資料１

サイバーセキュリティ戦略（案）・サイバーセキュリティ 2018（案）

資料１－１　サイバーセキュリティ戦略（案）の全体概要

資料１－２　サイバーセキュリティ 2018（案）の全体概要

資料１－３　サイバーセキュリティ戦略（案）・サイバーセキュリティ 2018（案）の概要

資料１－４　「サイバーセキュリティ戦略（案）」等に関する意見募集の結果の概要

資料１－５　「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－６　サイバーセキュリティ戦略（案）

資料１－７　サイバーセキュリティ 2018（案）※

※サイバーセキュリティ戦略が閣議決定された時点から効力を生じるものである。

サイバーセキュリティ戦略（案）の全体概要

資料１－１

中長期的

1　策定の趣旨・背景

１．１．　サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）

１．２．　2015年以降の状況変化（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年東京大会等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

２．１．　サイバー空間がもたらす恩恵

・人工知能（AI）、IoT※1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、既存構造を覆すイノベーションを牽引。**様々な分野で当然に利用**され、人々に豊かさをもたらしている。

２．２．　サイバー空間における脅威の深刻化

・技術等を**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・社会的な損失が生ずる可能性は拡大

※１　Internet of Thingsの略

3　本戦略の目的

３．１．　**基本的な立場の堅持**

（１）基本法の目的（２）基本的な理念（「自由、公正かつ安全なサイバー空間」）（３）基本原則（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）

３．２．　目指すサイバーセキュリティの基本的な在り方

（１）目指す姿（**持続的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**）（２）主な観点（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**）

戦略期間（2018～2021年（3年間））

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

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

＜施策例＞・**経営層の意識改革の促進（「費用」から「投資」へ）**
・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）
・セキュリティ・バイ・デザイン※2に基づくサイバーセキュリティビジネスの強化

※２　システムの企画・設計段階から情報セキュリティの確保を盛り込むこと

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

＜施策例＞・**中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定**

３．安全なIoTシステムの構築

＜施策例＞・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
・**IoT機器の脆弱性対策モデルの構築・国際発信**

等

国民が安全で安心して暮らせる社会の実現

１．国民・社会を守るための取組

＜施策例＞・脅威に対する事前の防御（**積極的サイバー防御**）策の構築
・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

＜施策例＞・安全基準等の改善・浸透（サイバーセキュリティ対策の**関係法令等における保安規制としての位置付け**）
・地方公共団体のセキュリティ強化・充実

３．政府機関等におけるセキュリティ強化・充実

＜施策例＞・**情報システムの状態のリアルタイム管理の強化**
・先端技術の活用による先取り対応への挑戦

４．大学等における安全・安心な教育・研究環境の確保

＜施策例＞・**大学等**の多様性を踏まえた対策の推進

５．2020年東京大会とその後を見据えた取組

＜施策例＞・**サイバーセキュリティ対処調整センターの構築の推進**
・成果のレガシーとしての活用

６．従来の枠を超えた情報共有・連携体制の構築

＜施策例＞・**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の強化

＜施策例＞・**サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化**

等

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堅持

＜施策例＞・**自由、公正かつ安全なサイバー空間**の理念の発信
・サイバー空間における法の支配の推進

２．我が国の防御力・抑止力・状況把握力の強化

＜施策例＞・国家の**強靭性の確保**
（①任務保証、②我が国の先端技術・防衛関連技術の防護、
③サイバー空間を悪用したテロ組織の活動への対策）
・サイバー攻撃に対する**抑止力の向上**
（①実効的な抑止のための対応、②信頼醸成措置）
・サイバー空間の**状況把握の強化**
（①関係機関の能力向上、②脅威情報連携）

３．国際協力・連携

＜施策例＞・**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

等

横断的施策

人材育成・確保	＜施策例＞**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（**高度人材**含む）、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進
研究開発の推進	＜施策例＞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）、**AI等**中長期的な技術・社会の進化を視野に入れた対応
全員参加による協働	＜施策例＞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、国民への情報発信**（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5　推進体制

本戦略の実現に向け、サイバーセキュリティ戦略本部の下、**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、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。**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。**　等

サイバーセキュリティ2018（案）の全体概要

資料１－２

項目	主な施策例
1. 経済社会の活力の向上及び持続的発展	
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	・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	・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	・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】
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	・「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	・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	・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】
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	・「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	・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】
2. 国民が安全で安心して暮らせる社会の実現	
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	・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	・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】
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	・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	・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※1の連携組織の設立【総務省】
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	・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	・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	・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	・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	・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】
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	・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	・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】
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	・「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	・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】
2.6 従来の枠を超えた情報共有・連携体制の構築	・ISAC※2を含む既存の情報共有の推進【NISCおよび関係省庁】
(1) 多様な主体の情報共有・連携の推進	・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	・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】
2.7 大規模サイバー攻撃事態等への対処態勢の強化	・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】

項目	主な施策例
3. 国際社会の平和・安定及び我が国の安全保障への寄与	
3.1 自由、公正かつ安全なサイバー空間の堅持	・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	・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	・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】
3.2 我が国の防御力・抑止力・状況把握力の強化	
(1) 国家の強靭性の確保	・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	・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	・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、法務省】
3.3 国際協力・連携	・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	・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	・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	・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. 横断的施策	
4.1 人材育成・確保	・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	・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	・「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	・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	・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	・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】
4.2 研究開発の推進	
(1) 実践的な研究開発の推進	・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	・「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】
4.3 全員参加による協働	・「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	・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】

※1 Computer Security Incident Response Teamの略（シーサート）。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。

※2 Information Sharing and Analysis Centerの略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。

サイバーセキュリティ戦略（案）・サイバーセキュリティ2018（案）の概要

資料１－３

- ◆ 新たなサイバーセキュリティ戦略(案)(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（案）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)（案）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

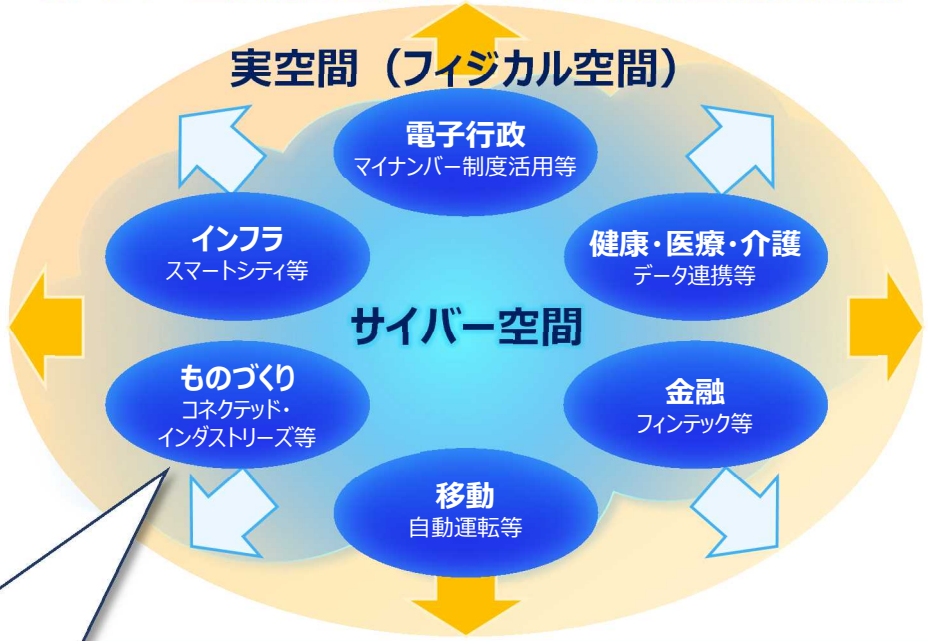
策定の趣旨・背景

【（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

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

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）

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＞

①サービス提供者の任務保証
- 業務・サービスの着実な遂行 -
Mission Assurance

- 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

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–
Cybersecurity Ecosystem

全ての主体が、サイバーセキュリティに関する取組を自律的に行いつつ、相互に影響を及ぼし合いながら、サイバー空間が進化していく姿を、持続的に発展していく一種の生態系にたとえて、「サイバーセキュリティエコシステム」と呼称する。

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

③参加・連携・協働
- 個人・組織による平時からの対策 -
New　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

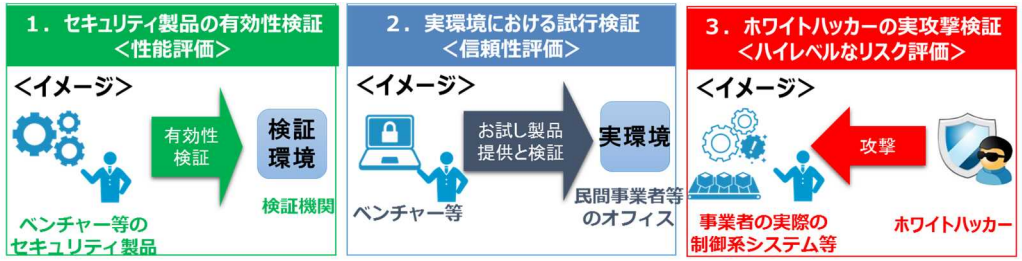
＜内閣官房＞
・官民の連携による、経営層に説明や議論ができる人材の発掘・育成、経営層向けセミナー等の開催

＜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。

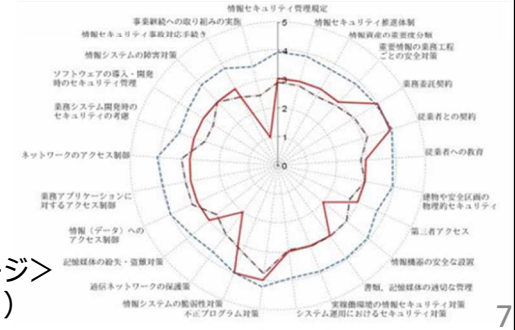
対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度）
		5％ ※ （法人税額の20%を限度）

【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】

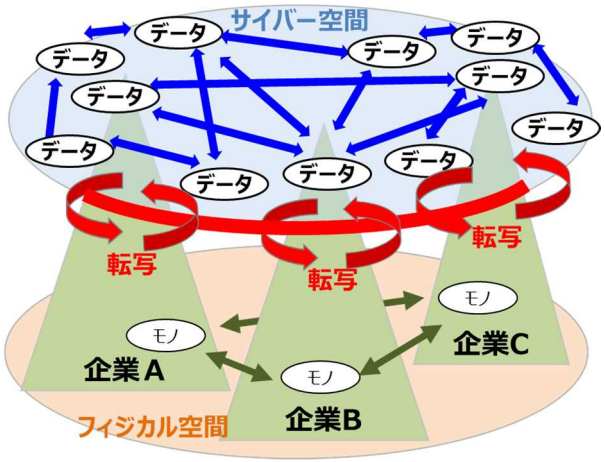
- サービスを創造するためのデータの信頼を確保

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

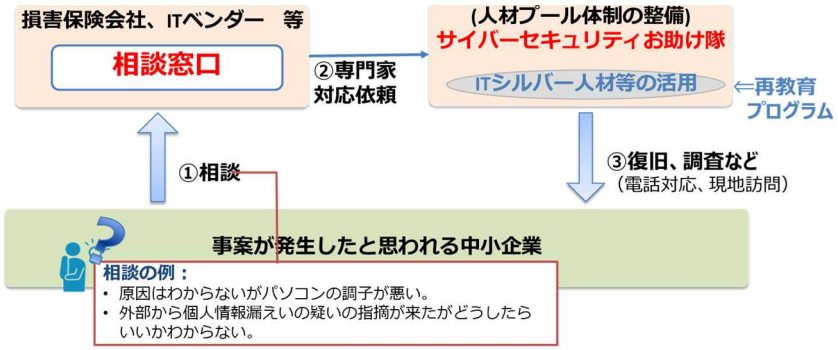
＜経済産業省＞

・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。

■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。

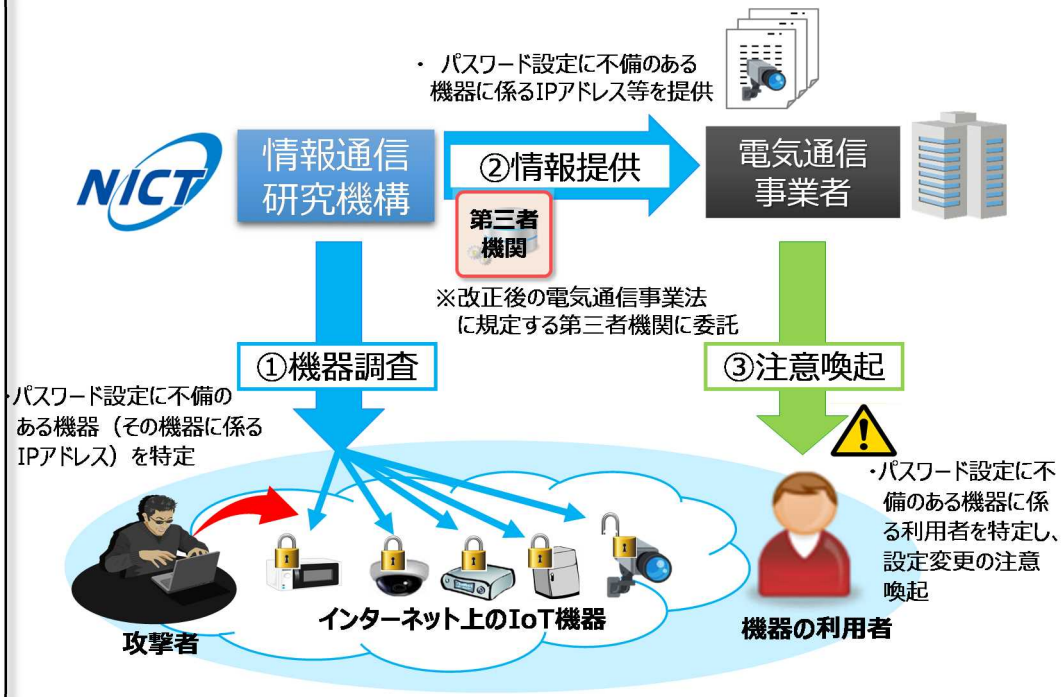
IoTシステムにおけるセキュリティの体系の整備と国際標準化

＜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．大学等における安全・安心な教育・研究環境の確保

- 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

- サイバー空間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）

政府機関等　地方公共団体　重要インフラ事業者　サイバー関連事業者　教育研究機関

リスクマネジメントの推進	安全基準等の改善・浸透	演習・訓練の実施・参加	セキュリティ人材の育成	情報収集・分析

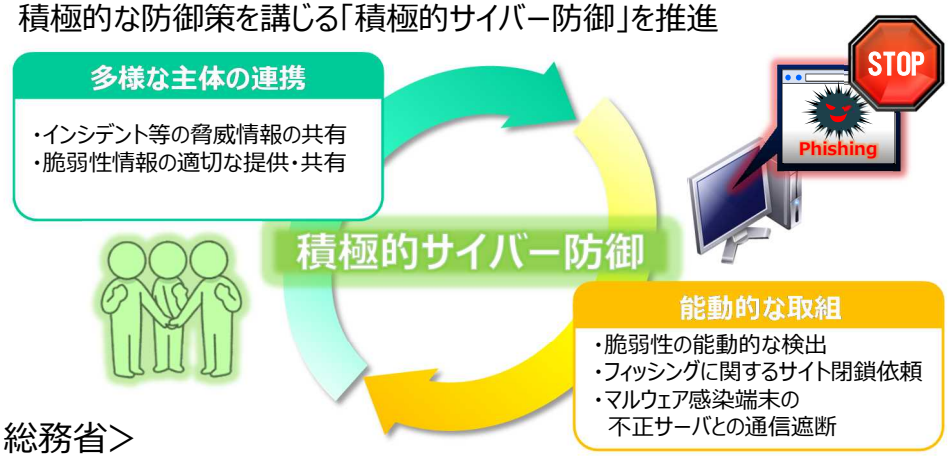
（参考①）国民・社会を守るための取組：取組の例

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

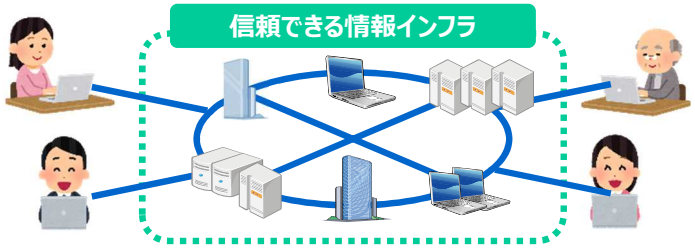


＜総務省＞
・先行的防御を可能にするための脅威情報の共有・活用の促進

＜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＞

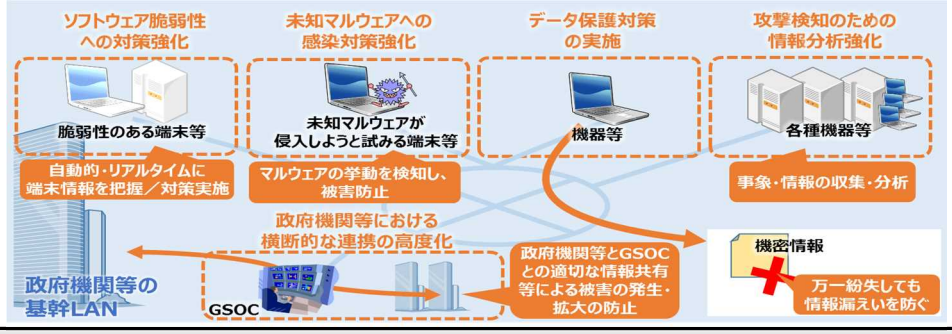
- セキュリティポリシーに関するガイドラインを随時更新
- 地方公共団体職員を対象とした集合研修・eラーニングを実施
- 緊急時対応訓練の支援及びCSIRTの連携組織の設立

