サイバーセキュリティ戦略・サイバーセキュリティ2018の概要

資料２－４

◆ 新たなサイバーセキュリティ戦略(2018年７月)は、サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの

◆ サイバーセキュリティ2018は、同戦略に基づく初めての年次計画であり、各府省庁はこれに基づき、施策を着実に実施

＜新戦略(2018年戦略)（平成30年7月27日閣議決定）の全体構成＞

1 策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2 サイバー空間に係る認識

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3 本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

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

～新たな価値創出を支えるサイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 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
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現

～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 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

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

5 推進体制

内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

現状認識と将来像（サイバー空間と実空間の一体化に伴う脅威の深刻化）

中長期

策定の趣旨・背景

【（2015年戦略策定時）連接融合情報社会の到来】
～実空間のヒト・モノがネットワークに**連接**され、
実空間とサイバー空間の**融合**が高度に深化～

一体化

【サイバー空間と実空間の一体化、活動空間の拡張】

サイバー空間に係る認識

・AI、IoT 、Fintech 、ロボティクス、３Dプリンター 、AR/VR など、**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に変革をもたらす**イノベーションを牽引する一方で、不確実さは常に内在**

サイバー空間がもたらす恩恵

・サイバー空間における技術・サービスが**制御され、様々な分野で当然に利用されており、人々に豊かさをもたらしている**。
・深層学習による**AIの進化**により、既に幅広い産業に応用され始めている。
・**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されつつある。

サイバー空間における脅威の深刻化

・サイバー空間における技術・サービスを**制御できなくなるおそれは常に内在しており、多大な経済的・社会的な損失が生じ得る。**
・重要インフラサービスの障害やIoT機器の意図しない作動により、様々な**業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ、国家安全保障上の問題**に発展する可能性
・サイバーセキュリティ対策の不備が、**金銭的な損害を直接引き起こし**、拡大することが予想される。

サイバー空間における脅威の深刻化に関する事例（国内外のサイバー攻撃等の事案）

【国内】

○民間企業を標的としたOSインジェクション攻撃（2016年4月）

2016年4月20日から同28日にかけて、ソフトウェアの脆弱性を突いたOSインジェクション攻撃により、 民間企業4社（日本テレビ、J-WAVE、栄光ゼミナール、エイベックス）から合計**142万人分の個人情報が流出**する事案が発生した。

○ダークウェブによるクレジットカード情報の取引（2017年4月）

発信元の特定が困難な**「ダークウェブ」と呼ばれるインターネット上のサイトで、日本のクレジットカード会社の利用者約10万人分の個人情報が売買**されていることが海外のセキュリティー会社の調査で分かった。サイバー攻撃を受けた企業などから流出したとみられる。

○金融機関を標的としたDDoS攻撃（2017年9月）

外国為替証拠金取引事業者など**金融事業者を狙ったDDoS攻撃**が継続。一部の事業者では攻撃による被害と障害復旧を公表した。

○仮想通貨の窃取を狙った攻撃（2018年１月）

登録申請中のみなし仮想通貨交換業者が保有していた仮想通貨（NEM）が不正に外部に送信され、**顧客からの預かり資産5億2,300XEM（約580億円）が流出**した。

【海外】

○バングラデシュ銀行（2016年2月）

2016年2月5日、バングラディシュ中央銀行がハッキングを受け、**約8,100万ドル（約91億円）が不正送金**された。ニューヨーク連邦準備銀行のバングラディシュ中央銀行の口座情報が流出し、その口座から他の銀行の口座に送金された模様であり、犯行は銀行が営業していない日に行われた。米国のセキュリティ会社は、攻撃手法は過去に北朝鮮の関与が断定された手法と同様だったと明らかにした。

○ドイツ原子力発電所（2016年4月）

2016年4月、ドイツの原子力発電所で、**燃料棒監視システムにてマルウェアが発見された**。マルウェアとしては、リモートアクセスを行うトロイの木馬と、ファイルを盗み取るマルウェアの2種類が存在していたが、同システムがインターネットに接続されていなかったことから、実質的な被害は出ていないようである。なお、感染対象としては、燃料棒監視システムとUSBメモリ18個

○Miraiによる大規模DDoS攻撃（2016年9月）

IoT機器に感染し史上最大規模のDDoS攻撃を仕掛ける新型マルウェア（いわゆる“Mirai”）が登場した。2016年9月、米セキュリティサイトKrebs on Securityが、ピーク時665GbpsのDDoS攻撃によって一時的にサイト閉鎖に追い込まれ、同22日には、フランスのインターネットサービスプロバイダーであるOVH社が、1.1Tbpsに達する大規模なDDoS攻撃を受けた。

○米Yahoo（2016年12月）

2013年8月に**10億件以上のアカウント情報が窃取**されていた。

○ウクライナ電力供給会社（2016年12月）

2016年12月17日深夜、ウクライナの国営電力会社Ukrenergoの**変電所がサイバー攻撃を受け**、キエフ北部及び周辺地域で**約1時間の停電が発生**

○英国の病院、仏ルノー等（2017年5月）

ランサムウェア**「WannaCry」の感染により、英国の国民保険サービス（NHS）関連システムが停止し、多数の病院で医療サービスが中断するなどの被害が続出。**また、仏ルノーでは車両の生産ラインの稼働が停止。その他にも、スペインのテレフォニカ、独のドイツ鉄道、米国のFedEx等、**世界各国で被害あり**。

2017年12月に、**米国は、このサイバー攻撃が北朝鮮によるものであるとして、北朝鮮を非難する旨発表**。同日、我が国も米国を支持し、北朝鮮を非難

(参考）諸外国の政策動向

米国

2017年５月、連邦政府のネットワーク及び重要インフラのサイバーセキュリティ強化に関する大統領令（EO13800）に署名。同大統領令に基づき、関係機関は以下の事項について報告書を発表

- 連邦政府のサイバーセキュリティ、IT近代化
- 重要インフラ防護
- ボットネット対策
- 抑止、国際協力
- 人材育成　等

EU

- 「ネットワーク情報セキュリティ指令」（NIS指令）を発行（2016年7月）、2018年５月までに加盟国において国内法化義務付け
- 「サイバー外交ツールボックス」の公表（2017年6月）
- サイバーセキュリティ強化に向けた政策パッケージの公表、サイバーセキュリティ法案（2017年9月）
- 一般データ保護規則（GDPR）が成立（2018年5月より施行）

英国

2016年11月に国家サイバーセキュリティ戦略を改訂

- 「防御」、「抑止」、「開発」を目的とすること
- 「積極的サイバー防御」の推進
- 「攻撃的サイバー能力」の保有・強化

等に言及

中国

2017年６月、「サイバーセキュリティ法」を施行し、同法に基づく以下関連規制を発行

- ネットワーク製品及びサービスの安全審査弁法
- 個人情報及び重要データの越境安全評価法
- 重要情報インフラ保護弁法　等

目指す姿（持続的な発展のためのサイバーセキュリティ　–「サイバーセキュリティエコシステム」の実現- ）

○　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※）の実現に寄与するため、実空間との一体化が進展しているサイバー空間の持続的な発展を目指す（「サイバーセキュリティエコシステム」の実現）。

○　このため、これまでの基本的な立場を堅持しつつ、３つの観点（①サービス提供者の任務保証、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していく。

※　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。（未来投資戦略2017より）

＜サイバーセキュリティの基本的な在り方のイメージ＞

- 自らが遂行すべき業務やサービスを「任務」と捉え、これを着実に遂行するために必要となる能力及び資産（*）の確保
- 一部の専門家に依存するのではなく、「任務」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

＊：人材、装備、施設、ネットワーク、情報システム、インフラ、サプライチェーンを含む

- 組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応

- 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取組
- 平時・事案発生時の、各々の努力だけでない、情報共有、個人と組織間の相互連携・協働を新たな「公衆衛生活動」と捉える

新たな価値創出を支えるサイバーセキュリティの推進

・全ての産業分野において、企業が事業継続を確固なものとしていくとともに、新たな価値を創出していくための動きを支えるための基盤として、一体的にサイバーセキュリティの確保に取り組む
・その際には、サイバーセキュリティ対策をリスクマネジメントの一環として捉え、取り組むことが重要

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

- 経営層の意識改革の促進（「費用」から「投資」へ）
- 企業のサイバーセキュリティ対策に関する積極的な情報発信・開示の促進
- 官民が連携してサイバーセキュリティ保険の活用を推進
- セキュリティビジネス強化に向けたガイドライン策定、リスク分析、研究開発等

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

- 脅威を明確化し、運用レベルでの対策を実現する業種横断的指針の作成
- 産業分野ごとの具体的対応策の提示
- 中小企業の取組の推進

３．安全なIoTシステムの構築

- IoTシステムに関するサイバーセキュリティの体系整備と国際標準化
- IoT機器の脆弱性対策モデルの構築・国際発信

（参考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：取組の例

経営層におけるサイバーセキュリティに取り組む必要があるとの認識を広げて必要な対策の検討・導入を促すとともに、市場がその取組を企業価値向上につながるものとして評価し、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の形成を目指す。

