善及び関係主体における共同訓練の実施等を推進し、サイバー攻撃に係る対処態勢を強化する。

また、危機管理体制との連携を強化し、サイバー空間、物理空間の両方に影響を与える事象にも適切に対処する。

b．政府機関・独法等における防護体制の在り方

近年のネットワーク技術、セキュリティ技術等の進展を踏まえ、現行の監視・検知・対応技術を見直し、より効率的・効果的な技術の在り方とともに総合的な運用・管理方策について検討し、政府機関・独立行政法人・指定法人に適用する。

c．地方公共団体におけるセキュリティ対策の向上

中小規模の地方公共団体におけるセキュリティ対策の向上を支援する。その際、こうした団体における人的・予算的な制約の現実を考慮し、クラウド等を活用したシステムの一層の集約化も併せて検討する。

d．大学におけるセキュリティ対策の向上

多岐に渡る情報資産、多様なシステムの利用実態といった大学における多様性を踏まえ、当該特性に応じて、大学のマネジメント面・技術面の取組の強化を促進するとともに、大学の相互の協力による自立的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る枠組みを整備し、これらの取組を支援する。

e．サイバー犯罪・サイバー攻撃対策の強化

民間事業者等と連携し、サイバー空間における情報収集・分析機能及び緊急対処態勢を強化するとともに、民間事業者等における適切な対策を促すための広報啓発活動に加え、犯罪抑止に資する徹底した捜査活動や新たな手法等の検討を推進する。

（ウ）国際社会の平和・安定及び我が国の安全保障

ａ．我が国の安全の確保

サイバーセキュリティを脅かす不正行為や、国家の関与が疑われるものも含め、組織的かつ周到に準備されたサイバー攻撃が高度化していることを踏まえ、これら脅威からサイバー空間を守り、その自由かつ安全な利用を確保するとともに、重要な社会システムを防護するべく、サイバー空間の状況把握・分析能力の一層の向上や対処機関の能力の質的・量的向上の取組を加速化する。その際、国全体として、関係機関相互の連携強化及び役割分担の明確化を図りつつ、組織・分野 横断的な取組を総合的に推進するとともに、有志国・機関との連携をさらに推進する。また、国民の安全・権利を保障し、国家安全保障を図るため、採り得る全ての有効な手段を選択肢として確保する。

ｂ．先端技術の防護

先端的な技術を保有する国立研究開発法人について、科学技術競争力や安全保障等に係る技術情報を保護する観点から、当該法人のマネジメント・技術面の取組を促進するとともに、これら法人相互の協力による自立的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る支援を本格化させる。

また、先端的な技術情報を保有する大学に対しても、サイバー攻撃による当該情報の漏えいを防止するための取組を促すとともに、支援する。なお、これら取組の実施に当たっては、研究や教育の進展に資するよう、その特性にも配慮する。

ｃ．国際連携の強化

戦略の目的及び戦略に基づきサイバー空間を健全に発展させ、安全に利用できる役割を担う立場としての我が国の基本的方針に則り、サイバー空間における国際的な「法の支配」の確立、ルールづくり、信頼醸成、能力開発その他の取組について国際的な連携を進める。ＡＳＥＡＮなど開発途上国との連携を図る際には、「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）」（平成２８年１０月戦略本部報告）を念頭に置いて、必要な協力・支援等を進める。

特に、バーチャル情報連携センターを構築・運用する際には、国際的な連携を重視する。

ｄ．サイバー犯罪・サイバー攻撃対策の国際的な連携の強化

国際機関、外国治安情報機関等との間における捜査共助、職員派遣等の国際連携を推進し、国境を容易に越えるサイバー空間の脅威に対処する。

（エ）基盤的施策

ａ．研究開発等の推進

ＩｏＴ技術、ＡＩ、ＡＲ／ＶＲ技術などによって、実空間とサイバー空

間の融合が高度に深化し、新しい価値が創出されていく中で、単に情報システムへの脅威に対応するだけでなく、「人間」や「人間が安心して暮らすことのできる社会システム」を守り、強くしていくための方策をサイバーセキュリティに関する研究開発戦略として策定し、必要な研究開発の推進及び前述の先端的な技術がもたらす社会的影響等の検討を支援する。その際、技術面にとどまらない異分野（脳科学、政治学などの社会科学、文化人類学など）の方法論も視野に入れる。

また、サイバー攻撃の解析等に要する関連技術の研究開発を推進するとともに、関係主体が安全に、また安心してシステムやサービスを利活用できるようセキュリティに関する基準を策定する。

ｂ．普及啓発

今後のＩＴ社会の一層の進展、ＩｏＴの普及等から一般利用者がサイバー社会により触れる機会がより多くなるとともに、中小企業等はサイバーセキュリティ対策に十分な投資ができないことを踏まえ、その対策を支援する観点から、普及啓発に関するプログラムを策定する。一般利用者がサイバーセキュリティの考え方に関心を持つ機会を設けるとともに、中小企業等を含め、適切なセキュリティ対策を講じることを支援する。