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

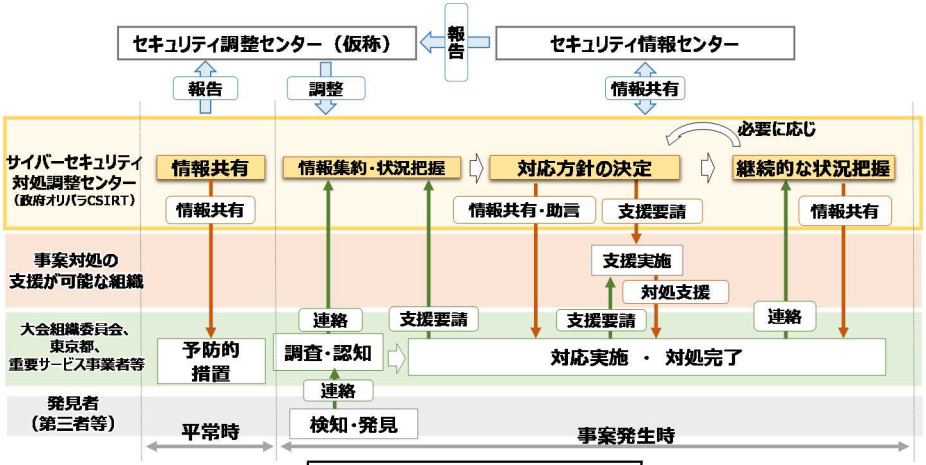
2020年東京大会とその後を見据えた取組

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

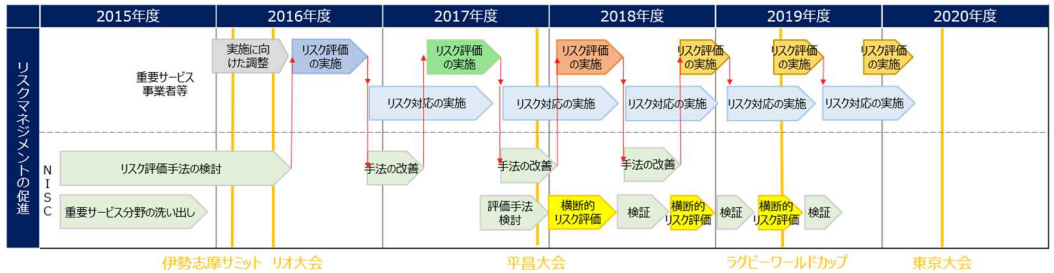
＜内閣官房＞

・「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

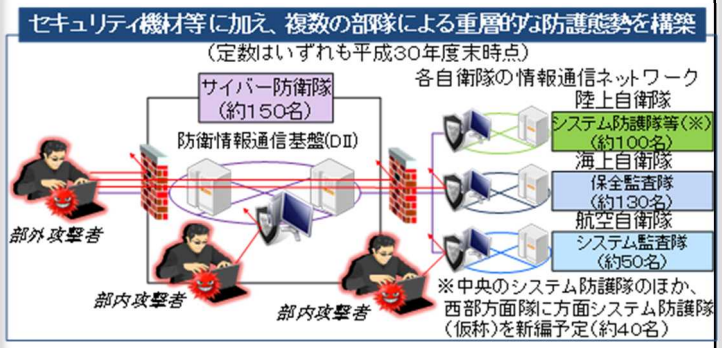
- セキュリティマネジメント体制の確立、維持、改善などを目的として日ASEANサイバーセキュリティ政策会議等を実施

（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

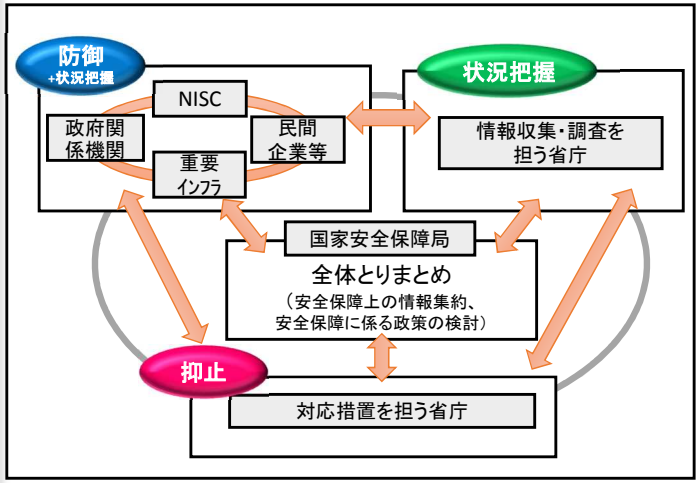


・調達する情報システムに係る情報セキュリティ上のサプライチェーンリスク対策として、調達仕様書に係る関連規則の整備を行う。

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

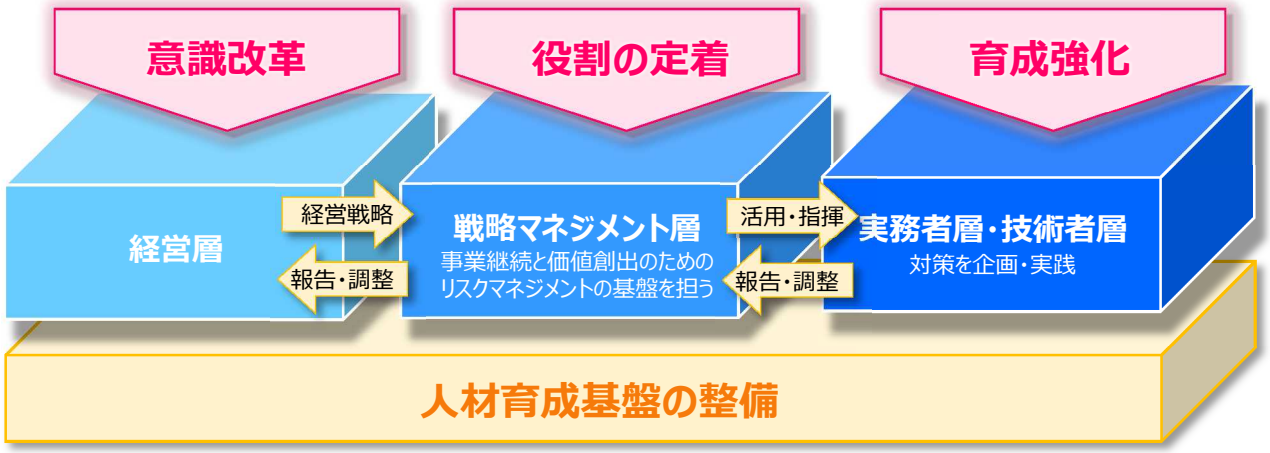
＜警察庁＞
・サイバー空間に関する観測機能の強化等によるサイバーフォースセンターの技術力の向上

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

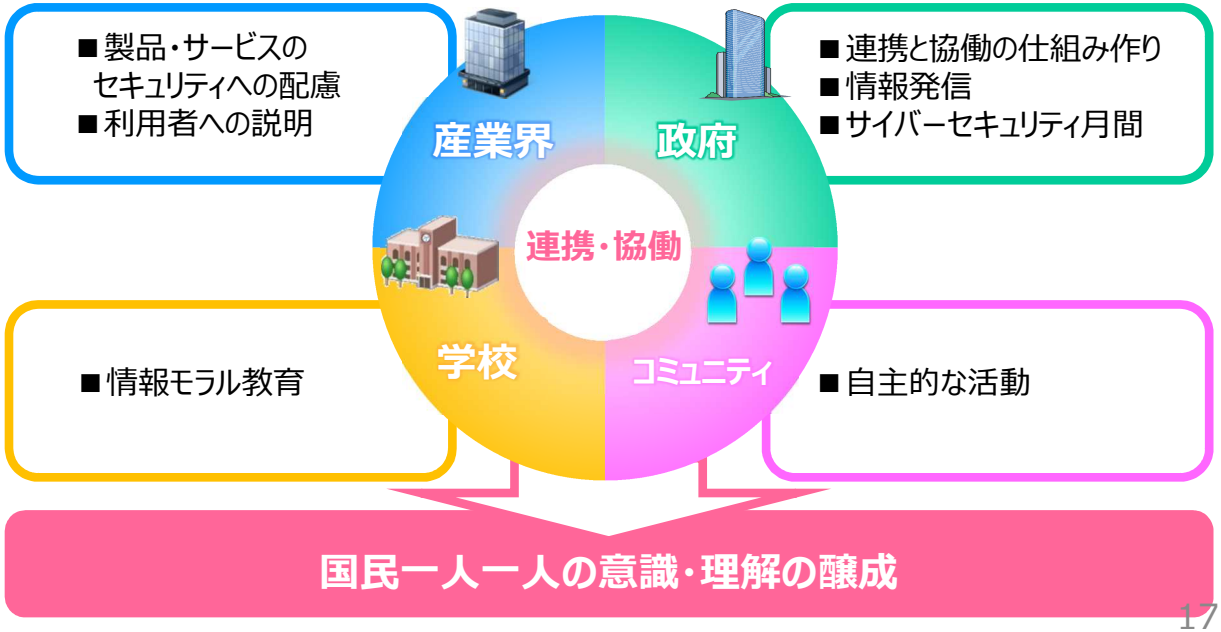


２．研究開発の推進

- 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

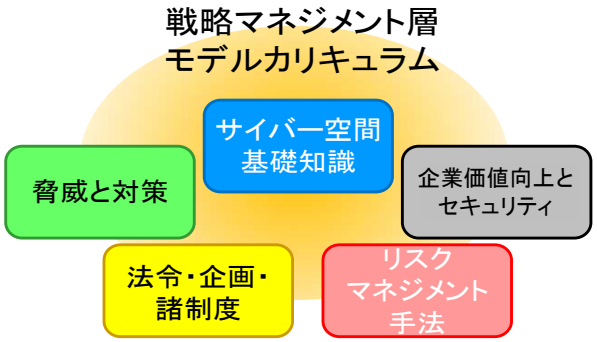


(参考①）人材育成・確保：取組の例（１／２）

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

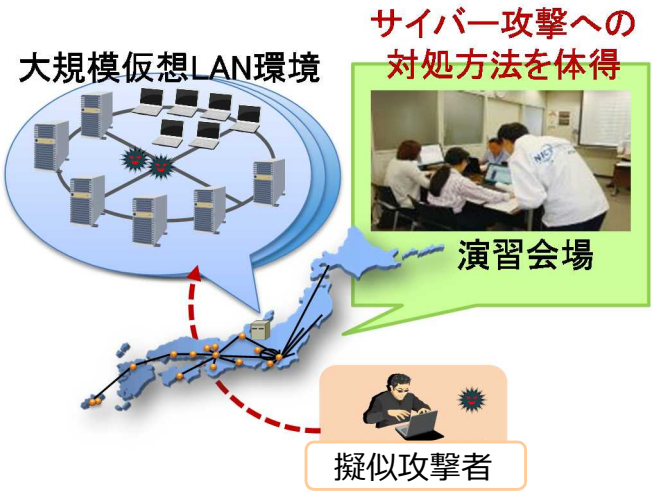
＜内閣官房＞
・戦略マネジメント層育成に向けて、必要な知識・スキルを身に着けるための試行的取組を検討



＜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。

各府省庁セキュリティ・IT人材確保・育成計画

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

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！

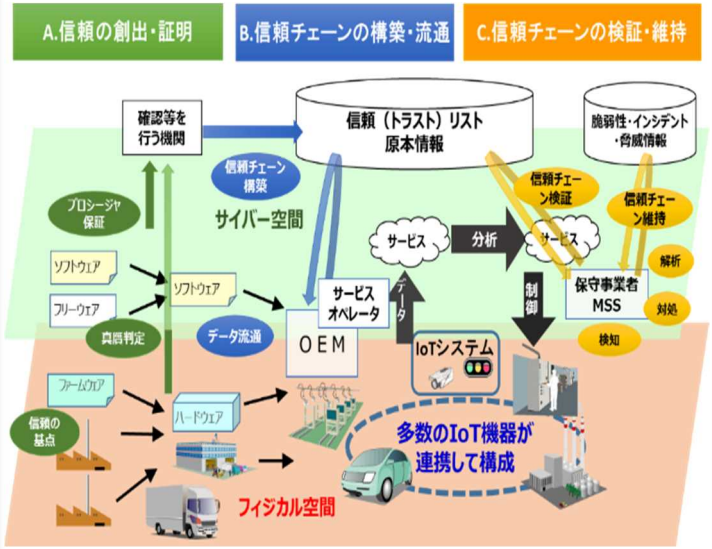
(参考③）研究開発の推進：取組の例（１／２）

・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＞

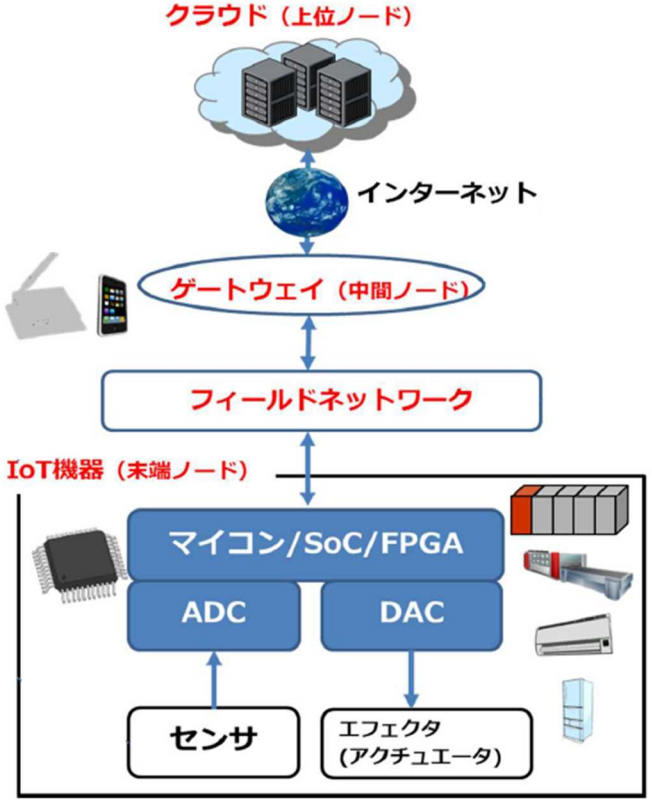
・セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、中小企業を含むサプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及び社会実装を推進。



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

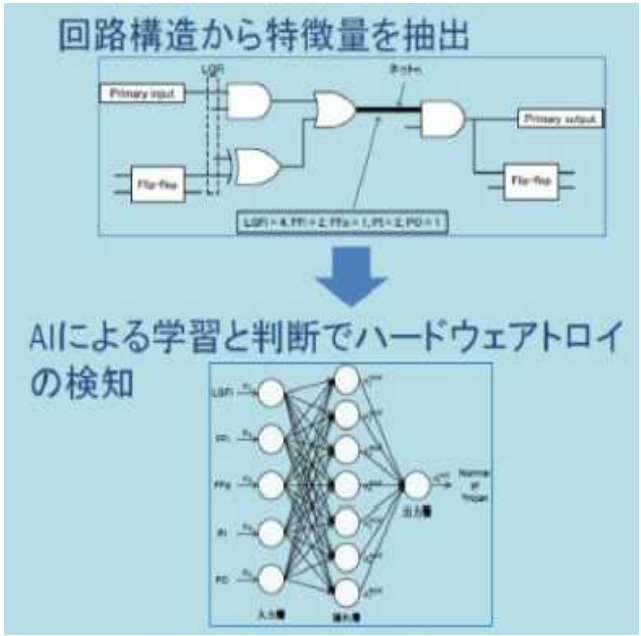
＜経済産業省＞

・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

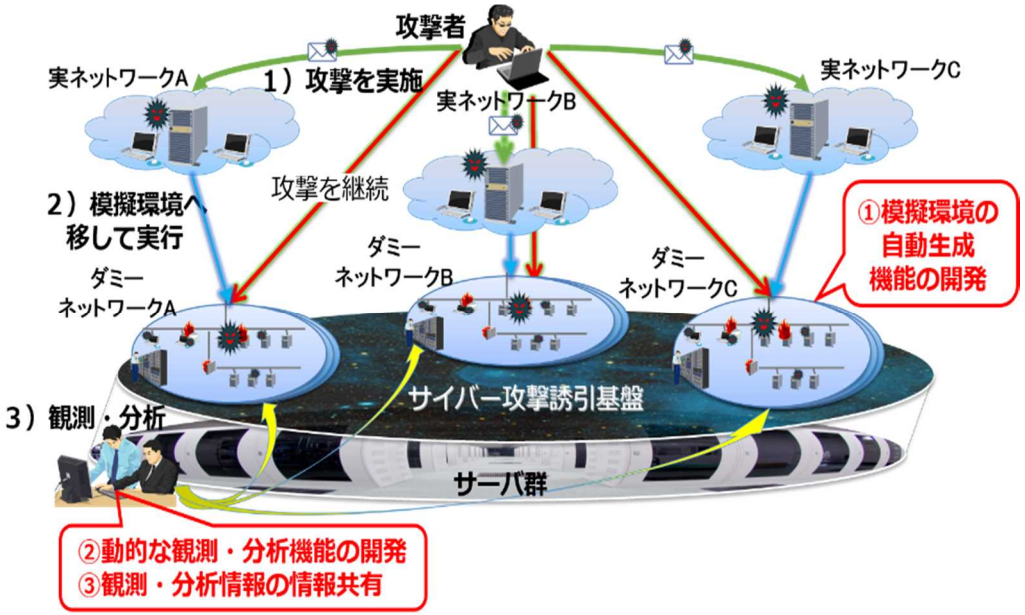


(参考④）研究開発の推進：取組の例（２／２）

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

データベース

結果を蓄積

広域ネットワークスキャナ

・ポートスキャン、バナーチェック等により、機器の種類、通信に用いるポート、稼働中のOSのバージョン、脆弱性の有無等の情報を取得
・スキャン結果を基にスキャンに用いるパラメータを設定

広域ネットワークスキャン

インターネット

家庭内におけるIoTワイヤレス機器

重要インフラとしてのIoTワイヤレス機器

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

情報セキュリティハンドブック NISC

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。

内閣

内閣総理大臣

IT総合戦略本部

高度情報通信
ネットワーク社会の
形成に係る施策を
迅速かつ重点的に推進

連携

サイバーセキュリティ戦略本部

本部長　：内閣官房長官
副本部長：サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　：国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（IT）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣
有識者本部員(7名)

重要インフラ専門調査会	研究開発戦略専門調査会	普及啓発・人材育成専門調査会	サイバーセキュリティ対策推進会議（CISO等連絡会議）

連携

国家安全保障会議（NSC）

我が国の安全保障に関する
重要事項を審議

閣僚が参画

重要インフラ所管省庁

・金融庁
・総務省
・厚生労働省
・経済産業省
・国土交通省

その他関係省庁

・文部科学省（セキュリティ教育）等

協力

事務局

内閣官房　内閣サイバーセキュリティセンター(NISC)

内閣サイバーセキュリティセンター長
副センター長（内閣審議官）

GSOC　CYMAT

協力

閣僚本部員5省庁

・警察庁
・総務省
・外務省
・経済産業省
・防衛省

重要インフラ事業者等　政府機関（各府省庁）　企業　個人

（別紙）新戦略（案）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（案）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（案）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) 国家の強靭性の確保	◎：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】

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果の概要

資料１－４

■ 実施方法：NISCのWebページ、内閣官房のWebページ、電子政府の総合窓口（e-Gov）に掲載して公募

■ 実施期間：2018年６月７日（木）～６月21日（木）

■ 意見総数：27者から97件【16企業・団体から延べ72件、11個人から延べ25件。】

【意見の種類】

・戦略本文に係る意見：66件

- ・総論（策定の趣旨・背景、サイバー空間に係る認識、本戦略の目的）：13件
- ・経済社会の活力の向上及び持続的発展：10件
- ・国民が安全で安心して暮らせる社会の実現：24件
- ・国際社会の平和・安定及び我が国の安全保障への寄与：7件
- ・横断的施策：9件
- ・推進体制3件