経営層の意識改革

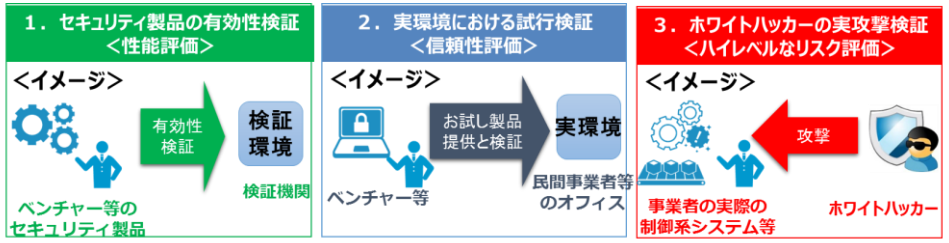
＜内閣官房＞
・官民の連携による、経営層に説明や議論ができる人材の発掘・育成、経営層向けセミナー等の開催

＜経済産業省＞
・取締役会の関与の促進や投資家への啓発の観点から、サイバーセキュリティへの経営層の関与を、上場企業で行われている「取締役会の実効性評価」の評価項目へ組み込むことを促進
・コーポレート・ガバナンス・システムに関する議論の中で、「守り」のリスク管理の一環として、サイバーセキュリティ対策を位置付けることを検討

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

＜経済産業省＞
・サイバーセキュリティ対策のニーズ明確化・具体化、シーズ発掘、ビジネスマッチングのための「コラボレーション・プラットフォーム」の設置（2018年6月より活動開始）
・日本のセキュリティニーズに応じたサイバーセキュリティ製品の有効性や、IoT機器等の脆弱性等を実機を通じて検証する仕組みの構築

＜実戦的サイバーセキュリティ検証基盤の全体像＞



サイバーセキュリティに対する投資の促進

＜総務省・経済産業省＞
・サイバーセキュリティ対策が講じられたデータ連携により生産性を向上させる取組に関するシステム・製品の導入に対して税額控除等を措置する「コネクテッド・インダストリーズ税制」により、事業者のセキュリティ対策の強化と生産性向上を同時に促進

【計画認定の要件】

データ連携・利活用
セキュリティ面
生産性向上目標

➢ 認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度） 5％ ※ （法人税額の20%を限度）

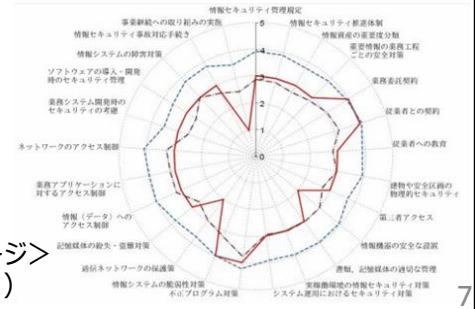
【対象設備の例】
データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、ＡＩ、ソフトウェア等）、サイバーセキュリティ対策製品 等

最低投資合計額：5,000万円
※ 計画の認定に加え、平均給与等支給額の対前年度増加率≧３％を満たした場合。

＜総務省＞
・ベストプラクティスも盛り込んだ「セキュリティ対策情報開示ガイドライン」（仮称）を策定、公表

＜経済産業省＞
・「サイバーセキュリティ経営ガイドライン」の活用促進に向け、「対策事例集」と自社の状況（成熟度）を把握するための「可視化ツール」の整備・活用を推進

＜可視化ツールのイメージ＞
（米国ＮＰＯとも協力）



(参考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：取組の例

サイバー空間と実空間の一体化が加速的に進展する中、「Society 5.0」の実現に向け、サプライチェーン全体を俯瞰した取組を推進する。

サイバーセキュリティ対策指針の策定

＜経済産業省＞

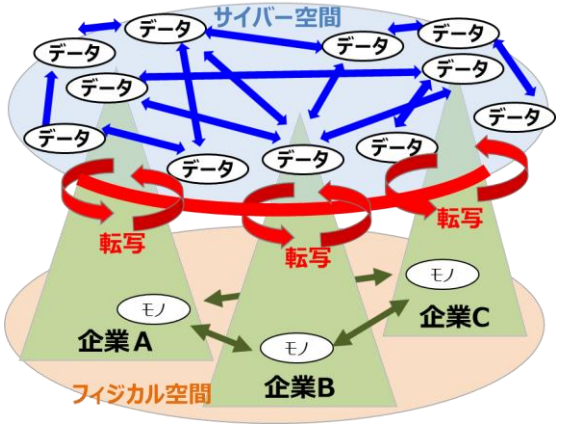
・サプライチェーンにおける脅威を明確化し、運用レベルでの対策が実施できるような業種横断的な指針として、「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定

・産業分野ごとに守るべきものやリスクに違いも存在するため、産業分野ごとにセキュリティ水準の検討を進めるとともに、その上で、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進める。

サイバー空間におけるつながり
【第３層】
- サービスを創造するためのデータの信頼を確保

フィジカル空間とサイバー空間のつながり
【第２層】
- フィジカル・サイバー間を正確に“転写”する機能の信頼を確保

企業間のつながり（従来型サプライチェーン）
【第１層】
- 適切なマネジメントを基盤に各主体の信頼を確保



中小企業の取組の促進

＜経済産業省＞

・中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION」への登録を促す。

★ 一つ星　★★ 二つ星

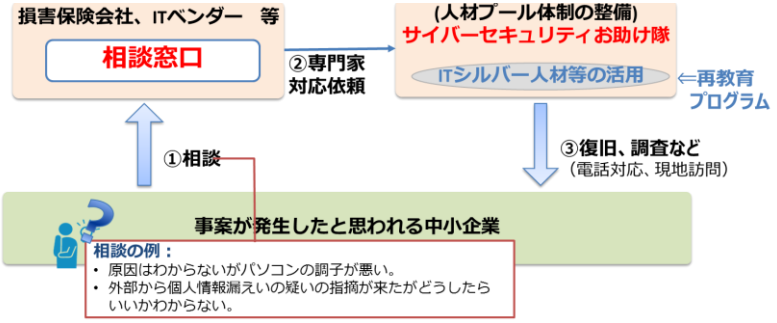
SECURITY ACTION ★ セキュリティ対策自己宣言

SECURITY ACTION ★★ セキュリティ対策自己宣言

■2018年7月現在で、自己宣言企業は13,000社弱

■中小企業庁と連携して、宣言企業数を大幅に加速させることが急務

・24時間相談窓口などの体制を持つ損保会社等と連携して、中小企業のサイバーセキュリティに関するトラブル対応を支援する「サイバーセキュリティお助け隊」を創設するとともに、ITに従事してきたシルバー人材の再教育などを通じて人的リソースを確保



＜サイバーセキュリティ保険等と連携した「サイバーセキュリティお助け隊」のイメージ＞

(参考③) 安全なIoTシステムの構築：取組の例

経済社会の発展に不可欠なインフラとしてのサイバー空間に悪影響を及ぼし得る脆弱なモノのサイバーセキュリティ対策が喫緊の課題。
官民が連携し、安全なIoTシステムの構築に取り組む。

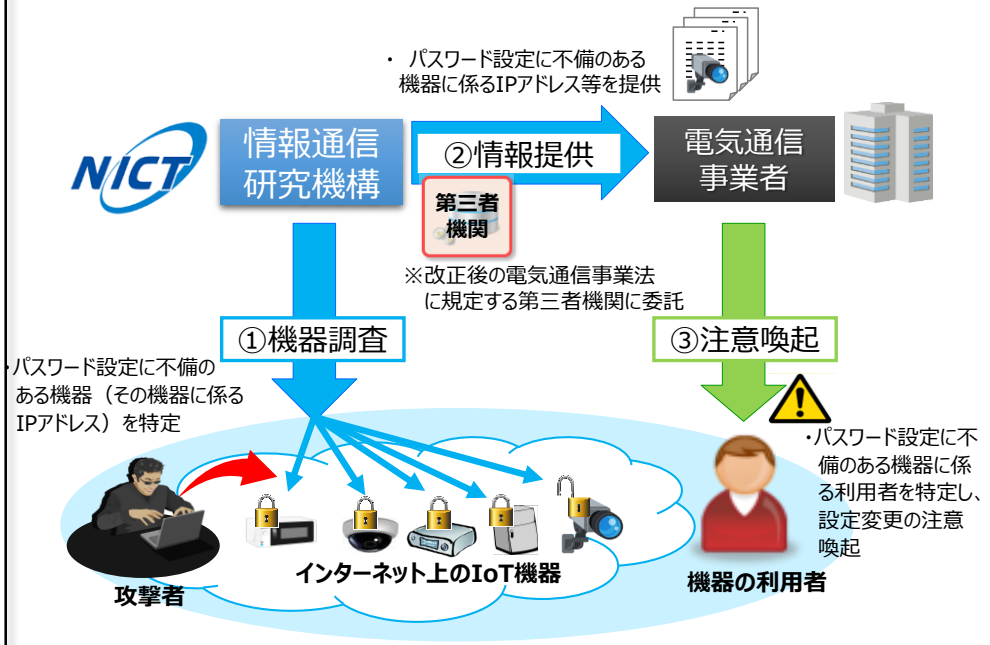
IoTシステムにおけるセキュリティの体系の整備と国際標準化

＜内閣官房＞
・各主体の間での共通認識の醸成と、役割や機能の明確化を図った上で、協働した取組を推進

自律的なIoTシステムに係る関係省庁の取組を推進するとともに、各主体が協働できるよう情報共有等の取組を推進する。

脆弱性対策に係る体制の整備

＜総務省＞
パスワード設定に不備のある機器の調査・特定を行い、利用者への注意喚起を円滑に行えるような所要の制度整備を推進



パスワード設定に不備のある機器の調査を行い、電気通信事業者の協力の下、当該機器の利用者を特定し、設定変更を促す取組を行う。

国民・社会を守る任務を保証

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、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、そして国民一人一人に至るまで、多様な関係者が連携して多層的なサイバーセキュリティを確保することが重要であり、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していく。