・政策展開（サイバーセキュリティ2018）に係る意見：29件

・その他の意見：2件

■ （参考）提出者名：

株式会社ICS研究所、エムティインターナショナル株式会社、経団連産業技術本部、一般社団法人サイバーリスク情報センター公益財団法人笹川平和財団、在日米国商工会議所、一般社団法人新経済連盟、一般社団法人JPCERTコーディネーションセンター、次世代ICカードシステム研究会、石油化学工業協会、石油連盟、電気事業連合会、一般社団法人日本化学工業協会、特定非営利法人日本セキュリティ監査協会、特定非営利法人日本ネットワークセキュリティ協会、株式会社ラック、個人（11人）

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
1	個人（1）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	プラットフォーム開発について、最も危険なのは賄賂などが未だにある国による開発である。国内ではなく、海外からの攻撃が問題となり、最初から海外視点を置かないと防御は難しい時代に入っているのではないか。	悪意ある主体や国家の関与が疑われる脅威について、本戦略(案)（2.2. サイバー空間における脅威の深刻化）において、「この空間は、場所・時間の制約を受けずに、悪意ある主体を含む全ての者が、新たな情報通信技術を悪用・濫用し、容易に活動できる場である。」、「国家の関与が疑われる大規模な事案も発生している。」と記載しています。 御意見も踏まえ、プラットフォームを含む情報インフラについて、その信頼性が揺らぐ懸念があることを明記することとし、本戦略(案)（2.2. サイバー空間における脅威の深刻化）において、以下のように追記することとします。 「さらに、一部の国が優越的な地位からサイバー空間を管理・統制することにより、情報インフラの信頼性が揺らぐ懸念もある。」
2	個人（2）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	電力および電気通信の重要インフラの業務継続が最も重要であることを記述されたい。	本戦略(案)（4.2.2 官民一体となった重要インフラの防護）に記載されている「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」において、重要インフラ分野の重要性については特に区別しておらず、電力及び電気通信に限らずどの分野も重要であると考えられるため、原案のとおりとします。
3	個人（2）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	サイバー空間は動的な脅威によって動的にリスクが変化する空間であるため、継続的監視に基づくリスクマネジメント（ISO27005）を適用する必要がある。	本戦略(案)（3.2. 目指すサイバーセキュリティの基本的な在り方）において、リスクマネジメントについて、「「リスクについて組織を指揮統制するための調整された活動」と定義」と記載しつつ、脚注37で「国際標準化機構（ISO）の定義」と明記しており、対応しておりますので、原案のとおりとします。
4	個人（2）	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	電磁パルス脅威の記述を追加してほしい。	御指摘の「スーパーEMP兵器等による電磁パルス脅威」が具体的に何を指すのか必ずしも明確ではないと考えられますが、悪意ある主体や国家の関与が疑われる脅威について、本戦略(案)（2.2. サイバー空間における脅威の深刻化）において、「この空間は、場所・時間の制約を受けずに、悪意ある主体を含む全ての者が、新たな情報通信技術を悪用・濫用し、容易に活動できる場である。」、「国家の関与が疑われる大規模な事案も発生している。」と記載しており、原案のとおりとします。
5	次世代ICカードシステム研究会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	サイバー空間を構成するネットワークのセキュリティについては触れられていません。ネットワークセキュリティについて、もっと言及すべきではないか。	本戦略(案)（4.2. 国民が安全で安心して暮らせる社会の実現）において、「政府機関や重要インフラ事業者等が提供するサービスの全体の基盤となる信頼できる情報インフラ」について記載しております。 御意見も踏まえ、この記載の前提となる認識として、同（2.2. サイバー空間における脅威の深刻化）においても、ネットワークセキュリティを含む情報インフラについて、その信頼性が揺らぐ懸念があることを明記することとし、以下のように追記することとします。 「さらに、一部の国が優越的な地位からサイバー空間を管理・統制することにより、情報インフラの信頼性が揺らぐ懸念もある。」
6	次世代ICカードシステム研究会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	秘匿性，完全性に係る社会への影響は多く記載されているものの，可用性といった今後のあるべきインフラについて十分な記載がありません。そのため，今後のサイバー空間の前提である環境のあるべき姿についても言及すべきではないか。 例えば，「2．2－（1）」の障害について，爆発的な利用によるインフラの飽和といったことも考えられるのではないか。	本戦略(案)（3.2. 目指すサイバーセキュリティの基本的な在り方）において、「信頼できるサイバー空間が自律的・持続的に進化・発展することを目指す」と記載しており、この記載は、「可用性といった今後のあるべきインフラ」についても包含しているため、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料1－5