１．国民・社会を守るための取組

- 「積極的サイバー防御」の構築
  （脅威情報の共有・活用の促進、脆弱性情報の提供等）
- サイバー犯罪への対策

２．官民一体となった重要インフラの防護

- 重要インフラ行動計画に基づく取組の推進
- 地方公共団体の取組強化

３．政府機関等におけるセキュリティ強化・充実

- 情報システムの状態のリアルタイム管理の強化（新たな統一基準群に基づく取組等）

４．大学等の多様性を踏まえた対策の推進

- 各層別研修及び実践的な訓練・演習の実施

５．2020年東京大会とその後を見据えた取組

- サイバーセキュリティ対処調整センターの構築

６．従来の枠を超えた情報共有・連携体制の構築

- 多様な主体の情報共有・連携の推進

７．大規模サイバー攻撃事態等への対処態勢強化

- サイバー攻撃と実空間の双方の危機管理に挑むための対処態勢の強化

国民が安全で安心して暮らせる社会の実現

任務保証の実現（サービスの安全かつ持続的な提供）

情報共有・連携
（サイバーセキュリティ協議会、政府オリパラCSIRT等）

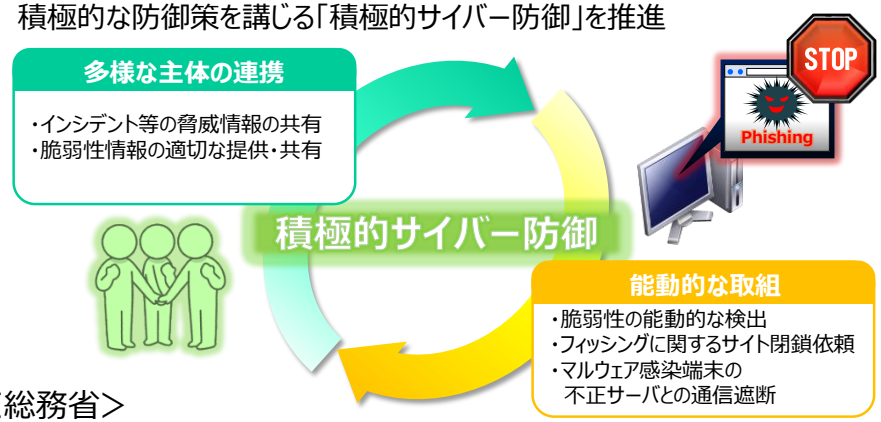
（参考①）国民・社会を守るための取組：取組の例

サイバー空間の脅威の深刻化に伴い、社会全体におけるサイバーセキュリティへの危機意識が高まっている状況を踏まえ、全ての主体が、自主的にセキュリティの意識を向上させ、主体的に取り組むとともに、連携して多層的にサイバーセキュリティを確保する状況を作り出していく

安全・安心なサイバー空間の利用環境の確保

「積極的サイバー防御」の推進

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」を推進

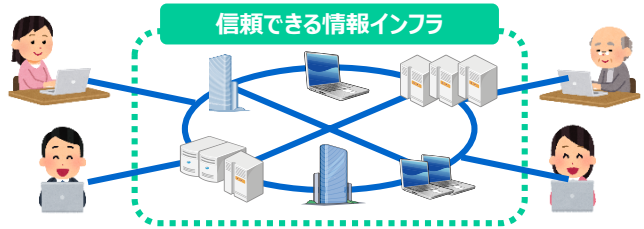


＜総務省＞
・先行的防御を可能にするための脅威情報の共有・活用の促進

＜経済産業省＞
・IoT機器を含むソフトウェア等の脆弱性対策情報ポータルサイト（JVN）において対策情報の公表、対策ツールの提供等を通じ、利用者の対策を推進
・フィッシングに関するサイト閉鎖依頼その他の対策実施に向けた取組

信頼できる情報インフラの整備の促進

＜内閣官房、総務省、経済産業省＞
・情報通信ネットワークに関連するハードウェア、ソフトウェアの市場動向及び技術開発動向等について調査を実施



仮想通貨、自動運転車等に関する対策の推進

＜金融庁＞
・仮想通貨交換業者におけるサイバーセキュリティの強化に向け、実効性のある自主規制機能の確立を促す

＜国土交通省＞
・国連自動車基準調和世界フォーラム（WP29）での自動車のサイバーセキュリティ対策に係る国際基準の策定の議論を主導

サイバー犯罪への対策

サイバー犯罪の実態把握・取締りの推進

＜警察庁、法務省＞
・取締り・捜査に必要な専門的知識・技能の習得のための各種研修の実施

＜総務省＞
・能動的・網羅的なサイバー攻撃観測技術の開発

官民が連携したサイバー犯罪対策の推進

＜警察庁、総務省、経済産業省＞
・被害防止のための広報啓発活動や最新の手口・被害実態等の情報共有の推進

＜警察庁＞
・民間事業者等の知見を活用した人材育成

＜警察庁、総務省＞
・事後追跡可能性の確保

（参考②）重要インフラ、政府機関、大学等におけるセキュリティ対策の推進：取組の例

官民一体となった重要インフラの防護

重要インフラの防護については、「任務保証」の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現するため、「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」に基づいた取組を推進

第４次行動計画に基づく主な取組

＜内閣官房、重要インフラ所管省庁＞

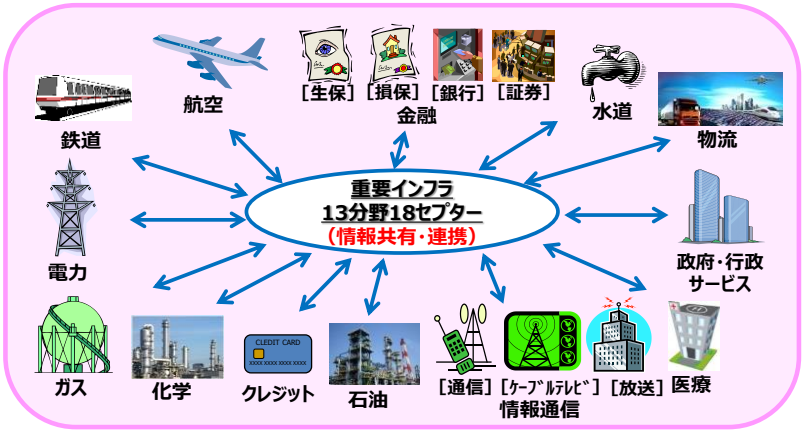
・リスクマネジメントの活動全体が継続的かつ有効に機能するよう取組を推進

・安全基準等を策定するための指針を浸透させ、業務内容や組織の規模等を考慮した安全基準等を継続的に改善

・サイバー攻撃による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

・官民の枠を超えた様々な規模の主体の間での訓練・演習を実施

・制御系システムに関する人材育成、脅威情報の情報共有等を推進



空港については2018年4月1日以降重要インフラ分野としての取組を開始。

地方公共団体のセキュリティ強化・充実

＜総務省＞

・セキュリティポリシーに関するガイドラインを随時更新

・地方公共団体職員を対象とした集合研修・eラーニングを実施

・緊急時対応訓練の支援及びCSIRTの連携組織の設立

政府機関等におけるセキュリティ強化・充実

新たな技術を活用し、情報システムのセキュリティ水準の向上を進めるとともに、その確認を通じて、従来の攻撃側優位の状況を改善する。併せて、組織的な対応能力の充実を行う

＜内閣官房、関係府省庁＞

・情報システムの防御能力の向上と状態のリアルタイムでの把握

・政府機関等における横断的な連携の高度化

大学等における安全・安心な教育・研究環境の確保

大学等において自律的にサイバーセキュリティ対策を行うとともに、大学等の連携協力によるサイバー攻撃への対応体制の構築や情報共有等を国が積極的に支援

＜文部科学省＞

・大学等の多様性を踏まえた対策を推進

・大学等の連携協力による取組を推進

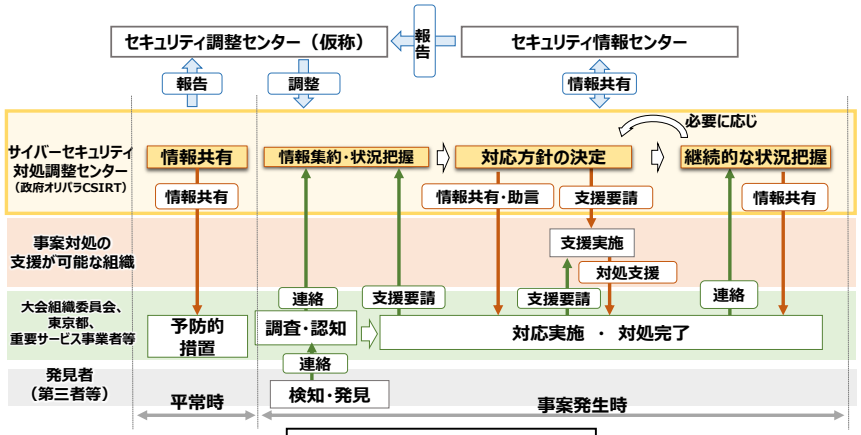
（参考③）2020年東京大会とその後を見据えた取組、情報共有や事態対処に関する取組：取組の例

2020年東京大会とその後を見据えた取組

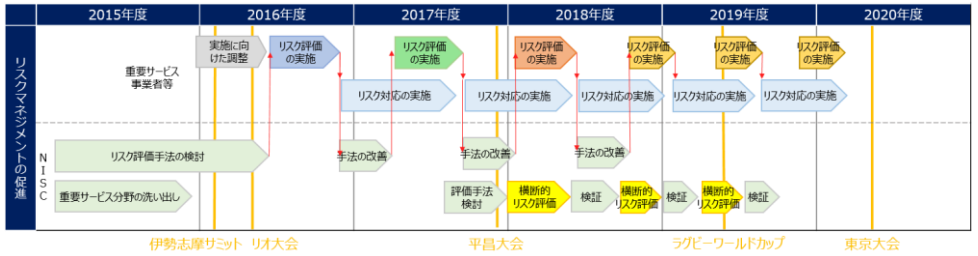
2020年東京大会のサイバーセキュリティの確保及びその後を見据えた施策を推進

＜内閣官房＞
・「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推進本部」の下の「セキュリティ幹事会」で決定された基本戦略に基づき大会の安全に関する情報の集約等の取組を推進

サイバーセキュリティ対処調整センターの構築



リスクマネジメントの促進



・大会後も各種施策は適用範囲を拡大して引き続き推進し、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、以降の我が国の持続的なサイバーセキュリティの強化のために活用

従来の枠を超えた情報共有・連携体制の構築

「参加・連携・協働」の観点から、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の推進を支援し、新たな役割を果たしていく

＜内閣官房＞
・官民の多様な主体が相互に連携し、安心して相互にサイバー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構築
・各主体が積極的に情報共有に貢献できる環境整備、処理の自動化等を推進

大規模サイバー攻撃事態等への対処態勢強化

大規模なサイバー攻撃の脅威から国民・社会を守るために、国が一丸となってサイバー空間の脅威への危機管理に臨む

＜関係府省庁＞
・関係府省庁、重要インフラ事業者等が連携したサイバー空間と実空間の横断的な対処訓練の実施

＜警察庁、個人情報保護委員会、経済産業省＞
・官民連携の枠組みを通じた情報共有を推進
・民間事業者等の対処能力の向上を支援する取組を推進

自由、公正かつ安全なサイバー空間の堅持

国際社会の平和・安定及び我が国の安全保障のために、自由、公正かつ安全なサイバー空間は必要不可欠である。自由、公正かつ安全なサイバー空間を堅持するため、国際場裡において我が国の立場を発信し、我が国の安全の確保に取り組み、国際協力・連携を進める。

１．自由、公正かつ安全なサイバー空間の堅持

- 自由、公正かつ安全なサイバー空間の理念の発信
  (我が国の意見表明や情報発信、サイバー空間の発展を妨げる取組への対抗等)
- サイバー空間における法の支配の推進
  (国際法の適用、規範の形成・普遍化についての議論への関与等)

２．我が国の防御力・抑止力・状況把握力の強化

- 国家の強靭性の確保
  (関係機関の任務保証、先端技術等の防護等)
- サイバー攻撃に対する抑止力の向上
  (実効的な抑止のための対応、信頼醸成措置等)
- サイバー空間の状況把握の強化
  (関係機関の能力向上、脅威情報連携等)

３．国際協力・連携

- 知見の共有・政策調整
- 事故対応等に係る国際連携の強化
- 能力構築支援

（参考①）サイバーセキュリティ分野における国際連携：取組の例

サイバー空間に関するグローバルな議論

- サイバー空間における国際法の適用・規範の形成と普遍化、我が国の意見表明や情報発信、最先端の知見の共有、信頼醸成、情報共有等を目的として、Ｇ７、ＯＥＣＤ、インターネット・ガバナンス・フォーラム、国連サイバー政府専門家会合（GGE）、Meridian（※１）、IWWN（※２）、サイバー空間に関する国際会議（ロンドン・プロセス）、ＡＲＦ（※３）等に参加

※１　重要インフラ防護に関する国際連携を推進する場として2005年に英国で始まった会合。我が国の他、欧米やアジアの各国の政府職員が参加し、重要インフラ　防護に関するベストプラクティスの交換や国際連携の方策等について議論

※２　2004年に米国土安全保障省と独連邦内務省の主導により創設された枠組。サイバー空間の脆弱性、脅威、攻撃に対応する国際的取組を促進することを目的とする。先進各国のサイバーセキュリティ担当機関及び国を代表するCSIRT（インシデント対処を行う部門）が参加

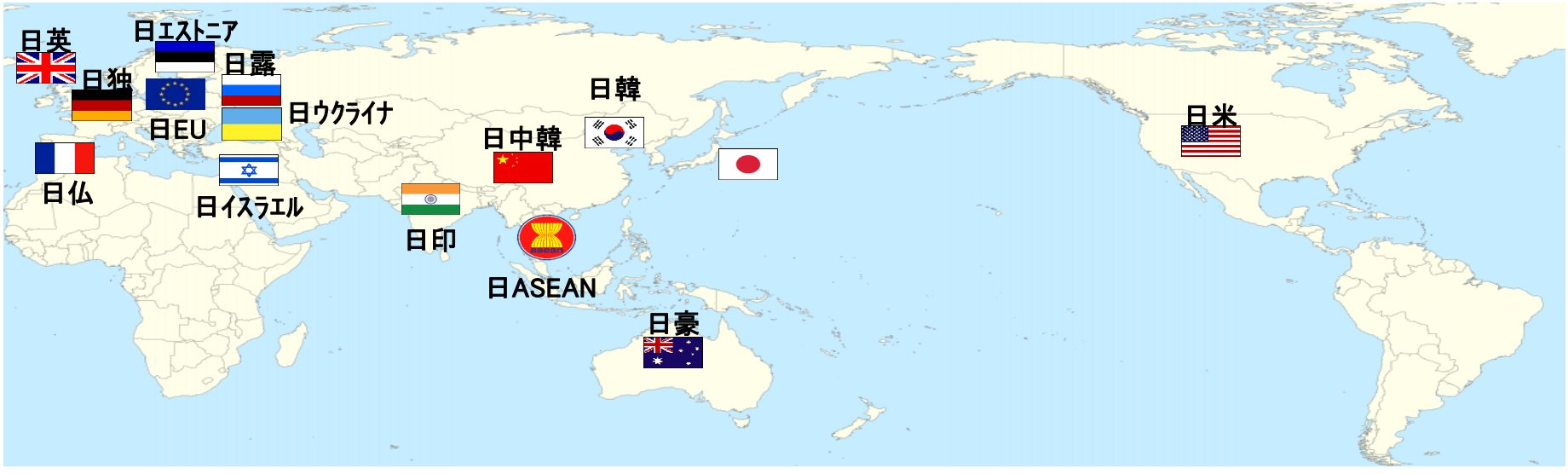
※３　我が国が、2017年にマレーシア・シンガポールと共に立ち上げた「サイバーセキュリティに関するＡＲＦ会期間会合」において、アジア・太平洋地域のサイバーセキュリティに関する安全保障環境を向上させるため、ASEAN地域フォーラムを通じた信頼醸成に取り組んでいる。

二国間協議

- 各国との知見の共有・政策調整を目的として、英国、インド、米国、EU、中韓、イスラエル、仏、エストニア、豪州、ロシア、独、韓及びウクライナとの間でサイバー協議を実施。各国との間で年1回程度の頻度でサイバー空間に関する政府横断的な政策協議を継続的に実施。我が国のサイバーセキュリティ政策を紹介しつつ、具体的トピックを議論