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
7	特定非営利法人日本セキュリティ監査協会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	法の支配に関し、「また、同様に、この空間では、既存の国際法が適用される。今後、サイバー空間が安全で信頼できる空間として持続的に発展していくためには、引き続き、既存の国際法の適用、規範の形成が不可欠である。」の部分について、サイバー空間に適用できる国際法はないとの諸説もあることから、「国際間においても、既存の国際法の枠組みの適用に加えて、より安全なサイバー空間形成のための規範の形成が不可欠である。」と修文すべき。	我が国は、サイバー空間にも既存の国際法が適用されるという立場を取っています。本戦略(案)（3.1. 基本的な立場の堅持）において、「引き続き、既存の国際法の適用、規範の形成が不可欠である。」と記載しており、御指摘の「より安全なサイバー空間形成のための規範の形成」についても包含していると考えられるため、原案のとおりとします。
8	特定非営利法人日本セキュリティ監査協会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	「サイバーセキュリティエコシステム」という言葉は、他の箇所で使用しない場合、該当の一文は削除した方がよい。	「サイバーセキュリティエコシステム」は、本戦略（案）（3.2.目指すサイバーセキュリティの基本的な在り方）に記載している「生物における免疫系のように、全ての主体が、サイバーセキュリティについて自らの役割を認識し、サイバーセキュリティに関する取組を自律的に行うこと」を象徴する用語であるため、原案のとおりとします。
9	特定非営利法人日本セキュリティ監査協会	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	バングラディシュ中央銀行がハッキングを受け、約 8,100万ドルが不正送金。 ⇒「が不正送金」を「の不正送金」へ変更し、読みやすくすることを提案します。	御意見を踏まえ、以下のように修文することとします。 「バングラディシュ中央銀行がハッキングを受け、約8,100万ドルが不正送金された事案」
10	公益財団法人笹川平和財団	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	基本法第2条では、サイバーセキュリティを「電磁的方法によって取り扱われる情報の漏洩等の安全管理に必要な措置ならびに情報システム及び情報ネットワークの安全性・信頼性の確保」と定義しているが、多様な主体の連携のため、国際的なサイバー空間の認識の動向を踏まえ、今後「サイバーセキュリティ」の対象は実空間も含むものとして幅広く考えていく必要がある。」	サイバー空間と実空間の一体化の進展を踏まえ、本戦略(案)（3.2.目指すサイバーセキュリティの基本的な在り方）において、「全ての主体が、サイバーセキュリティについて自らの役割を認識し、サイバーセキュリティに関する取組を自律的に行うことが求められる。」、「皆が力を合わせて取り組むこと、すなわち協働が求められる。」と記載しており、サイバーセキュリティに関する取組を幅広く進めることとしているため、原案のとおりとします。御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
11	株式会社ラック	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	「サイバーセキュリティ戦略（案）」の趣旨等について、賛同いたします。	賛同意見として承りました。
12	経団連産業技術本部	1～3（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	政策展開（サイバーセキュリティ2018）に係る意見	経団連がこれまでの提言等において主張してきた重要事項の多くが盛り込まれており、全体として高く評価できる。	賛同意見として承りました。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
13	電気事業連合会	１～３（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	下記のとおり修正してはどうか。 【修正案】 3.2. (2)3つの観点 ①サービス提供者の任務保証 …すなわち、これは、サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供、万が一の事態における事業継続や緊急時対応に関する責任を全うするという考え方である。 【理由】 「安全かつ持続的な提供に関する責任」だけでなく、万が一の事象も起こりうるとの前提の下で、緊急時の早期・適切な対応といった趣旨を織り込むべきではないか。	本戦略(案)（3.2. 目指すサイバーセキュリティの基本的な在り方）において記載している「安全かつ持続的な提供」は、御指摘の「万が一の事態における事業継続や緊急時対応」を包含すると考えられ、また、「4.2.2(1)① リスクマネジメントの推進」において、「事業継続計画及び緊急時対応計画を策定することが重要である」と記載をしているため、原案のとおりとします。 御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
14	在日米国商工議会所 (The American Chamber of Commerce in Japan)	１～３（1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的）	戦略本文に係る意見	サイバー空間は容易に国境を超え多大な効果をもたらします。しかしその一方で、サイバーセキュリティ対策は予測がつかない対策を強いられます。したがって、以下の下線部分の文を盛り込むことにより、サイバー空間の拡がりを表すべき。 ⑤ 多様な主体の連携 サイバー空間は、国、地方公共団体、重要インフラ事業者、サイバー関連事業者その他の事業者、教育研究機関、個人などの多様な主体が活動することにより構築される多次元的な世界である。更にはサイバー空間上では国外の利害関係者とも容易につながり、サイバー空間の拡がりを特定することは極めて難しい。	本戦略(案)（1. 策定の趣旨・背景）において、「こうした発展を遂げた空間は、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・データを自由に生成・共有・分析することが可能な場であり、流通する場でもある。（中略）新たな価値を生み出していく可能性がある。」、同（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）において、「サイバー攻撃は容易に国境を越え、（中略）、サイバー空間の安全・安定の確保のためには、（中略）国際協力・連携を進める必要がある。」と記載しています。 このように、御指摘の「サイバー空間上では国外の利害関係者とも容易につながり、サイバー空間の拡がりを特定することは極めて難しい」に対応した記載となっているため、原案のとおりとします。 御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
15	株式会社ICS研究所　代表取締役社長　村上正志	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	戦略本文に係る意見	そのリスクを大きくする脆弱性情報を部品個体単位で即時確認できるトレーサビリティ管理環境を構築しこれを維持する必要がある 重要インフラや製造業や施設設備のHSE（Health, Safety & Environment）を脅かす要因の一つであるサイバーリスクへの対策も投資である。：HSE＆Securityという言葉を追加記入した方が良いセキュリティ認証CSMSの導入やEDSA認証取得の制御製品で制御システム構築することを保険契約条件に入れることを推進して行くとさらに加速すると考えます。それも企業経営では投資になります。	いただいた御意見は、今後の取組の検討や実施の推進に当たって参考とさせていただきます。 なお、以下のとおり本戦略（案）に記載しております。 ・トレーサビリティについては、本戦略（案）（4.1.2(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）において、「トレーサビリティ を確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する」と記載しています。 ・重要インフラ等の安全性については、本戦略（案）（4.2. 国民が安全で安心して暮らせる社会の実現）において、「業務やサービスが安全かつ持続的に提供されるよう、サイバーセキュリティの基本的な在り方で掲げた「任務保証」の考え方に基づく取組を推進していく」と記載しています。 ・サイバーセキュリティ保険については、本戦略（案）（4.1.1(2) サイバーセキュリティに対する投資の推進）において、サイバーセキュリティ対策の実施状況に応じて、適切に保険料が算定される仕組みにより、リスクへの備えに対するコストが明確になっていくため、投資が進めやすくなる可能性があることを踏まえ、「官民が連携してサイバーセキュリティにおける保険の活用を推進するための方策について検討を行う」と記載しています。 ・サイバーセキュリティに関する取組についての情報公開については、本戦略（案）4.1.1(2)（サイバーセキュリティに対する投資の推進）において、「投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくりを進めていく」と記載しています。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
16	個人（2）	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	戦略本文に係る意見	次のように修文されたい。 「その際には、サイバーセキュリティに係るリスクは企業が直面する様々なリスクの1つであるが、動的なリスクであるため、従来の静的なリスクマネジメントに加えて、継続的監視に基づく動的なリスクマネジメントを組み入れていくことが重要である。」	リスクマネジメントについては、本戦略（案）（3.2(2)② リスクマネジメント）において、「リスクの特定・分析・評価という個別の活動を指すのではなく、組織を指揮統制して、組織が有する有限の資源を適切に分配し、リスクに対応していく一連の活動の全体を意味している」としております。 御指摘の「動的なリスクマネジメント」との点についても、その主旨は含まれていると考えていることから、原案のとおりとしますが、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
17	株式会社ラック	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	戦略本文に係る意見	経営そのもののDX対応が喫緊の課題である現状を踏まえ、将来的には、経営層が広くICTに係る専門的知見を有し、ICT利活用「戦略マネジメント」の一環としてサイバーセキュリティを取扱うべきものと考える。 【修文案】 具体的には、経営層は、デジタルトランスフォーメーション（DX）の進展を十分認識し、取締役会等を通じたサイバーセキュリティに関する積極的な関与が期待されるとともに、リスクマネジメントのために必要となるサイバーセキュリティに関する一定の知識・能力を身につけることが求められる。その際、中短期的視点において、経営層に深い技術的な知識やスキルを期待することは必ずしも現実的ではない。このため、経営戦略、事業戦略におけるサイバーセキュリティのリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材（いわゆる「戦略マネジメント層」）を確保することが重要である。	デジタルトランスフォーメーションの進展の観点については、本戦略（案）（4.1.1(1) 経営層の意識改革）の箇所において、「サイバー空間の利用が急速に進展する中、自由であるがゆえに常に脅威が潜んでいるという認識に立って、そのための備えをすることが必須」としており、御指摘の観点も、重要と考えています。 また、将来的に経営層が広くICTに係る専門的知見を有するべきとの点については、現状では、経営層がサイバーセキュリティに関する一定の知識・能力を身につけることが必要ではあるものの、即座に深い技術的な知識やスキルを求めることは現実的ではないと考えているため、原案の記載ぶりとしておりますが、御指摘の点についても今後の取組の検討や実施の推進に当たって参考とさせていただきます。
18	株式会社ラック	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	政策展開（サイバーセキュリティ2018）に係る意見	民間のCIOその他の有為な者の活動について、ベストプラクティスとして共有・参照する取組みを検討いただきたい。	サイバーセキュリティ2018（案）の1.1.(2)サイバーセキュリティに対する投資の推進において、「経済産業省において、「サイバーセキュリティ経営ガイドライン」の実践的な定着を図るために、具体的な対策事例や情報共有活動事例等を示すプラクティスを作成する。また、企業がどの程度サイバーセキュリティ対策を実施するかの目安として活用できる可視化ツールを作成する」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
19	株式会社ラック	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	政策展開（サイバーセキュリティ2018）に係る意見	民間企業等における投資へのインセンティブ付与のため、より一般的・汎用的なサイバーセキュリティ対策に必要なシステム構築、サービス利用等の促進に係る税制優遇措置を講じていただきたい。	サイバーセキュリティ2018（案）の1.1(2)サイバーセキュリティに対する投資の推進において、「総務省及び経済産業省において、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる取組について、それに必要となるシステムやサイバーセキュリティ対策製品等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の活用を促すことで、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する。」との取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。
20	株式会社ラック	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	政策展開（サイバーセキュリティ2018）に係る意見	関係機関による当該「モノやサービス等」の先導的な導入を促進する仕組みについて検討いただきたい。	サイバーセキュリティ2018（案）の2.3(3)先端技術の活用による先取り対応への挑戦において、「内閣官房において、近年普及してきた情報システムの基盤の中でサイバー攻撃による高い耐性を有するものについて、これらの情報技術を、政府機関等において活用できる可能性について検証する」との取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。
21	特定非営利法人日本セキュリティ監査協会	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	政策展開（サイバーセキュリティ2018）に係る意見	研究開発に当たっては、サイバーセキュリティ人材のひっ迫等を考慮し、サイバーセキュリティに関する知見の蓄積及び利活用或いは次世代への継承を狙いとする自動化等の技術開発も視野に入れる。	サイバーセキュリティ2018（案）の4.2.(1)実践的な研究開発の推進では、例えば「文部科学省において、理化学研究所革新知能統合研究センター（AIPセンター）を通じ、革新的な人工知能基盤技術の構築と、サイバーセキュリティを含む社会的課題の解決に向けた応用研究等を進めていく」等の取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
22	経団連産業技術本部	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	政策展開（サイバーセキュリティ2018）に係る意見	ヒト・情報・技術・カネといったサイバーセキュリティ対策強化に必須のリソースを確保することが重要である。	賛同意見として承りました。 御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
23	日本ネットワークセキュリティ協会	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	政策展開（サイバーセキュリティ2018）に係る意見	投資促進のためにも、有価証券報告書でのリスク記載を義務化するなどの施策も、税制優遇などと合わせて施策として組み入れていただきたい。	サイバーセキュリティ2018（案）の1.1(1)経営層の意識改革において、「経済産業省において、取締役会のサイバーセキュリティへの関与を促すとともに、投資家に対するサイバーセキュリティの啓発を行う観点から、上場企業において行われる「取締役会の実効性評価」の評価項目について、サイバーセキュリティへの経営層の関与をその評価項目として組み込むことを促進する」との取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。
24	在日米国商工議会所（The American Chamber of Commerce in Japan）	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	政策展開（サイバーセキュリティ2018）に係る意見	セキュリティ・バイ・デザインによって、日本のモノやサービスの信頼性向上や海外展開の推進に寄与することとなると考えます。 国際競争の高まりや真正性や信頼性の検証が困難になるという理由のもとに、国外製品が排除されたり、または不当に扱われたりすることのないよう御配慮を要望します。	賛同意見として承りました。 内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
25	個人（3）	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	戦略本文に係る意見	市場の評価を受けて経営者を規律付けするために有価証券報告書等の開示情報を充実させることが適当である。	本戦略（案）（4.1.1(2) サイバーセキュリティに対する投資の推進）において、「投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくりを進めていく」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
26	個人（3）	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	戦略本文に係る意見	CEO後継者に求める素養として、サイバーセキュリティに関するナレッジや経験を例示するなどの方策が考えられる。	本戦略（案）（4.1.1(2) サイバーセキュリティに対する投資の推進）において、「投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくりを進めていく」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
27	個人（4）	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	政策展開（サイバーセキュリティ2018）に係る意見	中小企業の取組の促進に関して、サイバーセキュリティ相談窓口の設置、情報処理安全確保支援士等のインシデント発生時の専門家派遣制度の活用を盛り込み、インシデントに対応出来る環境を整備すべき	サイバーセキュリティ2018（案）の1.1(2)サイバーセキュリティに対する投資の推進において、「経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る」との取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。
28	特定非営利法人日本セキュリティ監査協会	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	戦略本文に係る意見	常用漢字外なので「拡がる」を「広がる」に修正した方がいいのではないか	御指摘を踏まえ、「サプライチェーンがグローバルに広がる中で」と修正することとします。
29	特定非営利法人日本セキュリティ監査協会	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	戦略本文に係る意見	(3)中小企業の取組の促進の第一文の根拠が不明確なので、 「大企業に比較して経営基盤が脆い中小企業の場合、サイバー攻撃による金銭的な損害や信用の低下による経営的打撃から回復することができにくい。」と修文してはどうか。	本戦略（案）の策定に当たっては「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」（平成30年5月31日）の内容を反映しているところ、同報告書（P23）において、より詳細に「中小企業は、大企業に比べて経営基盤が必ずしも盤石ではないため、サイバー攻撃により、金銭的な損害や信用の低下を招いてしまった場合、経営に与えるインパクトが極めて大きい」と記載しており、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
30	株式会社ラック	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	戦略本文に係る意見	国民生活の保護等の視点からサプライチェーンの中に中古品取引も含めて考えるべき。 【修文案】 サイバー空間と実空間の一体化が加速的に進展する中、「Society5.0」の実現に向けて、グローバルな規模で、これまで取引がなかった異なる業種の企業間取引が生まれたり、中古品等の個人間取引が急速に拡大したりしている。	多様なつながりの一つの形態に個人間取引も含まれ得るところ、本戦略（案）（4.1.2(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）において、「調達者が機器・サービス等の利用に際し、その信頼を確認できるよう、官民が連携して、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要」としており、ご指摘の「中古品等の個人間取引」の観点についても、その主旨は含まれていると考えていることから、原案のとおりとしますが、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
31	株式会社ラック	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	政策展開（サイバーセキュリティ2018）に係る意見	中古品のリスクについて国民に対して広く普及・啓蒙する取り組みを進めていただきたい。	いただいた御意見は、今後の取組の検討や実施の推進に当たって参考とさせていただきます。 なお、サイバーセキュリティ2018（案）の4.3全員参加による協働において、「内閣官房において、行動計画に基づき、NISCが中核的役割を担いつつ、各府省庁や民間の取組主体と協力して、「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進める」との取組を進めています。
32	株式会社ラック	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	政策展開（サイバーセキュリティ2018）に係る意見	Logisticレイヤーにおけるファームウェア書き換え、チップのすり替え等を防止する観点から、デバイスの製造者において、筐体の要所を複製が困難な封印等でシールするような仕組みを検討いただきたい。	いただいた御意見は、今後の取組の検討や実施の推進に当たって参考とさせていただきます。 なお、サイバーセキュリティ2018（案）の1.2.(2)サプライチェーンにおける機器・サービスのサイバーセキュリティを確認できる仕組の構築において、「内閣府において、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、社会全体の安全・安心を確立するため、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を推進する。本プロジェクトでは、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、業務データを安全に流通させるためのトレーサビリティ確保技術、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。」との取組を進めています。
33	在日米国商工議会所（The American Chamber of Commerce in Japan）	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	政策展開（サイバーセキュリティ2018）に係る意見	ブロックチェーン技術をめぐるセキュリティについても考慮に入れた戦略を検討することが経済社会の活力向上に一層資するものと考えます。	本戦略（案）（4.4.2(1) 実践的な研究開発の推進）において、「AI、ブロックチェーンなどの先進的な技術を用いたサイバーセキュリティ確保の技術（中略）について重点的に取り組む」こととしており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
34	エムティインターナショナル株式会社	4．1．3　安全なIoTシステムの構築	戦略本文に係る意見	安全なIoTシステムの構築の原点は、プログラム対策の安全性の担保である。 データ生成の実態確認の為にプログラムテストが必須である。完全なプログラム開発とはコンパイルアップ時点でSyntaxチェックに加えSemanticsチェックも完了していることである。データ生成の完全性を担保するシナリオ関数技術が必須である。	本戦略（案）（4.1.3 安全なIoTシステムの構築）において、「官民が連携して、安全なIoTシステムの構築に取り組む」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
35	次世代ICカードシステム研究会	4．1．3　安全なIoTシステムの構築	戦略本文に係る意見	IoT機器のライフサイクルとして、「提供・購入」，「設定・展開」についても言及すべきではないか。	本戦略（案）（4.1.3(2) 脆弱性対策に係る体制の整備）において、「ライフサイクル」には、いただいた御意見の主旨も含んでおり、例えば具体的な取組の一つである総務省の「IoTセキュリティ総合対策」では、設計・製造、販売(輸入を含む。)、設置、運用・保守、利用の段階に分けて、取組を整理しております。引き続き安全なIoTシステムの構築に向けた検討や実施の推進に当たって参考とさせていただきます。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
36	株式会社ラック	4．1．3　安全なIoTシステムの構築	政策展開（サイバーセキュリティ2018）に係る意見	グローバルなサイバー攻撃等のリスクを回避する観点から、一定の要件が保証されないIoT機器の国内販売を禁ずる措置を検討いただきたい。	サイバーセキュリティ2018（案）の1.3(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、(2) 脆弱性対策に係る体制の整備の取組の中で、必要なサイバーセキュリティの要件を整理し、その要件を満たすIoT機器の利用を推奨することや、国際標準化に向けた取組を推進する等、安全なIoTシステムの構築に向け取組を進めて参ります。
37	株式会社ラック	4．1．3　安全なIoTシステムの構築	政策展開（サイバーセキュリティ2018）に係る意見	サイバー攻撃の情報共有に当たって、ベンダや関係者から開示された情報の取り扱いに十分留意するよう検討いただきたい。	サイバーセキュリティ2018（案）の2.6(1)多様な主体の情報共有・連携の推進において、「国の行政機関、重要インフラ事業者、サイバー関連事業者等官民の多様な主体が相互に連携し、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の創設に向けて検討を進める。」としており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
38	在日米国商工議会所 (The American Chamber of Commerce in Japan)	4．1．3　安全なIoTシステムの構築	政策展開（サイバーセキュリティ2018）に係る意見	日本独自の基準や規制を設定するのではなく、国際標準の採用を推奨する。	賛同意見として承りました。 サイバーセキュリティ2018（案）の1.3.(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の、「安全なIoTシステムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組」に盛り込むこととし、国際標準との整合性を取るべく推進して参ります。
39	個人（2）	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	積極的サイバー防御については、本来、毛沢東によれば攻勢防御であり、「報復の抑止」としてのサイバー攻撃能力を含めた定義にすべきである。	「積極的サイバー防御」は、サイバー攻撃に対して能動的に防御していく取組のことであり、必ずしも「報復の抑止」までを考慮したものではありませんが、御意見として承ります。
40	特定非営利法人日本セキュリティ監査協会	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	下記下線部分の追記を提案します さらに、国民が仮想通貨を…引き続き議論を主導していく。 一方で、2022年の成人年齢の引き下げ等を見据えて、新たな技術に対する国民のサイバーセキュリティリテラシーの向上のため、産学官の連携をより一層強化し、サービスの提供事業者が利用者教育を行うなどの幅広い施策を検討する。	本戦略（案）（4.4.3 全員参加による協働）において、「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」、「サイバーセキュリティについての教育を推進する」と記載しており、原案のとおりとします。
41	株式会社ラック	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	民間事業者等が安心して解析等の業務に従事できるよう、サイバーセキュリティに関する法令解釈を明確化する旨を記述されたい。	「いわゆるコンピュータ・ウイルスに関する罪」については、既に法務省等が考え方を公表しています。サイバーセキュリティをめぐる環境の変化を踏まえると、サイバーセキュリティに関する法令解釈を網羅的に明示することは困難と思われ、前述のとおり既に主なものについては公表されていることから、原案のとおりとします。 一方で、官民連携によるサイバー犯罪対策を推進するためには、研究者や民間事業者等が法令に則った上で安心してサイバーセキュリティ事業に従事できることが重要であるため、官民連携の推進に当たって参考とさせていただきます。
42	日本ネットワークセキュリティ協会	4．2．1　国民・社会を守るための取組	戦略本文に係る意見	サイバーセキュリティ事業従事者逮捕事案等の発生を受け、ICTの利用促進を阻害しない適切な取締りについて記述されたい。	ICTの利用促進を阻害しないという点については、戦略本文（3．本戦略の目的）において、基本的な理念（「自由、公正かつ安全なサイバー空間」を目指す）や基本原則（③開放性、④自律性）として考え方を記載しております。 本戦略（案）は、上記考え方を踏まえた上での取組として記載していることから、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
43	公益財団法人笹川平和財団	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	官民連携の更なる強化が必要であること、 その際、重要インフラ事業者における連絡担当者には、関連資格保有者にセキュリティクリアランスを施した上で充てることが望ましく、また、そのような枠組みによる事業者の負担軽減も必要であるため、4.2.2（1）に⑥として以下の文章を追加すべき。 「⑥官民連携の更なる強化 　サイバー攻撃への迅速な対応を行うため、重要インフラ事業者における連絡担当者の指定（既存の国家資格保持者等を活用）及び重要インフラ事業者から内閣サイバーセキュリティセンターへのインシデントの報告の義務化を検討する。その際、報告の義務化に伴う重要インフラ事業者の負担軽減のため税制優遇等の助成措置についても併せて検討する。」	「官民連携の強化」は重要なポイントであるため、本戦略（案）において様々な個所に記載しております。 インシデント報告を促進することにより官民連携を強化することについては、御意見を踏まえ、同（4.2.6⑵ 情報共有・連携の新たな段階へ）において、以下のように修文することとします。 「サイバーセキュリティインシデント等に係る、自ら保有する情報を積極的に提供する主体が評価される環境を整備していく。」 また、「報告の義務化に伴う重要インフラ事業者の負担軽減のため税制優遇等の助成措置」については、今後の取組の参考とさせていただきます。
44	石油化学工業協会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	「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」でも「相互依存性等を踏まえた重要インフラ事業者等のクラス分け」が示されており、分野ごとに差異があることは理解されている。「サイバーセキュリティに関する意識や取組の進捗に温度差がある」ことを、一概に解決すべき「課題」と決めつけるべきではない。	「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」において、「相互依存性等を踏まえた重要インフラ事業者等のクラス分け」を記載しており、分野ごとの取組について差異があることは御認識のとおりですが、趣旨は、一部の重要インフラ事業者等による先導的取組について、更に強化・推進していくとともに、他の重要インフラ分野に広めていく、ということであり、全体的な底上げを行っていくということです。 したがって、分野ごとの取組について差異があることを課題として捉え、その課題を解決するために全体的なセキュリティレベルの底上げを行っていく、という記載は適切と考えておりますので、原案のとおりとします。
45	石油化学工業協会	4．2．2　官民一体となった重要インフラの防護	政策展開（サイバーセキュリティ2018）に係る意見	「安全等を維持する観点から、サイバーセキュリティ対策を関係法令等における保安規制として位置付けるなど、制度的枠組みを適切に改善していく」との記述がある。 　重要インフラ事業者は「サイバーセキュリティ基本法」に則って自主的に取組んできているところである。法制化の検討に際しては、初めから法制化ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提である。対象となる事業者へのサイバー攻撃による障害の影響の大きさと、これに対応するための事業者の負担に十分に配慮されたい。	「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」に盛り込まれている内容であり、原案のとおりとします。 なお、サイバーセキュリティの完全性・可用性・機密性をどのように位置付けていくかについては、関係法令等の目的によって当然異なりますので、その目的に照らして、妥当な位置付けとなるように考えており、そのような意味で、「適切に改善」していくとしています。
46	個人（5）	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	「4.2.2　官民一体となった重要インフラの防護」項目にて『重要インフラ分野ごとに、サイバーセキュリティに関する意識や取組の進捗に温度差があるという課題がある。』との指摘に賛同する。 「（2）安全基準等の改善・浸透」にて、より具体的に情報セキュリティの国家資格である「情報処理安全確保支援士」を必置とする事を提案する。 重要インフラ事業者について、企業間格差を是正するためにも関係法令等における保安規制として導入することを強く要望し提案する。 「地方公共団体のセキュリティ強化・充実」においても 前述の通り国家資格である「情報処理安全確保支援士」の有資格者の配置を要件として盛り込むことを提案したい。	本戦略（案）は、今後3年程度の基本的な施策の方向性を示したものであり、個別具体的な取組を記載することは考えておりませんが、「情報処理安全確保支援士」に関する提案については、今後の取組の参考とさせていただきます。 また、「関係法令等における保安規制として導入する」ことについては、本戦略（案）（4.2.2⑵② 安全基準等の改善・浸透）において、「安全等を維持する観点から、サイバーセキュリティ対策を関係法令等における保安規制として位置付けるなど、制度的枠組みを適切に改善していく」と記載しています。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
47	石油連盟	4．2．2 官民一体となった重要インフラの防護	戦略本文に係る意見	電力、ガス、石油の3分野以外で制御系システムを利用している分野における当事者意識を高め、関係全分野での対策を推進する目標に鑑み以下の通り修文すべき。 「電力、ガス、石油分野等の重要インフラ事業者の中には、サービス提供のために制御系システムを用いている事業者がある。この制御系システムに不具合が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。」	御意見を踏まえ、「4.2.2(1)⑤ 制御系システムのセキュリティ対策」において、以下のように修文することとします。 「電力、ガス、石油分野等の重要インフラ事業者の中には、サービス提供のために制御系システムを利用している事業者がある。サイバー攻撃等により制御系システムに大きな影響が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。」
48	一般社団法人日本化学工業協会	4．2．2 官民一体となった重要インフラの防護	戦略本文に係る意見	重要インフラサービスを安全かつ持続的に供給する「任務保証」については、同じサービス障害が発生した場合でも重要インフラ分野ごとにその影響は異なる。 サイバーセキュリティに関する全体的な底上げを行う際にも、分野ごとの特性を考慮した対応が必要である。	「分野ごとの特性を考慮した対応」については、本戦略（案）（4.2.2(1)② 安全基準等の改善・浸透）において、「業務の内容、組織の規模、システムの使用期間、国際競争力への影響等を考慮して安全基準等を改善する取組を継続的に推進する。」と記載をしており、既にその要素は盛り込んでいます。
49	電気事業連合会	4．2．2 官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 重要インフラの防護については、「任務保証」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するために、・・・ 【理由】 第4次行動計画では、「『機能保証』とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。」とあり、「機能保証」という表現を「任務保証」という表現に変更する際に、「重要インフラサービスの防護や機能維持を確約することではない」ということは抜け落ちないようにしてもらいたい。 「安全かつ持続的な提供に関する責任」だけでなく、万が一の事象も起こりうるとの前提の下で、緊急時の早期・適切な対応といった趣旨を織り込むべきではないか。	御意見を踏まえ、本戦略（案）（4.2.2 官民一体となった重要インフラの防護）について、以下のように修文することとします。 「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」（以下「行動計画」という。）の5つの施策群に基づいた取組を推進してきた。」
50	電気事業連合会	4．2．2 官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 （注釈部分） 47 「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「重要インフラサービスの防護や機能維持を確約することではなく、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。 【理由】 第4次行動計画では、「『機能保証』とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。」とあり、「機能保証」という表現を「任務保証」という表現に変更する際に、「重要インフラサービスの防護や機能維持を確約することではない」ということは抜け落ちないようにしてもらいたい。 「安全かつ持続的な提供に関する責任」だけでなく、万が一の事象も起こりうるとの前提の下で、緊急時の早期・適切な対応といった趣旨を織り込むべきではないか。	御意見を踏まえ、本戦略（案）（4.2.2 官民一体となった重要インフラの防護）について、以下のように修文することとします。 「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」（以下「行動計画」という。）の5つの施策群に基づいた取組を推進してきた。」 なお、本戦略（案）の脚注46には、「任務保証」の考え方の基となる「2015年戦略」の「機能保証（任務保証）」を記載することとし、以下のとおり修文することとします。 「「2015年戦略」では「機能保証（任務保証）」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。」

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
51	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	『このような課題を解決するため、経営資源が限られ、サイバーセキュリティに十分な資源を割り当てることが難しい重要インフラ事業者等におけるセキュリティ対策モデルに関する検討を含め、…』とあるが、具体的にどのような取組みか、本戦略上どこに反映されているのか。	この記載の趣旨は、「サイバーセキュリティに関する全体的な底上げを行う必要がある」ということであり、「サイバーセキュリティに十分な資源を割り当てることが難しい重要インフラ事業者等におけるセキュリティ対策のモデルに関する検討」は、「全体的な底上げ」の一例として挙げているものです。具体的な取組については、関係主体で検討していく必要があると考えています。
52	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 ①リスクマネジメントの推進 重要インフラサービスは、サイバー攻撃発生時であっても安全かつ持続的に提供されることが望まれている。提供できるようにする必要がある。このため、重要インフラ事業者等は、事前のセキュリティ対策を講じるだけでなく、横断的かつ複合的なリスクを念頭に置いたリスクアセスメントの結果を踏まえ、「任務保証」の考え方に基づき、万が一の事態において、早期かつ適切に対応するため、を踏まえた事業継続計画及び緊急時対応計画を策定することが重要である。 【理由】 サイバー攻撃発生時に「安全かつ持続的に提供できるようにする必要がある」というのは、この戦略の中で記載されている「リスクを完全に除去することは不可能である」との内容にはそぐわない。	重要インフラは他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものであることから、そのような事態に陥らないようにするためにも、そのサービスの安全かつ持続的な提供は必要であるため、原案のとおりとします。 また、「事業継続計画及び緊急時対応計画」自体が「万が一の事態において、早期かつ適切に対応するため」のものであるため、この部分についても原案のとおりとします。
53	電気事業連合会	4．2．2　官民一体となった重要インフラの防護	戦略本文に係る意見	【修正案】 (1)行動計画に基づく主な取組 ⑤制御系システムのセキュリティ対策 電力、ガス、石油分野等では、サービスを提供するために制御系システムを利用しているため、サイバー攻撃により制御系~~この~~システムに大きな影響が~~不具合が~~生じると通常のサービスが提供できなくなり、国民生活に大きな支障が出るおそれがある。制御系システムの特性を踏まえたセキュリティ対策が十分に行われ、サービスが安全かつ持続的に提供できるよう、官民一体となって、制御系システムに関する人材育成を推進するとともに~~し~~、タイムリーに脅威情報の収集・分析・展開等を行っていく。 【理由】 1つの制御系システムが不具合を起こした場合にサービス影響が必ず発生するように誤解を招きかねない表現であるため、表現を見直した。 二文目は主語が不明確であり、本節のタイトルから「官民一体となって」という言葉を入れた。また、情報の収集・分析・展開は官庁からもタイムリーに提供されることを期待して言葉を補った。	御意見を踏まえ、本戦略（案）（4.2.2(1)⑤ 制御系システムのセキュリティ対策）について、以下のように修文することとします。 「電力、ガス、石油分野等の重要インフラ事業者の中には、サービス提供のために制御系システムを利用している事業者がある。サイバー攻撃等により制御系システムに大きな影響が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。制御系システムの特性を踏まえたセキュリティ対策が十分に行われ、サービスが安全かつ持続的に提供できるよう、官民一体となって、制御系システムに関する人材育成を推進するとともに、適時、脅威情報の収集・分析・展開等を行っていく。」
54	一般社団法人日本化学工業協会	4．2．2　官民一体となった重要インフラの防護	政策展開（サイバーセキュリティ2018）に係る意見	「サイバーセキュリティ対策を関係法令等における保安規制として位置付けるなど」の部分を削除していただきたい。 はじめから規則や法規制ありきの対応ではなく、法益や対象業種の特性を踏まえて必要性や在り方を慎重に検討することが大前提であると考える。	御指摘の箇所については、「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」に盛り込まれている内容であり、原案のとおりとします。 なお、サイバーセキュリティの完全性・可用性・機密性をどのように位置付けていくかについては、関係法令等の目的によって当然異なりますので、その目的に照らして、妥当な位置付けとなるように考えており、そのような意味で、「適切に改善」していくとしています。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料1－5