能力構築支援

- セキュリティマネジメント体制の確立、維持、改善などを目的として日ASEANサイバーセキュリティ政策会議等を実施

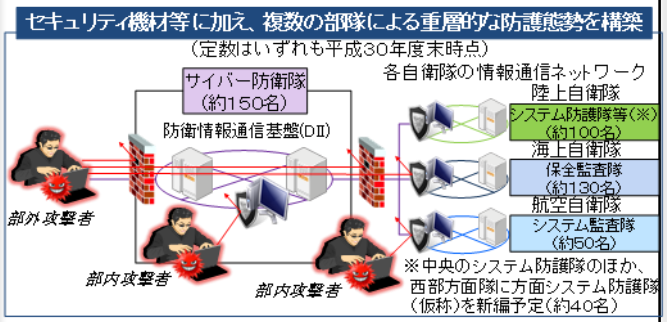


（参考②）我が国の防御力・抑止力・状況把握力の強化：取組の例

サイバー攻撃から我が国の安全保障上の利益を守るため、サイバー攻撃に対する国家の強靭性を確保し、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）のそれぞれを高める。

国家の強靭性の確保

＜防衛省＞
・サイバー攻撃対処を行う部隊の能力の向上、自らの活動が依存するネットワーク・インフラの防護の強化、自衛隊の任務保証に関係する主体との連携の深化

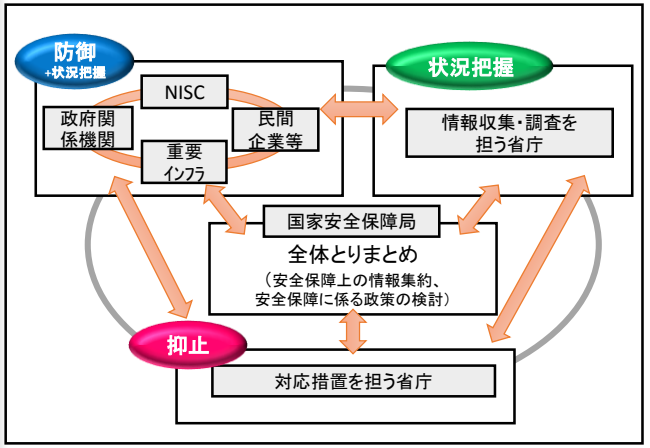


・調達する情報システムに係る情報セキュリティ上のサプライチェーンリスク対策として、調達仕様書に係る関連規則の整備を行う。

サイバー攻撃に対する抑止力の向上

＜内閣官房、関係省庁＞
・同盟国・有志国と連携し、政治・経済・技術・法律・外交その他の取り得るすべての有効な手段と能力を活用し、断固たる対応をとる。

・内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進



＜内閣官房、外務省、関係省庁＞
・ARFや二国間協議等において、政策の共有や連絡体制の構築等を通じた信頼醸成

サイバー空間の状況把握力の強化

＜内閣官房、外務省、警察庁、法務省＞
・諸外国関係機関との情報交換等国際的な連携を通じた、サイバー攻撃に関する情報収集・分析

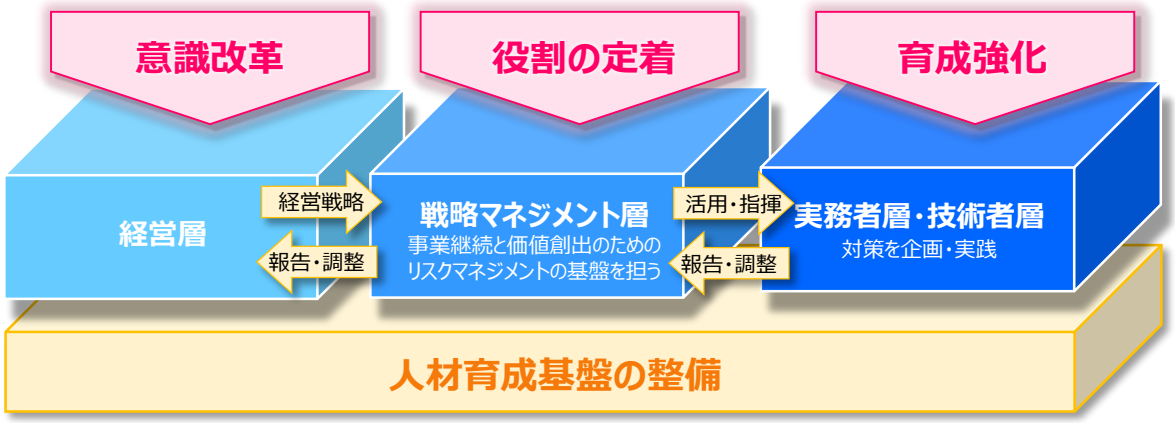
＜警察庁＞
・サイバー空間に関する観測機能の強化等によるサイバーフォースセンターの技術力の向上

サイバーセキュリティに関する共通基盤的な取組の推進

サイバーセキュリティを支える基盤的取組として、横断的・中長期的な視点で、人材育成・確保や研究開発に取り組むとともに、
サイバー空間で活動する主体としての国民一人一人が、サイバーセキュリティに取り組むような全員参加による協働を推進

１．人材育成・確保

- 「戦略マネジメント層」の育成・定着
- 実務者層・技術者層の育成
- 人材育成基盤の整備、国際連携の推進
- 各府省庁のセキュリティ人材の確保・育成強化



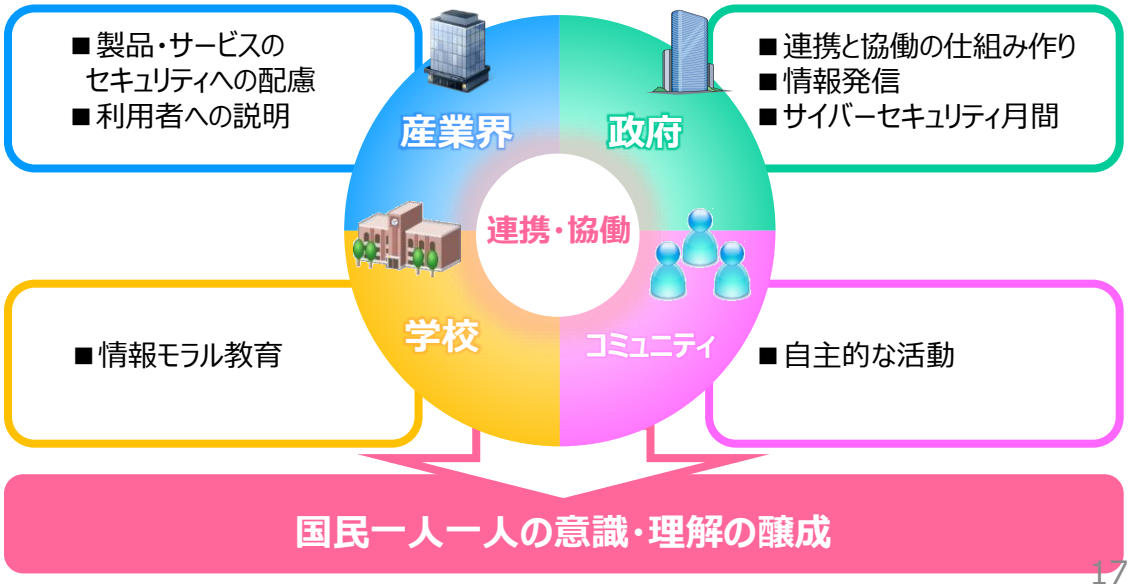
２．研究開発の推進

- 実践的な研究開発の推進

  （検知・防御等の能力向上、不正プログラム等の技術的検証を行うための体制整備等）
- 中長期的な技術・社会の進化を視野に入れた対応

３．全員参加による協働

- サイバーセキュリティの普及啓発に向けたアクションプランの策定とそれに基づく連携・協働
- 「サイバーセキュリティ月間」などを通じた情報発信

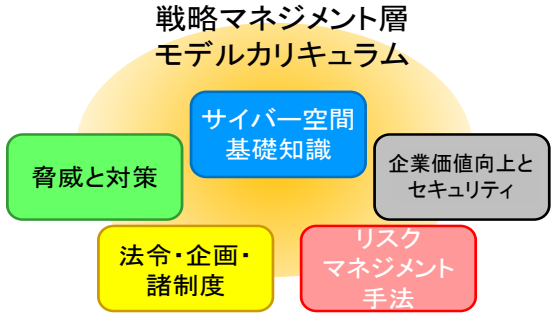


(参考①) 人材育成・確保：取組の例（１／２）

人材の需要と供給を相応するための好循環を形成するため、産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化

「戦略マネジメント層」の育成・定着

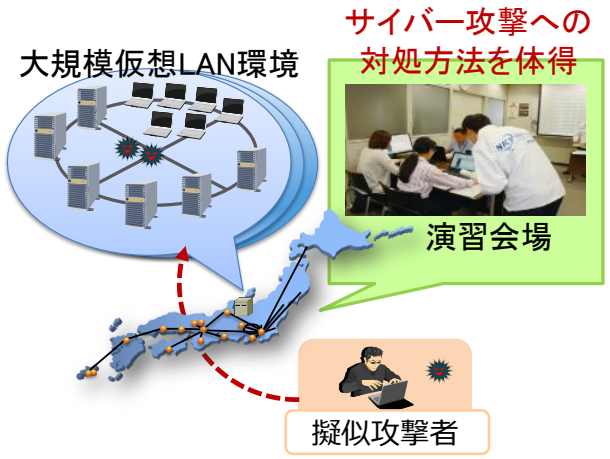
＜内閣官房＞
・戦略マネジメント層育成に向けて、必要な知識・スキルを身に着けるための試行的取組を検討



＜経済産業省＞
・重要インフラ等における実際の制御システム等の安全性・信頼性検証を実施

実務者層・技術者層の育成

＜総務省＞
・NICTに組織した「ナショナルサイバートレーニングセンター」を通じ実践的サイバー防御演習（CYDER）を実施



＜経済産業省＞
・日本ネットワークセキュリティ協会が実施するセキュリティ技術コンテスト「SECCON 2018」の普及・広報支援

人材育成基盤の整備、国際連携の推進

＜文部科学省＞
・新学習指導要領の実施を見据え、発達の段階に応じた情報セキュリティを含めた情報活用能力を培う教育を一層推進する。また、教員等を対象とした研修を実施する。

＜総務省＞
若手セキュリティイノベーター育成プログラム「SecHack365」の実施

SecHack365演習風景

＜内閣官房＞
・人材育成に取り組む大学や公的機関等の研究・教育プログラムに係る基準や諸外国との連携方策について検討

(参考②) 人材育成・確保：取組の例（２／２）

サイバーセキュリティ人材育成総合強化方針（平成28年3月31日 サイバーセキュリティ戦略本部決定）に基づき、各府省庁におけるセキュリティ人材の着実な確保・育成を継続して進めていく。

「各府省庁セキュリティ・IT人材確保・育成計画」に基づく育成

＜内閣官房・各府省庁＞
「サイバーセキュリティ人材育成総合強化方針」に基づき策定した「各府省庁セキュリティ・IT人材確保・育成計画」について、内閣官房の主導によりPDCAサイクルをさらに充実させ、諸施策をより一層推進する。

① 体制の整備・人材の拡充
- セキュリティ・ITに係る体制の整備
- ポストに応じた適切な処遇の確保を実施

② 有為な人材の確保
- 積極的な広報の実施
- 適性が認められる者の採用

③ セキュリティ・IT人材育成支援プログラム
- 研修の積極的受講
- NISC等への出向、大学院等への派遣の推進

各府省庁セキュリティ・IT人材確保・育成計画

④ 人事ルート例（キャリアパスのイメージ）
- 高位のポストまでを見据えた人事ルート例を設定

⑤ 一般職員のリテラシー向上
- 新人研修等でのセキュリティ・IT研修の実施等

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、毎年度計画の**見直し**を実施！

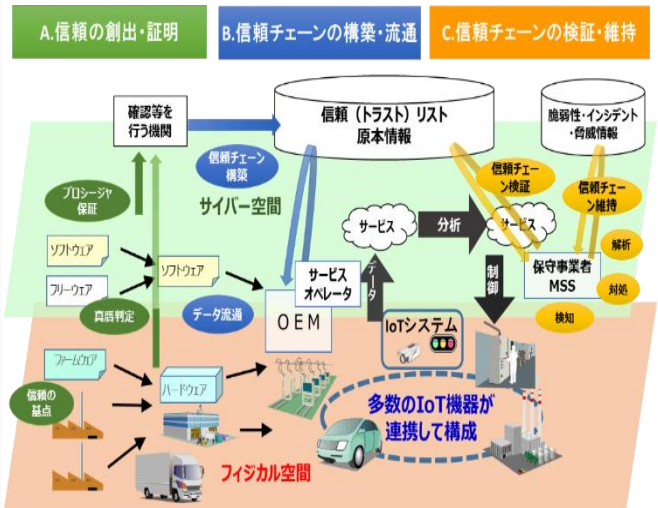
(参考③）研究開発の推進：取組の例（１／２）

・実空間とサイバー空間が一体化していく中、サイバー空間におけるイノベーションの進展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を実施
・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である。

IoT社会に対応したサイバー・フィジカル・セキュリティ

＜内閣府SIP＞

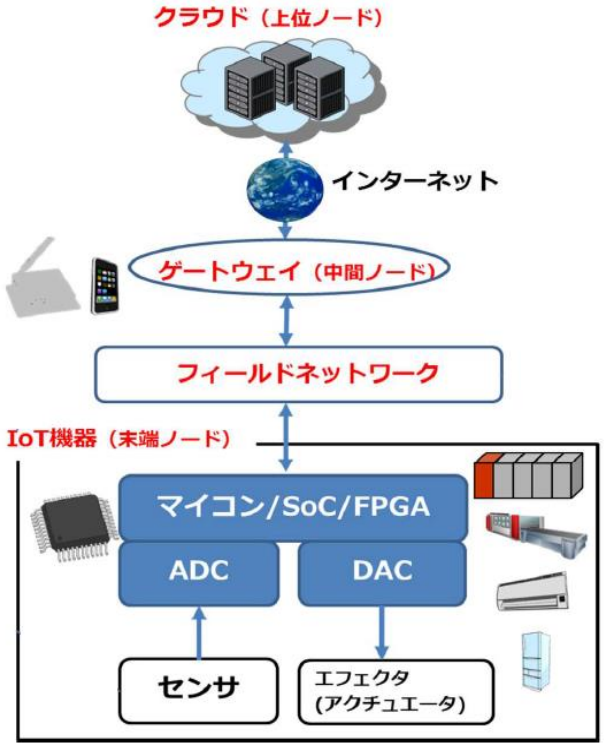
・セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、中小企業を含むサプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及び社会実装を推進。



IoTの安全確保に不可欠なハードウェアセキュリティの確保

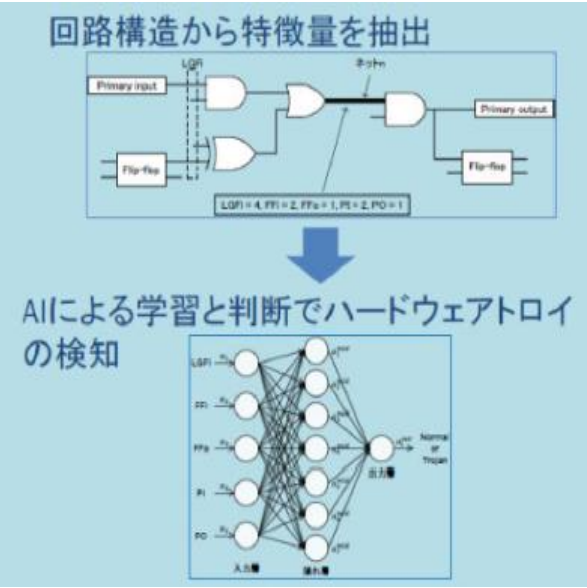
＜経済産業省＞

・高機能暗号や計測セキュリティ、通信制御機器、複製不可能デバイスなどのハードウェアセキュリティ基盤を構築することで、多様なIoT機器からクラウドまでセキュアな環境を実現



＜総務省＞

・IoT機器などのハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発を実施。未知のハードウェアトロイを誤りなく検知することが目標

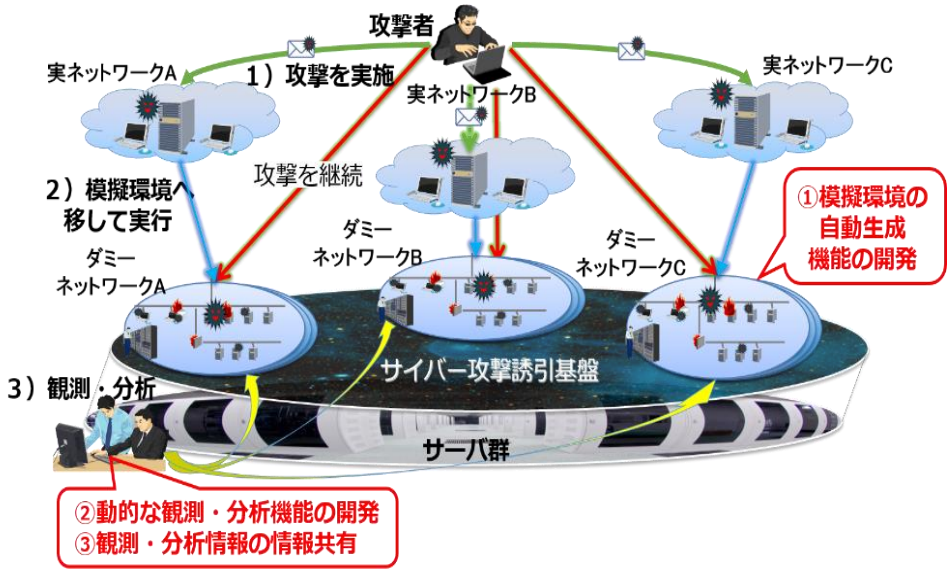


(参考④）研究開発の推進：取組の例（２／２）

サイバー攻撃誘引基盤の構築（STARDUST)