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
55	エムティインターナショナル株式会社	4．2．3　政府機関等におけるセキュリティ強化・充実	戦略本文に係る意見	政府機関等におけるセキュリティ強化・充実について、プログラム構造の欠陥対策を第1義で対策を考えなければ外壁対策では不可能である。今回のテーマ全てがプログラム問題であることを認識すべき。	OSも含めたソフトウェアの攻撃耐性を向上させる取組も重要と考えますが、昨今のサイバー攻撃の状況を鑑みれば、本戦略（案）（4.2.3(1)① 情報システムの防御能力の向上と状態の把握）に記載したように、IT資産管理、アカウント管理の徹底及び事案発生時の情報漏えいを防ぐためのデータ保護など、多層的な防御の取組を推進することとしているため、原案のとおりとします。
56	個人（2）	4．2．3　政府機関等におけるセキュリティ強化・充実	戦略本文に係る意見	表現を適正化するべき。 「ITの資産管理の自動化」について、「情報システムの状態をリアルタイムに把握し」という表現は少しあいまいな表現であるため、「情報システムの脆弱性、セキュリティ設定等をリアルタイムに把握し」に修文されたい。	情報システムの防御能力のために、情報システムを構成する機器やソフトウェアに関わる様々な項目を迅速に把握することを想定しており、全体を捉えた記載としているため、原案のとおりとします。
57	個人（2）	4．2．3　政府機関等におけるセキュリティ強化・充実	戦略本文に係る意見	表現を適正化するべき。 「効率的な情報システムの状態の把握」について、同様に「情報システムの脆弱性、セキュリティ設定等のリアルタイムの把握」に修文されたい。	情報システムの防御能力のために、情報システムを構成する機器やソフトウェアに関わる様々な項目を迅速に把握することを想定しており、全体を捉えた記載としているため、原案のとおりとします。
58	電気事業連合会	4．2．4　大学等における安全・安心な教育・研究環境の確保	戦略本文に係る意見	大学等の位置づけを国際関係などと関連させて取り扱うべき。	大学等は、国民に対する直接的な関わりが強いことから、本戦略（案）（4.2. 国民が安全で安心して暮らせる社会の実現）に盛り込んでおり、原案のとおりとします。
59	特定非営利法人日本セキュリティ監査協会	4．2．5　2020年東京大会とその後を見据えた取組	戦略本文に係る意見	表現の見直し。 「次により」を後ろに持ってきた方が読みやすいとの意見。	御意見を踏まえ、以下のように修文することとします。 「このため、以下のとおり、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する。」
60	一般社団法人JPCERTコーディネーションセンター	4．2．5　2020年東京大会とその後を見据えた取組	戦略本文に係る意見	将来的に、「サイバーセキュリティ対処調整センター」を「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（ナショナルCSIRT）として活用」するとの方針が記載されていることについての意見。 NISCとJPCERT/CCが、いわゆる「ナショナルCSIRT」の機能を分担して担ってきたものを新組織の所掌とすることは、国内外における混乱は必至であり、どのような役割分担を担う方針なのか、また、国内、国外に対してどのような説明を行うのか明らかにしてほしいというもの。	「サイバーセキュリティ対処調整センター」をナショナルCSIRTとして活用するため具体的な活用の方法、役割・業務については、今後、2020年東京大会に向けて対処態勢を確立していく過程で、既存の枠組が実施する国際連携・国内調整に混乱が生じないように、関係省庁・関係機関と調整を進めてまいります。
61	株式会社ラック	4．2．5　2020年東京大会とその後を見据えた取組	政策展開（サイバーセキュリティ2018）に係る意見	オリパラの際のサイバーセキュリティ対処調整センターの運用については、民間のセキュリティベンダーを含む関係機関等との協力関係を構築強化すべき。当社も可能な限り協力する。	東京大会を見据え、貴社を含む多くの民間セキュリティベンダーとの協力関係を強化していきたいと考えております。
62	電気事業連合会	4．2．5　2020年東京大会とその後を見据えた取組	戦略本文に係る意見	重要サービス事業者という文言が使用されているが、重要インフラ事業者の誤記ではないか。	重要サービス事業者には「重要インフラ事業者」に含まれる事業者もあれば、含まれない事業者もあります。以前から、2020年東京大会の開催・運営に重要なサービスを提供している事業者を「重要サービス事業者」と呼称しているところ、ここでもその意味で使用しており、誤記ではないため、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
63	公益財団法人笹川平和財団	４．２．６　従来の枠を超えた情報共有・連携体制の構築	戦略本文に係る意見	情報共有について、各主体単独で対応困難なものについて、政府が主導的にサイバーセキュリティの実務を担っていく必要がある旨を追記すべき。	本戦略（案）（4.2.6 従来の枠を超えた情報共有・連携体制の構築）において記載されている「新たな役割」の中には、ケースに応じて政府が主導的に対応を行うことも含んでいるため、原案のとおりとします。
64	公益財団法人笹川平和財団	４．２．６　従来の枠を超えた情報共有・連携体制の構築	戦略本文に係る意見	情報共有について、日本版AISを構築するため、内閣官房内閣サイバーセキュリティセンターがサイバー脅威情報共有システムの技術使用を定める旨を追記すべき。	「日本版AIS」を含め、先進的な情報共有システムの推進が必要であるとの観点から、本戦略（案）（4.2.6(2) 情報共有・連携の新たな段階へ）に「寄せられる情報に対して、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、各々の主体が真に必要とする情報の共有を実現していく。」と記載しているため、原案のとおりとします。
65	一般社団法人JPCERTコーディネーションセンター	４．２．６　従来の枠を超えた情報共有・連携体制の構築	戦略本文に係る意見	「従来の枠」が判然とせず、官民関係や業界区分が無くなるように読むことができ、それは不適切と考えられるため、官民や業界といった従来の枠を踏まえつつ新たな段階の情報共有の姿を検討し、環境造成や意見醸成に努める旨の記述に変更すべき。	サイバーセキュリティのための情報共有・連携の枠組みにおいては、例えば、所管省庁を同じくする複数の業界が情報共有体制を構築する動きが見られるなど、新しい連携が生まれつつあります。「官民や業界といった従来の枠を超えて」との記載は、官民関係や業界区分を前提としつつも、それに囚われない新しい動きの推進等を想定したものであり、趣旨としては明確と考えますので、原案のとおりとします。 御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
66	公益財団法人笹川平和財団	４．３．１　自由、公正かつ安全なサイバー空間の堅持	戦略本文に係る意見	IoT通信プロトコル等サイバー空間における国際標準の策定において主導的な立場を確保する旨を記載すべき。	本戦略（案）（4.1.3(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）において、「官民が連携の下、安全なIoTシステムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する」と記載されており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
67	特定非営利法人日本セキュリティ監査協会	４．３．１　自由、公正かつ安全なサイバー空間の堅持	戦略本文に係る意見	「既存の枠組みの存在」が何を想定しているのかが理解できるように「各種の国際条約等を踏まえた既存の枠組み」と修正すべき。	「既存の枠組み」の中には国際条約の他、国内法、国際的な協力に係る取組、政府の関与のあり方やルール形成のプロセス等が含まれますので、原案のとおりとし、御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
68	個人（2）	４．３．２　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	「均衡性のある対抗措置」に基づく「サイバー攻撃能力」による「報復の抑止」を明示すべき。	本戦略（案）（4.3.2(2)① 実行的な抑止のための対応）において、「我が国は、悪意ある主体の行動を抑止し、国民の安全・権利を保障するため、国家の関与が疑われるものも含め、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、同盟国・有志国とも連携し、脅威に応じて、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。」と記載しており、原案のとおりとします。
69	公益財団法人笹川平和財団	４．３．２　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	関係機関の情報収集に関する法的要件の見直しの検討についても検討を進めるべき。	本戦略（案）（4.1.3 安全なIoTシステムの構築）において、「プライバシーの問題などの共通課題やそれぞれの取組について、全体像が俯瞰できる形で可視化するとともに、情報共有を行うための仕組みを構築する」と、また、「ネットワーク上の脆弱なIoT機器の対策については、パスワード設定に不備のある機器の調査・特定を行い、電気通信事業者において当該機器の利用者への注意喚起を円滑に行えるよう、所要の制度整備を着実に進める」と記載されており、これらに基づく取組の検討や実施の推進に当たって参考とさせていただきます。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
70	特定非営利法人日本セキュリティ監査協会	４．３．２　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	「カウンターサイバーインテリジェンス」について括弧や注釈などで意味を記載すべき。	御意見を踏まえ、以下のように注釈を追加します。 「情報通信技術を用いた外国の敵意ある諜報活動に対抗する情報防衛活動」
71	電気事業連合会	４．３．２　我が国の防御力・抑止力・状況把握力の強化	戦略本文に係る意見	国内の脅威情報共有（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、教育研究機関など）推進について記載すべき。	本戦略（案）（4.2.6 従来の枠を超えた情報共有・連携体制の構築）の箇所において、「官と民、業界、国内外といった枠を超えた情報の共有・連携を推進していく」と記載されており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
72	次世代ICカードシステム研究会	４．３．３　国際協力・連携	戦略本文に係る意見	「国際標準」、「デジュール標準」、「デファクト標準」といった検討の場についても配慮すべき。	本戦略（案）（4.1.3(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）の箇所において、「官民が連携の下、安全なIoTシステムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する」と記載されており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
73	個人（6）	４．４．１　人材育成・確保	戦略本文に係る意見	おそらく、サイバー犯罪が出来るほどのプロは、中々居ない 日本の現場では”卑怯な奴は俺が捕まえる”と努力されています。これらの方は、日本のエライ方ではなく、庶民です。 国として、ある程度、身分保障が有っても、良いのではないか。	本戦略（案）（4.4.1人材育成・確保）において、「教育等を通じ、資格・評価基準等によって可視化された確かな知識と実践力を備えた人材が、適切な処遇を受け、更に実務経験を積み重ねることにより、人材の需要と供給が相応されるといった好循環の形成が必要である。」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
74	個人（7）	４．４．１　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	戦略マネジメント層の育成において、ITパスポート試験を必要な前提知識にしてはどうか。	サイバーセキュリティ2018（案）の4.1.(1)戦略マネジメント層の育成・定着において、「内閣官房において、戦略マネジメント層を担う人材の育成に向けて、必要な知識・スキルを身に着けるための試行的取組について検討する」との取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。
75	個人（7）	４．４．１　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	情報処理の促進に関する法律を改正して、情報セキュリティマネジメント試験を「情報処理安全管理推進士」、登録システムアドミニストレータ試験（登録シスアド）を創設してはどうか。	サイバーセキュリティ2018（案）の4.1.(2)実務者層・技術者層の育成において、情報処理安全確保支援士制度や情報セキュリティマネジメント試験の普及を図ることとしており、これらの取組の検討や実施の推進に当たって参考とさせていただきます。
76	個人（7）	４．４．１　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	ITパスポート試験を合否制からスコア制によるITリテラシースタンダード1級、2級などを認定する方式に改めてはどうか。	サイバーセキュリティ2018（案）の4.1.(2)実務者層・技術者層の育成において、ITパスポート試験を含む情報処理技術者試験全般について、「内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る」との取組を盛り込むこととしました。 試験方式の変更については、現時点では検討しておりませんが、今後の取組の検討や実施の推進に当たって参考とさせていただきます。
77	個人（7）	４．４．１　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	ITパスポート試験について、従前にあった中問をペーパー方式で90分程度の試験として新たに新設してはどうか。	サイバーセキュリティ2018（案）の4.1(2)実務者層・技術者層の育成において、ITパスポート試験を含む情報処理技術者試験全般について、「内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る」との取組を盛り込むこととしました。 試験方式の変更については、現時点では検討しておりませんが、今後の取組の検討や実施の推進に当たって参考とさせていただきます。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
78	個人（7）	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	各省庁の全職員等について、ITパスポートの受験を義務化すべき。	政府の職員は、ITのスキルを向上させるため、総務省が実施している「情報システム統一研修」を受講することができますが、この研修の中には、ITパスポート試験のレベルと同等と位置付けられるよう用意された「情報システム入門」コースが含まれております。 これらの「情報システム統一研修」については、政府部内育成の専門人材である「橋渡し人材」を育成するために、政府機関における統一的な方針である「サイバーセキュリティ人材育成総合強化方針」等に基づき、役職に応じた段階的な受講を原則とするなどの取組を進めています。 いただいた御意見は、上記の取組の実施や推進に当たっての参考とさせていただきます。
79	公益財団法人笹川平和財団	4．4．1　人材育成・確保	戦略本文に係る意見	民間の高度専門人材の採用拡大を検討する。	人材育成のカリキュラムについては、「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」（平成30年5月）において、NICEのプログラムを含む事例に基づくモデルカリキュラムを例示しています。 また、各府省庁における人材確保・育成については、本戦略（案）（4.4.1(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）に「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」と記載しており、具体的には、「サイバーセキュリティ人材育成総合強化方針」に基づき、各府省庁において情報セキュリティ・ITに関する専門的知識・経験を有する者を任期付職員として積極的に採用するなどの取組を進めています。いただいた御意見は、これらの取組の実施や推進に当たって参考とさせていただきます。
80	一般社団法人サイバーリスク情報センター産業横断サイバーセキュリティ人材育成検討会	4．4．1　人材育成・確保	戦略本文に係る意見	戦略案の主旨について賛同。 以下の点を補強することで、戦略の影響力および効果が更に高まる。 1．産学官、各業界、各業界、産業横断などの多様な連携を促進することが肝要。 2．信頼の輪に基づく民間の主体的かつ持続的な活動を促進することで、迅速かつ柔軟な対応の実現とその実効性を高めることに繋がる。 3．セキュリティ人材育成を継続的に推進すること自体が大きな課題。我が国の産業構造・業務形態・人事慣行などの実状を踏まえたセキュリティ人材への多様なニーズに答えることを考慮すべき。 4．セキュリティ人材に少ない日本の経営層を支えるセキュリティ統括人材（戦略マネジメント層に該当）は重要な存在。	賛同の御意見として承りました。 「1．持続的かつ効果的な協調体制を構築・発展させるために、産学官、各業界、業界横断などの多様な連携を促進することが肝要。」と、「2．信頼の輪に基づき、民間（産業界）の主体的かつ持続的な活動（特に事例・ノウハウの共有など）を促進することで、迅速かつ柔軟な対応の実現とその実効性を高めることに繋がる。」につきまして、本戦略（案）（4.4.1 人材育成・確保）において、「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・確保を強化していく」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。 「3．全ての施策を支えるセキュリティ人材育成を継続的に推進すること自体が大きな課題。また、我が国の産業構造・業務形態・人事慣行などの実状を踏まえた、セキュリティ人材への多様なニーズにこと得ることを考慮すべき。」につきまして、戦略マネジメント層、実務者層・技術者層、あるいは突出した能力を有しグローバルに活躍できる人材の育成について記載しており、御意見の主旨も踏まえて取組を進めてまいります。 「4．特にセキュリティの専門家が少ない日本の経営層を支えるセキュリティ統括人材（戦略マネジメント層に該当）の存在は、より重要なものと位置付け」につきまして、本戦略（案）（4.4.1(1) 戦略マネジメント層の育成・定着）において「サイバーセキュリティに係るリスクを認識し、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場」として「戦略マネジメント層」を位置付け、経営層の理解の促進と、その定着を図ってまいります。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
81	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	・民間主導での、雇用機会、キャリアパス創出、適切な処遇が確保されることが重要。 ・短期で成果を上げるため、民間で既に行われているキャリアパスの明確化等の取組を参照する等、関係する主体との連携を推進してほしい。	人材の需要（キャリアパスや雇用機会）につきましては、「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書」（平成30年5月）（2．（3）　各層別の役割とキャリアパス）において「戦略マネジメント層」と「実務者層・技術者層」について想定されるキャリアパスを記載しており、一般の民間企業での参考としていただくことで、キャリアパスや雇用機会の創出の促進を図っております。 また、同報告書では、産業サイバー人材育成検討会の第１期報告書やIPA（ITSS+）での人材定義を紹介し、同様の取組の連係を図っております。 御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
82	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	先般制度化された登録セキスペについて、個人や民間企業等の資格取得・保持への更なるインセンティブ付与策を検討いただきたい。	サイバーセキュリティ2018（案）の4.1(2)実務者層・技術者層の育成において、「経済産業省において、情報セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として2016年に開始した情報処理安全確保支援士（登録セキスペ）制度の着実な実施と当該制度の普及のため、企業や団体への周知等を積極的に行う」との取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。
83	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	若年層に対する情報モラル教育の一環として、関連法令に係る普及啓発の強化、教員養成課程や教員の研修への盛り込み、各地で普及啓発に取り組む者へのインセンティブ付与策を検討していただきたい。	サイバーセキュリティ2018（案）の4.1(3)人材育成基盤の基盤、4.3.全員参加による協働において、「文部科学省において、独立行政法人教職員支援機構と連携し、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する」及び、「文部科学省において、ネットモラルキャラバン隊を通じ、スマートフォン等によるインターネット上のマナーや家庭でのルールづくりの重要性の普及啓発を実施する」との取組をもりこむこととしました。 御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。
84	株式会社ラック	4．4．1　人材育成・確保	政策展開（サイバーセキュリティ2018）に係る意見	高度なサイバーセキュリティ技術を持つ人材となることが期待される若年層向け環境整備に係る民主導の取り組みについて、各主体のよりいっそう積極的な関与を促進いただきたい。	サイバーセキュリティ2018（案）の4.1(3)人材育成基盤の基盤及びにおいて、「文部科学省において、新学習指導要領の実施を見据え、児童生徒の発達の段階に応じた、プログラミング的思考や情報セキュリティ、情報モラル等を含めた情報活用能力を培う教育を一層推進する」及び「総務省において、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」における「SecHack365」の取組を通じて、若年層のICT人材を対象に、高度なセキュリティ技術を本格的に指導し、セキュリティイノベーターの育成に取り組む」との取組を盛り込むこととし、施策の検討や実施の推進に当たって参考とさせていただきます。
85	個人（3）	4．4．1　人材育成・確保	戦略本文に係る意見	リボルビングドアなど官民交流の仕組みを作ることが人材不足を解消する一つの方法であると考える。	本戦略（案）（4.4.1 人材育成・確保）において、「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・確保を強化していく」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
86	一般社団法人新経済連盟	4．4．1　人材育成・確保	戦略本文に係る意見	国内の人材育成で、海外の知見を取り入れる旨の記載が必要。	本戦略（案）（4.4.1(5) 国際連携の推進）において、「我が国のサイバーセキュリティ人材の育成においても、国内で完結するのではなく、可能な限りグローバルな規模で切磋琢磨できるようにするべきである」及び「海外の人材育成を行う組織との間で様々な連携を促すための仕組み作りを主要国との連携の下で進める」と記載しており、国内での人材育成に海外からの知見を積極的に取り入れるという趣旨についても包含しているため、原案のとおりとします。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
87	個人（8）	4．4．1　人材育成・確保	戦略本文に係る意見	横断的施策に関して組織間のバラつきを埋めるため情報処理安全確保支援士制度を核とした専門人材の活用プラットフォームを構築することが必要と考える。	情報処理安全確保支援士制度においては、登録者の氏名、連絡先、得意分野・スキル等をウェブ上で公開することで、企業による活用の促進を図っています。今後も当該制度の普及に向け、企業や団体への周知を積極的に行うこととしており、御指摘の点も、取組の検討や実施の推進に当たって参考とさせていただきます。
88	個人（2）	4．4．2　研究開発の推進	戦略本文に係る意見	現状の攻撃者優位から防御者優位の状況に転換するための重要な基盤技術の1つとして、帰属特定技術の研究開発を推進する必要がある。	本戦略（案）（4.4.2(1) 実践的な研究開発の推進）において、「トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発を進める」と記載しており、これに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
89	公益財団法人笹川平和財団	4．4．2　研究開発の推進	戦略本文に係る意見	サイバーセキュリティ産業の育成については、政府の重要な横断的施策として特記することが望ましいため、「4.4.2. サイバーセキュリティ産業の育成」として政府による研究機関のACE指定等の創設やサイバーセキュリティ産業育成の国家戦略特区の設定の検討に関する文章を追加すべき。	本戦略（案）（4.1.1(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）において、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のための各種の施策を推進する旨、また同（4.4.1(5) 国際連携の推進）において、海外の人材育成を行う組織との間での様々な連携を促すための仕組み作りを推進する旨を記載しており、これらに基づく取組の検討や実施の推進に当たって参考とさせていただきます。
90	株式会社ラック	4．4．2　研究開発の推進	政策展開（サイバーセキュリティ2018）に係る意見	いわゆるコンピュータ・ウイルスに関する罪の成立要件を具体的かつ網羅的にお示しいただきたい。 また、同罪、不正アクセス禁止法その他の関係法令について、いわゆるセーフハーバールールの導入を検討いただきたい。	サイバーセキュリティ2018（案）の1.1(1)経営層の意識改革において、「内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う」との取組を盛り込むこととし、制度上の課題に関する調査・研究を推進していきます。
91	個人（9）	4．4．3　全員参加による協働	戦略本文に係る意見	「サイバーセキュリティ教育」の定義が曖昧な上、「情報モラル教育」の“一部”としてしまうと、“悪さをしない”ということだけに限定されるのではないか。 あらためて、情報安全を確保するという意味での“サイバーセキュリティ”を明確にすべき。そろそろ、積極的な“セキュリティマインド”を醸成するという意味での「サイバーセキュリティ教育」を前面に押し出すべき。 せめて、「情報モラル教育及びサイバーセキュリティ教育」としていただきたい。	本戦略（案）では、「自由、公正かつ安全なサイバー空間」を目指す上で、サーバーセキュリティに関する国民一人一人の理解を幅広い観点から促していくことを意図しております。御意見も踏まえ、主旨を明確にするため、以下のように修文することとします。 「学校教育での情報活用能力の育成を通じて、サイバーセキュリティについての教育を推進する。」