＜総務省＞

・高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能とする高度なサイバー攻撃誘引基盤を構築



広域ネットワークスキャンの軽量化を目指した研究

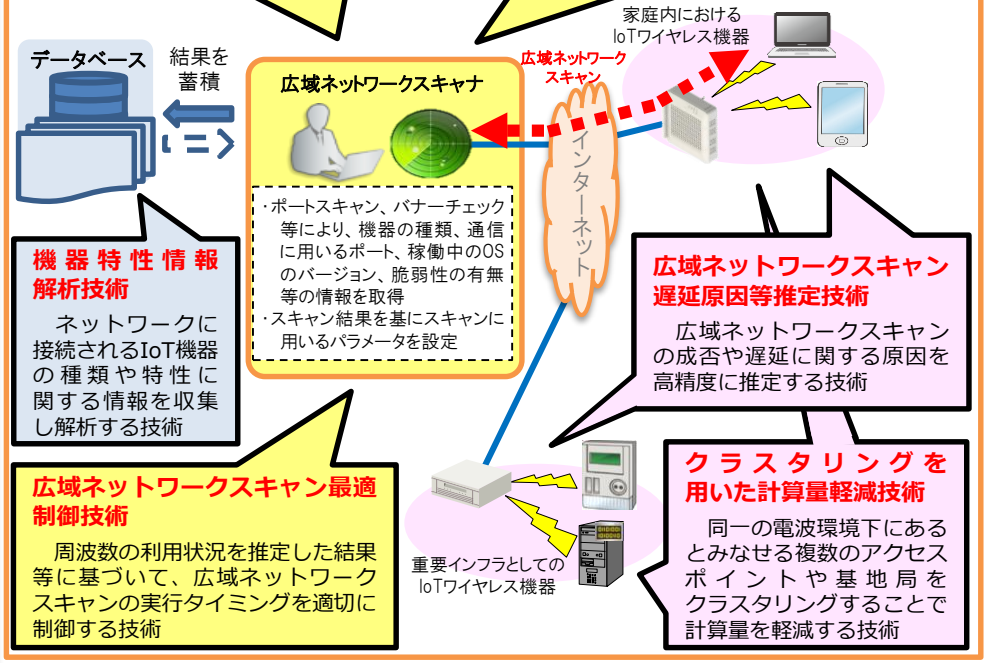
＜総務省＞

・正常な通信を阻害することなく、セキュリティ対策が必要な脆弱なIoT機器を特定することで、安全なICT基盤を実現

広域ネットワークスキャンを実現する要素技術

広域ネットワークスキャン頻度最適化技術
広域ネットワークスキャンの頻度を最適化する技術

広域ネットワークスキャン対象ポート選定技術
広域ネットワークスキャンを実施するポートを選定する技術



機器特性情報解析技術
ネットワークに接続されるIoT機器の種類や特性に関する情報を収集し解析する技術

広域ネットワークスキャン遅延原因等推定技術
広域ネットワークスキャンの成否や遅延に関する原因を高精度に推定する技術

広域ネットワークスキャン最適制御技術
周波数の利用状況を推定した結果等に基づいて、広域ネットワークスキャンの実行タイミングを適切に制御する技術

クラスタリングを用いた計算量軽減技術
同一の電波環境下にあるとみなせる複数のアクセスポイントや基地局をクラスタリングすることで計算量を軽減する技術

（参考⑤）全員参加による協働：取組の例

・サイバーセキュリティに関する国民一人一人の理解を促すための集中期間として、「サイバーセキュリティ月間」のさらなる充実を図る。

・また、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、サイバーセキュリティの普及啓発に向けたアクションプランを策定する。

「サイバーセキュリティ月間」の主な活動

NISC主催の普及啓発イベントの開催

○キックオフサミット@六本木

・各地域で活躍する普及啓発団体の取組紹介や啓発活動に関する課題について議論

・イベントの模様をインターネット全国配信。10,000以上のアクセス数を達成

<キックオフサミット>

○アナログハックを目撃せよ！2018@秋葉原

・幅広く国民のサイバーセキュリティに関する意識向上を図るため、官民連携によるイベントを実施。当日は約2,000名が来場


<アナログハックを目撃せよ！2018>

○ NATIONAL 318(CYBER) EKIDEN

・各府省庁対抗による、競技形式のサイバー攻撃対処訓練を実施

官民等による月間関連行事の開催

○30年度は全国で官民による計189件の関連行事を実施（29年度は155件）

○各府省庁の協力を得て、①重要インフラ、②中小企業等、③国民全般の分野における取組を拡大

【主な取組例】

○「金融ISACワークショップ」（約250名）

○「医療・介護　総合EXPO・メディカルジャパン大阪　医療ITソリューション展セミナー講演」（約300名）

○ 「SIP次世代農林水産業創造技術 生産システムフォーラム」（約300名）

著名な作品とのタイアップ

・サイバーセキュリティと親和性の高いTVアニメ『BEATLESS』とタイアップ

・ポスター配布、ウェブバナーを関係機関のウェブページに掲載

「情報セキュリティハンドブック」の普及

・サイバーセキュリティに関する基本的知識を分かりやすく紹介

・無料電子書籍に加え、スマホ・タブレット端末用の無料アプリを配信

推進体制のポイント

○ サイバーセキュリティの確保を通じて、情報通信技術及びデータの利活用を促進し、経済・社会活動の基盤とすること、我が国の安全保障を万全のものとすることは、従来からの方針。サイバーセキュリティ戦略本部の事務局であるNISCを中心に関係機関の一層の能力強化を図るとともに、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。

○ 各府省庁の施策が着実かつ効果的に実施されるよう、必要な予算の確保と執行を図る。別紙の担当府省一覧を含む各年度の年次計画を作成する。

（別紙）新戦略に基づく施策例及び担当府省庁一覧（サイバーセキュリティ2018）①

項目	担当府省庁 （◎：主担当、○：関係府省庁）	施策例
4.1. 経済社会の活力の向上及び持続的発展		
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		
(1) 経営層の意識改革	◎：NISC、経済産業省 ○：金融庁	・官民の連携による、経営層に説明や議論ができる人材の発掘・育成、経営層向けセミナー等の開催【NISC】
(2) サイバーセキュリティに対する投資の推進	◎：総務省、経済産業省	・サイバーセキュリティ保険の普及、情報開示・共有を促進するためのモデル事業の検討【総務省及び経済産業省】
(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	◎：経済産業省 ○：総務省	・セキュリティ製品・サービスの有効性検証、レーティングを実施できる環境整備の検討【経済産業省】
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		
(1) サイバーセキュリティ対策指針の策定	◎：経済産業省	・「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定【経済産業省】
(2) サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築	◎：内閣府 ○：総務省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）	・中小企業を含むサプライチェーン全体を守ることに活用できる「サイバー・フィジカル・セキュリティ対策基盤」の研究開発及びその社会実装の推進【内閣府】
(3) 中小企業の取組の促進	◎：NISC、総務省、経済産業省	・中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度「SECURITY ACTION」への登録を促すことによるセキュリティレベル向上の促進【経済産業省】
4.1.3 安全なIoTシステムの構築		
(1) IoTシステムにおけるサイバーセキュリティの体系の整備と国際標準化	◎：NISC、総務省、経済産業省	・「IoTセキュリティガイドライン」を様々な産業分野の標準仕様等への反映に向けた普及、国際的展開に向けた活動【総務省及び経済産業省】
(2) 脆弱性対策に係る体制の整備	◎：NISC、警察庁、総務省、経済産業省	・パスワード設定に不備のある機器の調査、IoT機器に対する脆弱性対策に関する実施体制の整備【総務省】
4.2. 国民が安全で安心して暮らせる社会の実現		
4.2.1 国民・社会を守るための取組		
(1) 安全・安心なサイバー空間の利用環境の構築	◎：NISC、内閣官房、内閣府、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ○：内閣官房、内閣府、宮内庁、警察庁、消費者庁、法務省、外務省、文部科学省、農林水産省、環境省、防衛省 ※内閣官房（◎）：内閣官房副長官補（国土交通、海上保安担当） ※内閣府（◎）：政策統括官（科学技術・イノベーション担当）	・ソフトウェア等の脆弱性に関する情報を利用者に提供【経済産業省】 ・情報通信ネットワークの変化、新たなサービス提供に伴い社会・経済に生じ得るリスク源の評価、情報通信ネットワークに関連するハードウェア、ソフトウェアの市場動向及び技術開発動向等についての調査【NISC、総務省、経済産業省】 ・仮想通貨交換業者におけるサイバーセキュリティの強化に向け、実効性のある自主規制機能の確立を促進【金融庁】
(2) サイバー犯罪への対策	◎：警察庁、総務省、法務省、経済産業省	・取締り・捜査に必要な専門的知識・技能の習得のための各種研修の実施【警察庁及び法務省】
4.2.2 官民一体となった重要インフラの防護		
(1) 行動計画に基づく主な取組	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ○：内閣官房、警察庁	・第４次行動計画に基づき、リスクマネジメントの推進、安全基準等の改善・浸透、深刻度評価基準、官民の枠を超えた訓練・演習の実施、制御系システムのセキュリティ対策等を推進【NISC及び重要インフラ所管省庁】
(2) 地方公共団体のセキュリティ強化・充実	◎：NISC、内閣府、総務省 ○：内閣官房 ※内閣府：番号制度担当室、個人情報保護委員会	・地方公共団体職員を対象とした集合研修・eラーニングを実施、セキュリティポリシーに関するガイドラインを随時更新【総務省】 ・緊急時対応訓練の支援及びCSIRTの連携組織の設立【総務省】