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料1－5

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
92	公益財団法人笹川平和財団	5. 推進体制	戦略本文に係る意見	中長期的には、 ・内閣サイバーセキュリティセンターを発展的に機能強化しサイバーセキュリティ庁として独立の機関とすべき。同庁への各府省の監督、サイバー攻撃の検知・収集・分析、サイバー攻撃に対処するための指揮命令及び予算要求の権限付与等について検討すべき。 ・インターネット利用者に対するサイバーセキュリティ対策賦課金の導入についても検討するべき。 【理由】 ・国家支援のサイバー攻撃や所属不明の大規模サイバー攻撃など高度・大規模なサイバー攻撃の対処まで民間の自主的な取り組みに任される ・様々な行政機関が分散的にサイバーセキュリティの人材育成・産業育成を実施している	本戦略(案)（5. 推進体制）において、「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」に記載しており、内閣サイバーセキュリティセンター及び関係機関の能力強化及び必要な予算の確保を図っていくこととしており、今後の取組の参考とさせていただきます。 なお、御意見も踏まえ、必要な予算の確保に関する趣旨を明確にするため、以下のように修文することとします。 「各府省庁の施策が着実かつ効果的に実施されるよう、経費の見積もり方針を定め、政府としての必要な予算の確保と執行を図る。」
93	次世代ICカードシステム研究会	5. 推進体制	戦略本文に係る意見	今回の戦略では「個人・組織による平時からの対策と連携」として民間の協力が求められており、本戦略の全体のロードマップについてもお示し頂きたい。	本戦略（案）（3.2. 目指すサイバーセキュリティの基本的な在り方）において、「3つの観点（中略）からサイバーセキュリティに関する官民の取組を推進することとし、サイバー空間における安全・安心と経済発展を両立させ、信頼できるサイバー空間が自律的・持続的に進化・発展することを目指す」と記載し、3年間の諸施策の目標及び実施方針を明確にしています。 また、それを達成するための具体的な施策についても、本戦略（案）（5. 推進体制）において「各年度の年次計画を作成する」と記載しているように、各年度の年次計画において明らかにすることとしています。
94	経団連産業技術本部	5. 推進体制	政策展開（サイバーセキュリティ2018）に係る意見	内閣サイバーセキュリティセンターのリーダーシップの下、これらの施策が着実に実行に移されるとともに、2020年の東京オリンピック・パラリンピックに向け、政党・省庁・業界・組織・地域等の壁を越えて、Society 5.0の実現に不可欠なサイバーセキュリティ強化に向けた取り組みが進展することを期待する。	賛同意見として承りました。
95	電気事業連合会	5. 推進体制	戦略本文に係る意見	下記のとおり修正してはどうか。 【修正案】 また、本部は、本戦略で示された方向性に基づき、各府省庁の施策が効果的に実施されるよう、実行費用の見積もり方針を定め、政府としての最適な予算の確保と執行を図る。 【理由】 国の姿勢は「やむを得ない経費」との意識が表れているのではないか。	サイバーセキュリティ基本法第25条で、本部の事務について「関係行政機関の経費の見積りの方針（中略）の作成」等とされていることを踏まえて記載しており、御指摘の「やむを得ない経費」という趣旨ではないため、原案のとおりとします。
96	個人（10）	–	不明	日中韓3カ国きょう情報通信相会合がおかしい。日本人の個人情報を中国に売り渡す動きではないか。	本意見募集と直接関係ないと考えられますが、御意見として承ります。

「サイバーセキュリティ戦略（案）」等に関する意見募集の結果一覧

資料１－５

通しNo	提出者	該当箇所	御意見の種類	御意見の要旨	御意見に対する主な考え方及び修正
97	個人（11）	－	不明	・社会構造が古い為に新しく改革し向上による概略案 ・教育内容の改正による具体案 ・女性社会進出での改正による具体案 ・外国人高度人材での導入で社会水準の向上による具体案 ・「ガバナンス（政治統治）」構造の改正による具体案 ・生活水準での基準による詳細案 ・官公庁が考案した無駄な政策の廃止による詳細案」	本意見募集と直接関係ないと考えられますが、御意見として承ります。

資料１－６

（案）

サイバーセキュリティ戦略

平成 30 年＊月＊日

この戦略は、サイバーセキュリティ基本法（平成26年法律第104号）第12条第５項において準用する同条第４項の規定に基づき、国会に報告するものである。

目次

1. 策定の趣旨・背景 …… 1

1.1. サイバー空間がもたらすパラダイムシフト …… 1

1.2. 2015 年以降の状況変化 …… 2

2. サイバー空間に係る認識 …… 4

2.1. サイバー空間がもたらす恩恵 …… 4

2.2. サイバー空間における脅威の深刻化 …… 6

3. 本戦略の目的 …… 8

3.1. 基本的な立場の堅持 …… 8

3.2. 目指すサイバーセキュリティの基本的な在り方 …… 10

4. 目的達成のための施策 …… 13

4.1. 経済社会の活力の向上及び持続的発展 …… 13

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 …… 13

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 …… 16

4.1.3 安全な IoT システムの構築 …… 17

4.2. 国民が安全で安心して暮らせる社会の実現 …… 20

4.2.1 国民・社会を守るための取組 …… 20

4.2.2 官民一体となった重要インフラの防護 …… 22

4.2.3 政府機関等におけるセキュリティ強化・充実 …… 24

4.2.4 大学等における安全・安心な教育・研究環境の確保 …… 26

4.2.5 2020 年東京大会とその後を見据えた取組 …… 27

4.2.6 従来の枠を超えた情報共有・連携体制の構築 …… 28

4.2.7 大規模サイバー攻撃事態等への対処態勢の強化 …… 30

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 …… 31

4.3.1 自由、公正かつ安全なサイバー空間の堅持 …… 31

4.3.2 我が国の防御力・抑止力・状況把握力の強化 …… 32

4.3.3 国際協力・連携 …… 35

4.4. 横断的施策 …… 37

4.4.1 人材育成・確保 …… 37

4.4.2 研究開発の推進 …… 39

4.4.3 全員参加による協働 …… 41

5. 推進体制 …… 43

1. 策定の趣旨・背景

1.1. サイバー空間がもたらすパラダイムシフト

現代科学の知見を基礎としたデジタル技術の急速な進展により生み出された、インターネットを中核的な基盤とするサイバー空間は、民間を中心とする多様な主体[1]の自律的な取組により、グローバルな拡張・発展を続けてきた。

こうした発展を遂げた空間は、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・データを自由に生成・共有・分析することが可能な場であり、流通する場でもある。この空間で活動する主体は、誰もが他の主体と関わり合いながら、新たな価値を生み出していく可能性がある。

こうした特徴を持つサイバー空間は、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あり、今後の経済社会の持続的な発展の基盤でもある。また、この空間は自由主義、民主主義、文化発展も支えている。この空間では、人間は創意工夫によって活動を飛躍的に拡張させることができる[2]。すなわち、サイバー空間は「無限の価値を産むフロンティア」である。我が国は、こうしたサイバー空間を堅持するため、採り得るあらゆる手段により、サイバーセキュリティに関する取組を行っていく。

今後、サイバー空間を前提とする人工知能（以下「AI」という。）などの計算機科学の知見の更なる進展により、新たな製品・サービスの創出が期待される。新たな製品・サービスの出現は、人々の日常の行動や生活環境を変えることにより意識の変化をもたらし、それが既存の手続、モデル、組織などの社会システムや産業構造の変革を促していく起点になる。これまで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「Society 5.0[3]」へのパラダイムシフトが生じつつある中、今後の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、検討する必要がある。

---

1 サイバーセキュリティ基本法（平成26年法律第104号）第16条において、「国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体」と規定されている。サイバー関連事業者については、同法第７条で「サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。)」と規定されている。

2 サイバーセキュリティ戦略（平成27年９月４日閣議決定）において、この特徴が社会に与えている大きな影響を、グーテンベルグの活版印刷が知の爆発を引き起こした歴史にたとえている。

3 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。（出典：未来投資戦略2017（平成29年６月９日閣議決定））

1.2. 2015 年以降の状況変化

サイバーセキュリティ基本法[4]（以下「基本法」という。）に基づき、サイバーセキュリティ戦略本部（以下「本部」という。）での検討を経て、2015 年９月に閣議決定されたサイバーセキュリティ戦略（以下「2015 年戦略」という。）は、３年間のサイバーセキュリティに関する施策の基本的な方針である。

2015 年戦略の策定後、官民データ活用推進基本法[5]や改正個人情報保護法[6]等のデータ利活用に関する一定の法的な基盤が整備された。また、政府は、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人間中心の社会[7]を目指す方針を決定した。こうした中、現在、実空間においてセンサやデバイスを介して生成された大量のデータが、サイバー空間において集積・分析されている。そして、そのデータを活用することにより付加価値をつけた新たな製品やサービスが実空間で提供されるという循環が様々な分野で始まっており、進展している。もはや、サイバー空間と実空間が独立して存在するのではなく、相互に作用する状態が生じており、両者を分けて捉えることはできない。むしろ、サイバー空間と実空間は一体として進化を続ける有機的なものとして捉えるべきである。

こうしたサイバー空間と実空間の一体化に伴い、社会に豊かさがもたらされる可能性が飛躍的に高まる。一方で、悪意ある主体がサイバー空間を利用する機会も増大し、実空間での経済的・社会的な損失のリスクが指数関数的に拡大・加速することが予想される。

こうした中、経済社会が、人々に豊かさをもたらし、持続的に発展するためには、その基盤であるサイバー空間のサイバーセキュリティが確保されつつ、自律的・持続的に進化・発展していく必要がある。サイバー空間の脅威に対して、一部の国においては、国家が優越的な地位から管理・統制することを重視するという潮流が出てきている。しかしながら、国家によるサイバー空間の管理・統制を強めることは、このような自律的・持続的な発展の可能性を閉ざすことになる。全ての主体の自律的な取組により発展してきたサイバー空間を尊重し、連携・協調してサイバーセキュリティの確保に取り組む必

4　平成26年11月６日成立。サイバーセキュリティという概念を法的に位置付け、各主体の責務などを明確化した。

5　官民データ活用推進基本法（平成28年法律第103号）。平成28年12月７日成立。官民データの推進に関する基本理念等が定められた。

6　個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成27年法律第65号）。平成27年９月３日成立。平成29年５月30日全面施行。適切に匿名加工する前提で個人に関わるデータの利活用を進めるための整備が行われた。

7　Society 5.0の内容（出典：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）

要がある[8]。

こうした認識の下、我が国は、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。）等の国際的なイベントを控えていることを見据え、2020年以降の目指す姿を念頭に置きつつ、サイバーセキュリティの基本的な在り方を明確にした上で、新たに取り組むべき課題を明らかにし、速やかに対策を実施することで、サイバーセキュリティ対策に万全を期していく。

本戦略は、こうした今後のサイバーセキュリティに係る我が国としての基本的な立場や在り方を明らかにするとともに、今後３年間の諸施策の目標及び実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるものである。

8　2015年９月に国連サミットで採択された「「持続可能な開発のための2030アジェンダ」、持続可能な開発目標（SDGｓ（Sustainable Development Goals））」は、持続可能な世界を実現するための17の目標を設定し、「誰ひとり取り残さない」社会の実現を目指すとしている。持続的な開発を目指すという点や、全ての主体が連携・協調して取り組むという点で、こうしたサイバーセキュリティの取組方針と共通点があると考えられる。

2. サイバー空間に係る認識

AI、IoT[9]、Fintech[10]、ロボティクス、３Dプリンター[11]、AR/VR[12]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しており、この結果、サイバー空間と実空間の一体化が進展している[13]。

本戦略の策定の前提として、こうしたサイバー空間がもたらす「恩恵」とこの空間における「脅威」の状況を的確に認識する必要がある。サイバー空間の知見や技術・サービスの恩恵を享受するためには、これらに常に内在している不確実さを制御することが不可欠であり、制御できない場合にはサイバーセキュリティに係る脅威が一気に高まるおそれがある。

2.1. 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・サービスは、様々な分野で当然に利用されるようになってきている状況である。今後も、サイバー空間が持続的に発展することにより、人々に豊かさをもたらすことが予想される。

(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

我が国におけるインターネット利用者数が増加し、その普及率は上昇している[14]。また、デバイス面ではスマートフォンの個人保有率が大きく伸び[15]、インターネット利用率は増加している[16]。SNS の利用割合も伸びており[17]、サイバー空間上で簡単にコミュニケーションを行える環境が整った状況である。このようにサイバー空間におけるサービスが社会に定着していき、自由な情報の流通にとどまらず、多様なコミュニティの形成、情報共有が進んでいる。

経済活動においても、ネットショッピングや株取引・オンラインバンキングの利用

---

9 Internet of Thingsの略

10 Finance（金融）とTechnology（技術）を組み合わせた造語。ブロックチェーンやビッグデータ、AIといった新たな技術を活用し、多くが急速に普及したスマートフォンやタブレット等を通じて行われる革新的な金融サービス（出典：平成29年版　情報通信白書）

11 通常の紙に平面（二次元）的に印刷するプリンターに対して、３DCAD、３DCGデータを元に立体（３次元のオブジェクト）を造形する機器（出典：一般社団法人日本３Dプリンティング産業技術協会のWebサイト）

12 Augmented Reality/Virtual Reality（拡張現実/仮想現実）

13 2015年戦略では、「実空間のモノやヒトが、サイバー空間上の情報の自由な流通とデータの正確な通信により物理的な制約を超えて多層的につながる（連接する）ことで、実空間とサイバー空間の融合が高度に深化した社会、すなわち「連接融合情報社会」が到来しつつある。」としている。

14 インターネット人口普及率（2014年末82.8%→2016年末83.5%）（出典：平成29年版　情報通信白書）

15 スマートフォンの個人保有率（2014年末44.7%→2016年末56.8%）（出典：平成29年版　情報通信白書）

16 インターネット利用率（2015年末83.0%→2016年末83.5%（出典：平成29年版　情報通信白書）

17 代表的SNS（LINE、Facebook、Twitter、mixi、Mobage、GREE）の利用率※の推移（全体）（2014年末62.3%→2016年末71.2%）（出典：平成29年版　情報通信白書）※６つのいずれかを使用

が進んでいるとともに、Fintech、シェアリングエコノミー[18]の分野で新サービスが次々登場し、これらがイノベーションを牽引している。また、生産年齢人口の減少、地域の高齢化といった社会的課題に関連する医療・介護、福祉、教育等の分野における情報通信技術の活用も進展している。

(2) AI の劇的な進化

AI については、昨今の計算機科学の知見が進展し、大量のデータが必要である機械学習の分野の研究が進展し、深層学習という手法が登場した。深層学習は、その登場により、AI の画像解析の精度を飛躍的に向上させ、製品の異常検知、ガンの診断、投資判断、翻訳等の精度を高め、経済社会において様々な機能の効率化・高品質化を加速させ、既に幅広い産業に応用され始めている。サイバーセキュリティにおいても、こうした可能性を持つ AI は、例えば、マルウェアの自動検知などの対策の自動化に活用されつつある。

深層学習による AI の進化は、機械・ロボットの世界でカンブリア爆発にたとえられるほどの変化をもたらすとの指摘[19]がある。深層学習では、従来の機械学習で人間が行う必要のあった識別・判断のための特徴量[20]の設計について、コンピュータが自ら特徴量を導き出すことができるようになり、これが AI の進化として着目されている。音楽、絵画、小説等の創作物や自動運転等のサービスにつながる出力（例：判定・判断・提案結果）について、人間が創作的な寄与をせずに、AI がこれらを自律的に生成する世界が現実的になりつつある。こうした AI が権利侵害や事故を起こした場合の責任を誰が負うのかといった問題が生ずる可能性があることも指摘[21]されている。

こうした AI の進展は、今後、AI を活用した全く新しい製品・サービスを出現させ、人々の日常の行動や生活環境を変えることにより、これまでの人間の物事に関する認識に変化をもたらし、それが既存の社会システムや産業構造の変革を促すことも予想される。