（別紙）新戦略に基づく施策例及び担当府省庁一覧（サイバーセキュリティ2018）②

項目	担当府省庁 （◎：主担当、○：関係府省庁）	施策例
4.2.3 政府機関等におけるセキュリティ強化・充実		
(1) 情報システムのセキュリティ対策の高度化・可視化	◎：NISC、総務省、厚生労働省、経済産業省	・政府機関情報システムのサイバー攻撃等に関する情報を収集・分析し、分析結果を各政府機関等へ適宜提供【NISC】
(2) クラウド化の推進等による効果的なセキュリティ対策	◎：NISC、内閣官房、総務省、経済産業省 ※内閣官房：情報通信技術（IT）総合戦略室	・政府機関におけるクラウドサービス利用状況の調査及び課題の把握、新たな政府のプライベート・クラウドとしての整備計画の策定【NISC及び総務省】
(3) 先端技術の活用による先取り対応への挑戦	◎：NISC	・サイバー攻撃による高い耐性を有する情報システム基盤の情報技術について、政府機関等での活用可能性を検証【NISC】
(4) 監査を通じたサイバーセキュリティの水準の向上	◎：NISC ○：内閣府、消費者庁、総務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省	・政府機関、独立行政法人等への監査・ペネトレーションテストの実施【内閣官房】
(5) 組織的な対応能力の充実	◎：NISC、総務省 ○：人事院	・政府機関におけるサイバー攻撃に係る対処要員の能力等の強化を図るため、研修や実践的サイバー防御演習(CYDER)を実施【NISC及び総務省】
4.2.4 大学等における安全・安心な教育・研究環境の確保		
(1) 大学等の多様性を踏まえた対策の推進	◎：文部科学省 ○：NISC	・自律的かつ組織的に取り組むべきサイバーセキュリティ対策についての検討、サイバーセキュリティに関するガイドライン等の策定【文部科学省】
(2) 大学等の連携協力による取組の推進	◎：文部科学省	・サイバー攻撃に関する情報や共通課題、事案対応の知見等を共有するための手法を検討【文部科学省】
4.2.5 2020年東京大会とその後を見据えた取組		
(1) 2020年東京大会に向けた態勢の整備	◎：NISC、警察庁	・「サイバーセキュリティ対処調整センター」の構築を推進、横断的リスク評価の実施【NISC】
(2) 未来につながる成果の継承	◎：NISC、警察庁、総務省、法務省	・大会後も各種施策は適用範囲を拡大して引き続き推進し、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、以降の我が国の持続的なサイバーセキュリティの強化のために活用【NISC】
4.2.6 従来の枠を超えた情報共有・連携体制の構築	◎：NISC、警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省	・ISACを含む既存の情報共有の推進【NISC及び関係省庁】
(1) 多様な主体の情報共有・連携の推進	◎：NISC	・サイバーセキュリティに関する施策の推進に係る協議を行うための協議会創設に向けた検討【NISC】
(2) 情報共有・連携の新たな段階へ	◎：NISC	・積極的に情報の共有に貢献する参加者が評価される環境整備に向けた検討【NISC】
4.2.7 大規模サイバー攻撃事態等への対処態勢の強化	◎：NISC、内閣官房、内閣府、警察庁、経済産業省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）、内閣府：個人情報保護委員会	・関係府省庁、重要インフラ事業者等と連携した初動対処訓練の実施【内閣官房】

（別紙）新戦略に基づく施策例及び担当府省庁一覧（サイバーセキュリティ2018）③

項目	担当府省庁 （◎：主担当、○：関係府省庁）	施策例
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		
4.3.1 自由、公正かつ安全なサイバー空間の堅持	◎：NISC ○：外務省	・ハイレベルの会談・協議等を通じ、サイバー空間における我が国の利益が達成されるよう、戦略的な取組を推進【NISC】
(1) 自由、公正かつ安全なサイバー空間の理念の発信	◎：NISC、外務省、経済産業省 ○：警察庁、総務省、防衛省	・各二国間協議や多国間協議に参画し、我が国の意見表明や情報発信を実施【NISC及び外務省】
(2) サイバー空間における法の支配の推進	◎：NISC、警察庁、法務省、外務省 ○：総務省、経済産業省、防衛省	・サイバー空間における国際法の適用や国際的なルール・規範作り等に積極的に関与し、我が国の意向を反映させるよう取組を推進【NISC及び外務省】
4.3.2 我が国の防御力・抑止力・状況把握力の強化		
(1) 国家の強靱性の確保	◎：NISC、内閣官房、警察庁、法務省、文部科学省、防衛省 ○：内閣府、総務省、外務省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省 ※内閣官房：内閣情報調査室	・サイバー攻撃対処を行う部隊の能力の向上、自らの活動が依存するネットワーク・インフラの防護の強化、自衛隊の任務保証に関係する主体との連携の深化【防衛省】
(2) サイバー攻撃に対する抑止力の向上	◎：NISC、内閣官房、警察庁、外務省、経済産業省、防衛省 ○：総務省、財務省 ※内閣官房：国家安全保障局	・内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進【内閣官房】
(3) サイバー空間の状況把握の強化	◎：内閣官房、警察庁、法務省、経済産業省、防衛省 ○：NISC、総務省、外務省 ※内閣官房：国家安全保障局、内閣情報調査室	・諸外国関係機関との情報交換等国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を継続的に実施【警察庁及び法務省】
4.3.3 国際協力・連携	◎：NISC ○：その他の府省庁	・各国機関との連携、国際会議への参加、我が国での国際会議の開催等を通じ、我が国の情報セキュリティ人材が海外の優秀な技術者等と研鑽を積む場を増やす取組の実施【NISC】
(1) 知見の共有・政策調整	◎：NISC、警察庁、総務省、外務省、経済産業省、防衛省 ○：法務省	・国際的な会議の場等を活用し、二国間協議に加え、各国とのサイバーセキュリティ分野における関係を強化【NISC及び外務省】
(2) 事故対応等に係る国際連携の強化	◎：NISC、経済産業省 ○：警察庁、外務省	・インシデント対応演習等を通じ、各国との情報共有・インシデント発生時の国外との情報連絡体制を整備【NISC】
(3) 能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省	・ASEAN等における能力構築を政府一体的に支援【NISC及び関係各省】
4.4. 横断的施策		
4.4.1 人材育成・確保	◎：NISC ○：総務省、文部科学省、経済産業省	・人材育成施策について、施策間の連携の強化、横断的かつ継続的に人材育成施策の全体像が把握できるよう「見える化」を推進【NISC】
(1) 戦略マネジメント層の育成・定着	◎：NISC、文部科学省、経済産業省	・戦略マネジメント層育成に向けて、必要な知識・スキルを身に着けるための試行的取組を検討【NISC】
(2) 実務者層・技術者層の育成	◎：警察庁、総務省、文部科学省、厚生労働省、経済産業省、防衛省 ○：NISC	・「ナショナルサイバートレーニングセンター」を通じ実践的サイバー防御演習（CYDER）の実施【総務省】 ・セキュリティ技術コンテスト「SECCON 2018」の普及・広報支援【経済産業省】
(3) 人材育成基盤の整備	◎：総務省、文部科学省、経済産業省	・発達の段階に応じた情報セキュリティを含めた情報活用能力を培う教育の推進、教員等を対象とした研修を実施【文部科学省】
(4) 各府省庁におけるセキュリティ人材の確保・育成の強化	◎：NISC、総務省 ○：その他の府省庁	・体制の整備・人材の拡充、一定の専門性を有する人材の育成等、政府部内のセキュリティ人材の充実に係る諸施策をより一層推進【NISC】
(5) 国際連携の推進	◎：NISC、経済産業省	・人材育成に取り組む大学や公的機関等の研究・教育プログラムに係る基準や諸外国との連携方策について検討【NISC】
4.4.2 研究開発の推進		
(1) 実践的な研究開発の推進	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）	・IoT機器のセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にしたうえでトラストリストを構築・確認する技術等を開発【内閣府】
(2) 中長期的な技術・社会の進化を視野に入れた対応	◎：NISC ○：その他の府省庁	・「サイバーセキュリティ研究開発戦略」について、目下の課題を解決すべく、融合領域の研究動向についての調査等を検討【NISC】
4.4.3 全員参加による協働	◎：NISC、総務省、文部科学省、経済産業省 ○：法務省	・「サイバーセキュリティ月間」をはじめとし、サイバーセキュリティに関する各種イベント等の開催や情報発信等を通じ普及啓発活動を推進【NISC】
5. 推進体制	◎：NISC、内閣官房 ○：総務省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）	・関係機関の一層の能力強化、サイバーセキュリティに関する自律的な取組の促進及び国内外への積極的な情報発信【NISC】