18　個人等が保有する活用可能な資産等を、インターネット上のマッチングプラットフォームを介して他の個人等も利用可能とする経済活性化活動（出典：平成29年版　情報通信白書）

19　「カンブリア爆発　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。ディープラーニングにより、見えるようになる。さらに次に何が起こるかを予想して動けるようになる。眼を持った機械が誕生する。機械・ロボットの世界でのカンブリア爆発が起こる。」（出典：平成29年２月３日日本経済再生本部第4次産業革命人材育成推進会議（第２回）資料１）

20　対象を認識する際に注目すべき特徴は何かを定量的に表すこと。ディープラーニング以前は人間の手で特徴量を設計していたが、ディープラーニングによって画像認識や音声認識などでコンピュータが自ら特徴量をつくりだすことが可能となった。（出典：平成28年版　情報通信白書）

21　「今後、AI生成物の出力に対する利用者（人間）の関与が減少していった場合に利用者に責任を負わせて良いのかという問題が生じる可能性もある」（出典：知的財産戦略本部「新たな情報財検討委員会報告書」（平成29年３月））

(3) IoTの進展

センサの小型軽量化、低廉化が進み、全てのモノがネットワークにつながるIoTの爆発的な普及が進んでいる。家電、自動車、ロボット、スマートメーター等のモノの活用だけでなく、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。

具体的に、電子行政やスマートシティ、ものづくり、自動運転、金融、健康・医療・介護等の分野[22]で生産性の向上やサービスの高付加価値化を進める動きがあり、そのサプライチェーン[23]の中でのデータ利活用が進むと予想される。また、サイバー空間を介して、分野を越えて協業を行ういわゆるオープンイノベーション[24]が進み、データを共有して分析することにより、人々に豊かさをもたらす新たなサービスが次々と創出される期待がある。

2.2. サイバー空間における脅威の深刻化

AI や IoT などの技術・サービスが人々に多くの恩恵をもたらす可能性がある一方で、こうした技術・サービスを提供する者がこれらを制御できなくなるおそれは常に内在しており、その場合には、逆に、多大な経済的・社会的な損失が生じ得る。サイバー空間と実空間の一体化が進展する中、こうした深刻な影響が生ずる可能性は指数関数的に拡大している。また、この空間は、場所・時間の制約を受けずに、悪意ある主体を含む全ての者が、新たな情報通信技術を悪用・濫用し、容易に活動できる場である。悪意ある主体とそのグループは、攻撃プログラムを含むデータや情報を容易に複製・流通させることが可能というデジタル技術の特性だけでなく、進展するAI やブロックチェーン[25]等の技術も柔軟に取り入れて自由に利用できる。このため、攻撃者には防御側と比べて非対称な優位性があり、特に、防御側の体制が従前の制度や技術体系を前提としている場合には、その優位性が高まると考えられる。

こうした中、実際に、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[26]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

22　世界最先端デジタル国家創造宣言・官民データ活用推進基本計画（平成30年６月15日閣議決定）において、我が国が集中的に対応すべき、①経済再生・財政健全化、②地域の活性化、③国民生活の安全・安心の確保といった諸課題に対し、官民データ利活用の推進等を図ることで、その解決が期待される８つの分野（電子行政、健康・医療・介護、観光、金融、農林水産、ものづくり、インフラ・防災・減災等、移動）が重点分野として指定されている。

23　供給網。取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと

24　組織内部のイノベーションを促進するために、意図的かつ積極的に内部の技術やアイディアなどの資源の流出入を活用し、その結果組織内で創出したイノベーションを組織外に展開する市場機会を増やすこと

25　ブロックチェーン技術のこと。電子署名とハッシュポインタを使用して改ざん検出が容易なデータ構造を持ち、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術（出典：日本ブロックチェーン協会「ブロックチェーンの定義」）

26　バングラディシュ中央銀行がハッキングを受け、約8,100万ドルが不正送金された事案。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（Mirai）の登場（2016年９月）。ウクライナの国営電力会社に変電所へのサイバー攻撃（2016年12月）等

ビス障害が国内外で生じ、経済社会の持続的な発展や国民生活の安全・安心等を脅かす事例が生じている。また、国家の関与が疑われる大規模な事案も発生している。さらに、一部の国が優越的な地位からサイバー空間を管理・統制することにより、情報インフラの信頼性が揺らぐ懸念もある。

今後、実空間との一体化が進展するサイバー空間において、官民のデータ利活用が更に進むと、IoT、サプライチェーン、オープンイノベーションの脆弱な部分を狙う動きや意図しない動きが発生する懸念は高まると考えられる。政府機関や重要インフラ事業者だけでなく、それ以外の事業者及び個人に対しても、深刻な影響が生ずる可能性が高まることが予想される。

(1) 業務・機能・サービス障害による社会への多大な影響

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もある。今後、サイバー空間と実空間の一体化が更に進めば、社会の機能障害、人命や生活へのリスクを含む国民の安全・安心、国家や民主主義の根幹をも揺るがす事態が生じるおそれもある。

(2) 情報の毀損及び漏えいによる競争力低下

IoT の爆発的な普及や、オープンデータ化が進む中、データを利活用した新たなサービスが増えていく。また、データの分析に当たってAIの活用が進む。深層学習に用いるデータはAIの性能に直結するものであり、データの重要性がますます高まる中、データの真正性[27]・完全性[28]が毀損されると、データを利活用したサービスの信頼が揺らぐことになる。

また、個人情報、営業秘密、価値あるデータを始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、組織・企業の社会的評価・信頼の低下を招くおそれがある。これらは、一度流出すれば取り返しがつかないものであり、組織・企業の競争力の低下に直接つながるものである。

(3) 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した事例が生じている。今後、経済社会がサイバー空間にますます依存していくことが想定される中、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。

27 ある主体又は資源が、主張どおりであることを確実にする特性
28 情報に関して破壊、改ざん又は消去されていないこと

3. 本戦略の目的

サイバー空間に係る現状認識の下、その将来像を視野に入れ、本戦略の目的として、以下のとおり、基本的な立場を堅持することや、こうした立場を踏まえて目指す「サイバーセキュリティの基本的な在り方」を示す。

3.1. 基本的な立場の堅持

我が国は、「基本法の目的」や 2015 年戦略で示した「基本的な理念」及び「基本原則」といった基本的な立場を堅持する。また、このような立場から、引き続き、悪意ある主体の行動を抑制し、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する。

(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」、「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」（以下「国際社会の平和・安定及び我が国の安全保障に寄与すること」という。）を目的としている[29]。本戦略においても、この３つの領域に政策目的を整理し、それぞれの目的に沿って、施策を推進することとする。

(2) 基本的な理念

基本法の目的に寄与するため、「自由、公正かつ安全なサイバー空間」を目指すこととし、この基本的な理念を堅持する。これは、サイバー空間で活動しようとする全ての主体が、正当な理由なく差別や排除されずに、表現の自由や経済活動の自由が保障され、情報・財産の窃取などの不正な活動を許さない安全な空間である。

(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当たって従うべき基本原則については、2015 年戦略で掲げた「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つの原則を堅持する。

① 情報の自由な流通の確保

サイバー空間が創意工夫の場として持続的に発展していくためには、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、維持されるべきである[30]。また、プライバシーへの配慮も引き続きなされるべきである。なお、情報の自由な流通で他者の権利・利益をみだりに害すことが

29 基本法第１条において、「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。」と規定されている。

30 基本法第１条において、「情報の自由な流通を確保しつつ」と規定されている。

ないようにしなければならない。

② 法の支配

サイバー空間と実空間の一体化が進展する中、サイバー空間においても、実空間と同様に、法の支配が貫徹されるべきである。この空間では、国内においては法令を含む各種ルールや規範が適用されている。また、同様に、この空間では、既存の国際法が適用される。今後、サイバー空間が安全で信頼できる空間として持続的に発展していくためには、引き続き、既存の国際法の適用、規範の形成が不可欠である。

③ 開放性

サイバー空間が新たな価値を生み出す空間として持続的に発展していくために、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、サイバー空間は全ての主体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していく[31]。

④ 自律性

サイバー空間は多様な主体の自律的な取組により発展を遂げてきた。サイバー空間が秩序と創造性が共存する空間として持続的に発展していくためには、国家が秩序維持の役割を全て担うことは不適切であり、不可能である。サイバー空間の秩序維持に当たっては、様々な社会システムがそれぞれの任務・機能を自律的に実現することにより、悪意ある主体の行動を抑止し、対応する以外にはなく、これを促進していく[32]。

⑤ 多様な主体の連携

サイバー空間は、国、地方公共団体、重要インフラ事業者、サイバー関連事業者その他の事業者、教育研究機関及び個人などの多様な主体が活動することにより構築される多次元的な世界である。こうしたサイバー空間が持続的に発展していくためには、これら全ての主体が自覚的にそれぞれの役割や責務を果たすことが必要である。そのためには、個々の努力にとどまらず、連携・協働することが求められる。国は、連携・協働を促す役割を担っており、その役割を果たすことができるように施策を推進していく[33]。

31　高度情報通信ネットワーク社会形成基本法（平成12年法律第144号）第３条において、「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」と規定されている。

32　基本法第３条第２項において、「サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促す」と規定されている。

33　基本法第３条第１項において、「サイバーセキュリティに対する脅威に対して、（中略）多様な主体の連携により、積極的に対応することを旨として、行われなければならない。」と規定されている。

3.2. 目指すサイバーセキュリティの基本的な在り方

前述の基本的な立場を踏まえ、「サイバーセキュリティの基本的な在り方」として、以下のとおり、サイバーセキュリティの取組により目指す姿や、その取組を進めるに当たって求められる３つの観点を示す。

(1) 目指す姿

我が国は、「無限の価値を産むフロンティア」である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[34]の実現を目指している。

こうした社会の実現に寄与するため、サイバー空間は、全ての主体が新たな価値の創造に参画することで発展していくことが必要である。この発展を持続的に支えるためには、生物における免疫系のように、全ての主体が、サイバーセキュリティについて自らの役割を認識し、サイバーセキュリティに関する取組を自律的に行うことが求められる。

このような視点に立って、サイバーセキュリティの取組を進めるに当たって、以下のように取り組むこととする。

具体的には、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）からサイバーセキュリティに関する官民の取組を推進することとし、サイバー空間における安全・安心と経済発展を両立させ、信頼できるサイバー空間が自律的・持続的に進化・発展することを目指すというものである。

このように、全ての主体が、サイバーセキュリティに関する取組を自律的に行いつつ、相互に影響を及ぼし合いながら、サイバー空間が進化していく姿を、持続的に発展していく一種の生態系にたとえて、「サイバーセキュリティエコシステム」と呼称することとする。

(2) ３つの観点

① サービス提供者の任務保証

～業務・サービスの着実な遂行～

「任務保証」とは、企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」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することである。その際には、一部の専門家に依存するのではなく、各々の組織の「任務」に該当する業務・サービスを遂行する観点から、その責任を有する者が主体的にサイバーセキュリティの確保に取り組

34 Society 5.0の内容（出典：科学技術イノベーション総合戦略2017、未来投資戦略2017）

むことが肝要である。

すなわち、これは、サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方である。

② リスクマネジメント

～不確実性の評価と適切な対応～

「リスクマネジメント」とは、組織が担う「任務」の内容に応じて、リスク[35]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である。これは、サイバー空間に本質的にある不確実さから、不可避的に導かれる観点である。

リスクは、「目的に対する不確実さの影響[36]」と定義され、目的を設定して初めて測れるものである。したがって、リスクは、組織の目的によって、その評価や対応が変わってくるものである。また、リスクマネジメントは「リスクについて組織を指揮統制するための調整された活動[37]」と定義されており、リスクの特定・分析・評価という個別の活動を指すのではなく、組織を指揮統制して、組織が有する有限の資源を適切に分配し、リスクに対応していく一連の活動の全体を意味している。

各々の組織の「任務」に該当する業務・サービスを認識せずに、リスクを過小評価して、サイバーセキュリティに必要な資源を分配しなければ組織の存立そのものに関わるような事態を招くおそれがある。一方で、リスクを過大評価して、サイバーセキュリティに過剰に資源を分配すれば組織の業務・サービスの遂行と持続的な成長に支障が生ずることとなる。

このようなリスクマネジメントの考え方は、個人においても、サイバー空間の知見や技術・サービスを活用して恩恵を享受している以上、求められるものである。

恩恵の享受に当たっては、その前提となる技術・サービスを制御できなくなるおそれというリスクが発生するのが一般的である。その際、機械的な予測は成り立たず、完全なリスクの除去は不可能であることから、リスクの性格や影響の現れ方に応じて適切に対処し、その効用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求められる。

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～

35 プラス及びマイナスの両面がある不確実性を意味することに留意
36 国際標準化機構（ISO）の定義
37 国際標準化機構（ISO）の定義

「参加・連携・協働」とは、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である。サイバー空間で活動する主体は、誰もが、その恩恵として新たな価値を生み出す可能性があり、内在するリスクから発生する脅威にさらされる可能性がある。このような観点から、サービスを提供する組織だけでなく、個人においても、基本的な取組を平時から行う必要がある。

具体的には、不正プログラムからの防御、脆弱性[38]の解消、認証における信頼性確保、個人情報の適切な管理等に関する対策が挙げられる。こうした取組は、実空間における公衆衛生活動や交通安全活動にたとえられる。

しかし、いつでもどこでもサイバー攻撃が生じるなど脅威が日常化していく中で、個々の努力による取組のみでは対応が困難であり、その取組を補強するため、組織を含む他者による積極的な助けも必要となる。

このため、皆が力を合わせて取り組むこと、すなわち協働が求められる。サイバー空間に関わる個人又は組織各々が、個々の努力で取り組むだけでなく、平時においても事案発生時においても、情報の共有を行い、個人と組織間で相互に連携・協働することをサイバー空間における新たな公衆衛生活動と捉えて、基本的な取組と位置付けていく必要がある。

我が国は、こうした基本的な取組を推進するため、官民連携で支援することが求められる。特に、国は、基本原則に掲げた「多様な主体の連携」の原則に基づき、連携・協働を促す役割を平時から積極的に担うことが求められる。

38　脅威の発生を誘引するような人、モノ、サービス上の欠落点

4. 目的達成のための施策

本戦略の目的を達成するため、戦略が寄与する政策領域ごとに、今後３年間に執るべき諸施策の目標や実施方針を示す。各施策は、前述の基本的な立場やサイバーセキュリティの基本的な在り方で示した３つの観点を踏まえたものであることが求められる。

4.1. 経済社会の活力の向上及び持続的発展

近年、企業においては、パソコン・スマートフォンを始めとするデジタル端末やインターネットの活用による業務の生産性の向上にとどまらず、経営改革や革新的なサービスの創出といった新たな価値を生み出す動きが進展している。サイバーセキュリティ対策をやむを得ない「費用」ではなく、こうした動きを支える基盤としての「投資」であると捉えて、一体的に取り組むことは、産業の成長及び国際競争力の強化につながり、我が国の経済社会の活力の向上及び持続的発展の観点から重要である。

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

サイバー空間と実空間の一体化が進展していく中で、企業が直面するサイバーセキュリティに係るリスクは、これまで以上に高まっていく。こうした中、企業におけるサイバーセキュリティに対する問題意識は、一部の業種や大企業を中心として高まっている。今後は、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つつ新たな価値を創出していくためには、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、取組を促進していく必要がある。

その際には、サイバーセキュリティに係るリスクは企業が直面する様々なリスクの一つであり、その対策をリスクマネジメントの一環として捉え、業種・業態等の状況に応じて、自然な形で対策が組織に浸透していくことが重要である。

(1) 経営層の意識改革

サイバーセキュリティ対策については、その取組自体が利益を生むものではないとの考え方が未だ支配的であると考えられる。この背景には、サイバー空間は自由に何の備えもなく利用できるものであり、散発的にしか起こらない、経営に対して影響が生じるような攻撃への対処は「費用」でしかないという考え方がある。しかしながら、サイバー空間の利用が急速に進展する中、自由であるがゆえに常に脅威が潜んでいるという認識に立って、そのための備えをすることが必須である。また、企業においては、サイバーセキュリティ対策の組織上の位置付けが明確になっていないと取組が進みにくいという側面がある。このため、経営層が、サイバーセキュリティ対策をやむを得ない「費用」ではなく、事業継続や新たな価値創出のために不可欠な「投資」であると捉えられるようにするため、経営層の意識改革が不可欠である。

具体的には、経営層は、取締役会等を通じたサイバーセキュリティに関する積極的な関与が期待されるとともに、リスクマネジメントのために必要となるサイバーセキュリティに関する一定の知識・能力を身に付けることが求められる。その際、経営層に深い技術的な知識やスキルを期待することは必ずしも現実的ではない。このため、経営戦略、事業戦略におけるサイバーセキュリティに係るリスクを認識し、経営層の方針を踏まえた対策を立案し、実務者・技術者を指導できる人材（いわゆる「戦略マネジメント層」）を確保することが重要である。また、経営層は、自社の対策だけでなく、外部委託先やサプライチェーン全体を視野に入れ、リスクマネジメントとして相応しいレベルの対策ができるような体制を整備するとともに、株主等に対してサイバー空間を活用したビジネスの恩恵とリスクを説明できるようにする必要がある。

このような状況を踏まえ、官民が連携して、経営層に対してサイバーセキュリティ対策に関する説明や議論ができる人材を発掘・育成するとともに、経営層向けセミナー等を開催し、経営層の意識改革を促していく。また、国は、サイバーセキュリティに取り組む企業による宣言の促進や、類似の企業の対策状況と比較することで、自社に必要な対策を可視化するためのツールの整備など、経営層に分かりやすくサイバーセキュリティ対策を訴求するための施策を推進する。また、学会等と連携しつつ、企業がサイバーセキュリティ対策の実施において参照すべき法制度に関する整理を行う。

(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、それに対応する経営上のインセンティブがあることが重要である。すなわち、財務的な観点を含め、サイバーセキュリティに係るリスクとその対策が可視化され、経営層がその現状を認識し、更に必要な具体的な対策を検討・導入するとともに、市場がその取組を企業価値の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継続的に生まれる、という好循環が形成されることが望ましい。

このため、投資家を意識して、企業が積極的にサイバーセキュリティに関する取組について情報発信・開示を行うことが重要であり、国は、ベストプラクティスの共有やガイドラインを策定するとともに、情報発信・開示の状況についての継続的な把握・評価に取り組む。加えて、投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組み作りを進めていくことも必要である。

また、企業に対するサイバーセキュリティの促進策について、サイバーセキュリティに対する投資のインセンティブが効果的に機能するよう、国はその活用状況をフォローしつつ、必要に応じて所要の措置を検討する。

このほか、サイバーセキュリティのリスクマネジメント手段の一つとして、保険の活用が広がっているが、サイバーセキュリティ対策の実施状況に応じて、適切に保険料が算定される仕組みにより、リスクへの備えに対するコストが明確になっていくため、投資が進めやすくなる可能性がある。こうした点を踏まえ、官民が連携してサイバーセキュリティにおける保険の活用を推進するための方策について検討を行う。

(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

企業が新たな価値を創出するためには、IoT、AI、VR、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、こうした技術の活用は、これまでになかった新たな脆弱性を生み、それが悪用されることで想定外のリスクが発生する可能性がある。このため、リスクの想定を先取りし、サイバーセキュリティ対策をモノやサービス等を創出する過程において可能な限りあらかじめ組み込んでおくこと（セキュリティ・バイ・デザイン）によって、サイバーセキュリティに関する品質の高いモノやサービス等を実現することが期待される。また、こうした取組は、我が国のモノやサービス等に対する信頼の向上につながるだけでなく、我が国が目指す質の高いインフラの海外展開の推進にもつながるものである。

一方、企業がこのような取組を進めようとしても、サイバーセキュリティに関する専門性を有していないなどの理由により、容易に進められない可能性があることに加え、国際競争力の強化や真正性・信頼性の検証が困難なセキュリティ製品・サービスへの依存を回避する観点から、我が国において具体的な解決策を提供できるサイバーセキュリティビジネスの強化が必要である。

このようなニーズに応えるため、大企業のみならずベンチャー企業を含め、先端技術による新たな価値創出に向けたチャレンジを支えられるよう、官民が連携して、機動的に先端技術の利用に伴うサイバーセキュリティに係るリスクの分析・明確化とそれに基づくガイドラインの策定や普及等に取り組む。また、こうした取組のために必要となる先端技術のリスク分析や脅威への対策に係る研究開発を推進する。これらの取組においては、セキュリティ・バイ・デザインの考え方を基本とすることが重要である。さらに、先端技術による新たな価値創出を目指す企業と、その先端技術の利用を支えるためのサイバーセキュリティ技術・サービスの供給者とのマッチングやサイバーセキュリティ技術・サービスの適切な評価に係る仕組みの構築等に向けた検討を行う。

加えて、我が国の高いサイバーセキュリティが確保されたモノやサービス等についての国際展開を促すため、トップセールスや展示会等を活用したアピールを行うほか、

サイバーセキュリティを理由とした自由貿易の障害となる措置を正当化する動きに対しては、国際的な連携の下、厳格に対処するなど、国際展開をしやすいビジネス環境の整備に取り組む。

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

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」の実現に向けて、グローバルな規模でこれまで取引がなかった異なる業種の企業間取引が生まれている。また、その取引自体が自動化されたものになるなど、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ている。そして、このような形態においては、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、実空間、さらには、経済社会全体にこれまで以上に広く波及し、甚大な悪影響を及ぼすおそれがある。このようなリスクを認識し、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である。

(1)　サイバーセキュリティ対策指針の策定

サプライチェーンにおけるつながりが多様かつ流動的な形態になる中、サイバーセキュリティの確保を進めていくためには、サプライチェーン全体に対して、一貫性をもった必要な対策が実装されることが不可欠である。また、このような取組を通じて、モノやサービスに関わる品質が新たな価値を生み出すことが期待される。

具体的には、官民が連携して、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を策定するとともに、その普及を図る。その際には、中小企業を含めた事業者が実際に対策を行いやすくするため、事業者の事情を踏まえた現実的に実施が可能な内容で、かつ、分かりやすいものとなるように十分に配慮する。また、事業者がリスクと対策費用のバランスを意識できるものとすることも重要である。

産業分野毎のサプライチェーンに関わるつながり方や守るべきもの、脅威の差異を意識しつつ、IoT 機器や組織等に求められる具体的な対応策を産業分野毎に示していく必要がある。さらに、サプライチェーンがグローバルに広がる中で、我が国における対策指針に基づくサイバーセキュリティ対策がグローバルに認められるようにするため、海外におけるルール化の動きも反映する必要がある。

(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

サプライチェーン全体としてのサイバーセキュリティを確保するためには、製造される機器、生成されて流通するデータ、それらを利用したサービス等のサプライチェーンの構成要素における信頼の確保が不可欠である。このため、それぞれの構成要素

がセキュリティ要件を満たした形で生成・流通されるよう、要件の明確化を図るとともに、その要件が満たされていることを確認等することにより信頼を創出する仕組みの構築が必要である。また、サプライチェーンにおける調達者が機器・サービス等の利用に際し、その信頼を確認できるよう、官民が連携して、信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。さらに、これらがサプライチェーンのつながりにおいて、連続的な仕組みとなるよう、トレーサビリティ[39]を確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する。

(3)　中小企業の取組の促進

中小企業は、サイバー攻撃により、金銭的な損害や信用の低下が生じた場合、経営に与えるインパクトが大企業と比べて大きい。また、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も懸念されている。一方、中小企業は、必ずしも高いサイバーセキュリティに関する知識やスキルを有しているとはいえず、サイバーセキュリティに対して十分な投資を行うことが難しいという事情を踏まえた上で、サイバーセキュリティ対策を推進する必要がある。

このため、国は、中小企業を対象として、安全な情報システムの利活用モデルの提示を含む理解しやすいサイバーセキュリティ対策の事例集を作成するとともに、サイバーセキュリティ保険の活用促進、中小企業がサイバーセキュリティに関するトラブル等について相談できる仕組みの強化を行う。また、官民が連携して、サイバーセキュリティに取り組んでいる中小企業が、それを自主的に宣言できる仕組みなどの可視化の取組を促進するとともに、インセンティブの仕組みとの連携により、効果的に中小企業のサイバーセキュリティを進めるための仕組み作りを行う。

4.1.3　安全な IoT システム[40]の構築

サイバー空間につながる様々なモノが急速に広がっており、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（機器）のサイバーセキュリティ対策が喫緊の課題となっている。また、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様々なモノ（IoT 機器）のつながりが拡大する中、こうしたつながりは、新たな脅威を生む可能性がある。このような状況を踏まえ、官民が連携して、安全な IoT システムの構築に取り組む必要がある。

(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

39　追跡可能性

40　家電、自動車、ロボット、スマートメーター等のあらゆるモノがインターネット等のネットワークに接続され、そこから得られるビッグデータの利活用等により新たなサービスの実現が可能となるシステム

これまで、IoT システムのサイバーセキュリティ対策については、官民が連携し、ガイドラインの策定を始めとする安全な IoT システムの実現に向けた様々な取組を推進してきた。今後は、安全な IoT システムが価値を創出することに重点を置き、一定の整合性・一貫性をもって戦略的に取り組む必要がある。

このため、我が国がこれまで示してきた安全な IoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素[41]に基づき、各主体の間で対策に係る基本理念、目標、方法、期限等についての共通認識の醸成と、各分野・各主体の役割や機能の明確化を図った上で、自律的にサイバーセキュリティに関わる取組を進めつつ、各主体が協働した取組を推進する。また、国は、こうした取組を促すため、官民の各主体が抱える分野個別の課題だけでなく、その範囲や定義、物理安全対策、責任分界点（既知の脆弱性への対応に関する製造者責任や運用者等の安全管理義務などインシデント発生時における各主体の法的責任を含む）やプライバシーの問題などの共通課題やそれぞれの取組について、全体像が俯瞰できる形で可視化するとともに、情報共有を行うための仕組みを構築する。さらに、IoT システムにおける価値創出の仕組みを、我が国の安全・安心といった強みを活かしながらグローバルな規模で展開し、安全な IoT システムの普及によって国際経済の発展に貢献するため、官民が連携の下、安全な IoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する。

(2) 脆弱性対策に係る体制の整備

IoT 機器に対するサイバー攻撃等の深刻化に対応するため、ネットワークの安全・信頼性を確保する観点で、産官学民及び民間企業相互間の連携と役割分担の下、対策を推進することが重要である。このため、官民が連携して、IoT 機器の脆弱性について、設計・製造、運用、そして破棄までのライフサイクル全体を見通したサイバーセキュリティ対策や、ネットワーク上の脆弱な IoT 機器の対策等のための体制整備が必要である。

ライフサイクルを見通した IoT 機器のサイバーセキュリティ対策については、それぞれの機器の利用方法やサイバーセキュリティ上の脅威、諸外国の検討状況や技術の進展の動向等を十分踏まえた上で、機器製造事業者、電気通信事業者、利用者等の各々の主体の相互理解と連携の下で取り組むべきである。その中で、官民が連携して、それぞれの IoT 機器について、その特性や利用方法等を踏まえつつ必要なサイバーセキュリティの要件を整理し、その要件を満たす IoT 機器の利用を推奨する。

また、ネットワーク上の脆弱な IoT 機器の対策については、パスワード設定に不備

41 「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10月サイバーセキュリティ戦略本部報告）

のある機器の調査・特定を行い、電気通信事業者において当該機器の利用者への注意喚起を円滑に行えるよう、所要の制度整備を着実に進める。また、対策の実施に当たっては、関係省庁等が一体となって、電気通信事業者、機器製造事業者等と連携して取り組む。

　将来的には、これらの我が国の対策をモデルとして、国際的な連携や標準化等を通じて海外に展開し、安全なネットワークの環境整備に貢献をしていく。

4.2. 国民が安全で安心して暮らせる社会の実現

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、教育研究機関、そして国民一人一人に至るまで、多様な主体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る。

特に、政府機関や重要インフラ事業者、事業者団体及び地方公共団体（以下「重要インフラ事業者等」という。）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る。サイバーセキュリティに係るリスクを完全に除去することは不可能であるとの認識の下、リスクを許容し得る程度まで低減し、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、サイバーセキュリティの基本的な在り方で掲げた「任務保証」の考え方に基づく取組を推進していく。

また、我が国は、2019 年のラグビーワールドカップや 2020 年東京大会などの国際的・国民的な大会を控えており、悪意ある主体によるサイバー攻撃の誘因となることも予想される。2020 年東京大会等を円滑に実施するとともに、その後も見据え、各々の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必要がある。

4.2.1　国民・社会を守るための取組

サイバー空間の脅威の深刻化に伴い、多くの国民がサイバー犯罪に不安感を持つようになっており、社会全体におけるサイバーセキュリティへの危機意識は高まっている。このような状況を踏まえ、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ことが不可欠である。

(1)　安全・安心なサイバー空間の利用環境の構築

サイバー犯罪・サイバー攻撃は複雑化・巧妙化しており、攻撃の種類も多種多様となっていることから、従来の受動的な対策だけでは対応しきれず、これまでよりも積極的な対策を行う必要がある。

このような状況を踏まえ、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[42]」を推進する。具体的には、国は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、攻撃者の情報を集めるための攻撃誘引技術の活用、ボットネット[43]対策等、サイバー犯罪・サイバー攻撃による被害

42　サイバー攻撃に対して能動的に防御していく取組のこと

43　ウイルス感染等により攻撃者の自由に操られる状態となったパソコン等の機器（「ボット」と呼ばれる）を束ねたネットワークのこと。DDoS攻撃やスパムメールの送信等に悪用される。（出典：独立行政法人　情報処理推進機構「情報セキュリティ白書2017」）

を未然に防止できるような取組を推進する。

また、政府機関や重要インフラ事業者等が提供するサービスの全体の基盤となる信頼できる情報インフラについて、国際海底ケーブル等のインフラ設備の防護の強化を含めた整備を促進する。このため、信頼性を評価するための検証や政府調達における運用改善等について検討し、対策を進める。

さらに、国民が仮想通貨取引を安全に利用できるよう、仮想通貨交換業者と連携し、対応を推進する。また、自動運転車やドローンについては、サイバー攻撃を受けて不正操作された場合には人命に影響を及ぼすおそれがあるため、かかる事態が生じないよう対策を推進する。特に、自動運転車については、国際場裡において国際基準策定の議論が進められており、引き続き議論を主導していく。

(2) サイバー犯罪への対策

サイバー空間が国民生活により身近なものとなる中で、世界規模のランサムウェア[44]感染被害や、国内の仮想通貨交換業者から多額の仮想通貨が不正に送信されたと見られる事案が発生するなど、サイバー犯罪が深刻な社会問題となっている。国民の安全と安心を守るためには、サイバー犯罪の実態把握、取締りを推進するとともに、関係機関・団体と連携し、国民一人一人の自主的な対策を促進するための広報啓発を行うほか、新たな手口のサイバー犯罪に対処できるよう、捜査能力・技術力の向上が不可欠である。

このため、国は、徹底した捜査活動や新たな捜査手法の検討、サイバー犯罪の被害を防止するための広報啓発活動等を推進する。また、高度な情報通信技術を用いた犯罪に対処するため、最新の電子機器や不正プログラムの解析のための技術力の向上、サイバー空間の脅威の予兆把握や脅威の技術的な解明のための総合的な分析を高度化すること等、情報技術の解析に関する態勢を強化する。さらに、民間事業者等の知見の積極的な活用や官民の人事交流を推進するとともに、情報の共有・分析、被害の未然防止、人材育成等の観点から、官民が連携したサイバー犯罪対策を推進する。

サイバー犯罪捜査等においては、サイバー空間における事後追跡可能性の確保が必要である。これには、関連事業者の協力や国際的な連携が不可欠であるため、必要な取組を行う。特に、通信履歴等に関するログの保存の在り方については、関係のガイドライン[45]を踏まえ、関係事業者における適切な取組を推進する。

44 データを暗号化して身代金を要求するマルウェア（malware。malicious softwareが短縮された語）
45 「電気通信事業における個人情報保護に関するガイドライン」の解説等

4.2.2　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[46]」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[47]」（以下「行動計画」という。）の５つの施策群[48]に基づいた取組を推進してきた。しかし、重要インフラ分野ごとに、サイバーセキュリティに関する意識や取組の進捗に温度差があるという課題がある。このような課題を解決するため、経営資源が限られ、サイバーセキュリティに十分な資源を割り当てることが難しい重要インフラ事業者等におけるセキュリティ対策のモデルに関する検討を含め、サイバーセキュリティに関する全体的な底上げを行う必要があり、各々の主体が自主的な取組を進めつつ、国も積極的な支援を行うことで、官民一体で取り組んでいく。

(1)　行動計画に基づく主な取組

重要インフラを防護するため、国は行動計画を策定・改定してきており、今後も引き続き、行動計画に基づく取組を推進していく。行動計画については、2020 年東京大会終了後に見直す予定であるが、社会動向の大きな変化等が生じた場合は、その前の時点においても、必要に応じて見直しを行う。

重要インフラ分野は、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきという観点から指定しているものである。社会的情勢に鑑み、必要に応じて、重要インフラ分野や対象とする重要インフラ事業者等を拡大することにより、セキュリティの取組の輪を広げていき、面としての防護を強化していくとともに、情報共有の取組を更に促進し、情報共有体制を拡充していく。

また、重要インフラ防護の取組を推進するためには、重要インフラ事業者等の経営層の積極的な関与が必要不可欠であることから、サイバーセキュリティに関する意識を高めるように経営層への働き掛けを行いつつ、以下の取組を推進する。

①　リスクマネジメントの推進

重要インフラサービスは、サイバー攻撃発生時であっても安全かつ持続的に提供できるようにする必要がある。このため、重要インフラ事業者等は、事前のセキュリティ対策を講じるだけではなく、横断的かつ複合的なリスクを念頭に置いたリスクアセスメントの結果を踏まえ、「任務保証」の考え方を踏まえた事業継続計画[49]及び緊急時

46　2015年戦略では「機能保証（任務保証）」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。
47　平成29年４月18日サイバーセキュリティ戦略本部決定
48　安全基準等の整備・浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント及び対処態勢の整備、防護基盤の強化
49　BCP（Business continuity planning）

対応計画を策定することが重要である。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、取組を推進する。

② 安全基準等の改善・浸透

重要インフラ事業者等における適切な対応を促進するため、国は、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や人的要因によるリスク軽減の在り方を含め、業務の内容、組織の規模、システムの使用期間、国際競争力への影響等を考慮して安全基準等を改善する取組を継続的に推進する。また、安全等を維持する観点から、サイバーセキュリティ対策を関係法令等における保安規制として位置付けるなど、制度的枠組みを適切に改善していく。

③ 深刻度評価基準

近年のサイバー攻撃の動向に鑑みれば、サイバー攻撃発生を検知した場合には、政府機関、重要インフラ事業者等の各々の主体の間で速やかに認識の共有を図り、迅速な対応の要否等の判断を行うことができるようにする必要がある。この実現に向けて、国民への周知による効果や影響に配慮しつつ、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し、事案の深刻度を評価・公表することにより、様々な主体が冷静かつ適切な対応を行うことができるよう促していく。また、この基準がより良いものとなるように適時見直しを行っていく。

④ 官民の枠を超えた訓練・演習の実施

重要インフラ事業者等が、サービス障害発生時であっても適切に対応できるよう、そのような事態を想定した訓練・演習を実施し、能力向上を図ることが大切である。国や関係機関は、官民の枠を超えた様々な規模の主体の間での訓練・演習を引き続き実施し、必要に応じて対象の拡大や内容の改善を図るなど、発展させていく。

⑤ 制御系システムのセキュリティ対策

電力、ガス、石油分野等の重要インフラ事業者の中には、サービス提供のために制御系システムを利用している事業者がある。サイバー攻撃等により制御系システムに大きな影響が生じると通常のサービスが提供できなくなり、国民生活に大きな支障が生じるおそれがある。制御系システムの特性を踏まえたセキュリティ対策が十分に行われ、サービスが安全かつ持続的に提供できるよう、官民一体となって、制御系システムに関する人材育成を推進するとともに、適時、脅威情報の収集・分析・展開等を行っていく。

(2) 地方公共団体のセキュリティ強化・充実

地方公共団体が提供するサービスは、国民生活に密着しているものであり、そのサ

ービスの提供に支障が出ると、地域の活動にも大きく影響が生じてしまう。リソースに限りのある団体におけるセキュリティ対策については、個別に技術的な対策をとることには限界があるものの、まず、サービス障害や、人為的ミスによるマイナンバーを含む情報漏えいに対してしかるべき対策を講じる必要がある。

こうした中、現行の国と地方の役割分担を背景に、国による直接の関与[50]が他の機関に比べて限定的な中で、全国の地方公共団体において対策の抜本的強化に取り組んできており、引き続き、高いセキュリティレベルを確保する必要があるため、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する。また、地方公共団体における業務の円滑化を考慮しつつ、業務用ネットワークのセキュリティレベルを確保するとともに、セキュリティ人材の確保・育成及び体制の充実並びに必要な予算を確保するための取組を推進する。

加えて、官民の認証連携について、利便性とセキュリティのバランスが取れたものとなるよう、環境整備を進めていく。

4.2.3 政府機関等におけるセキュリティ強化・充実

各政府機関においては、統一的な基準を踏まえた情報セキュリティ対策が講じられるとともに、当該基準に基づいた監査や、不正な通信の監視等の取組等を通じて、政府機関全体としての対策の水準の向上が推進されてきており、引き続きこれら取組を継続することが必要である。基本法の改正[51]により、独立行政法人及び基本法に基づく指定法人（以下「独立行政法人等」という。）に対する取組の枠組みが、政府機関に対するものと同様に拡充されたが、今後、独立行政法人等の多様な業務形態を踏まえ、その特性に応じた効果的な情報セキュリティ対策を進めていくことも重要な課題となる。

複雑化・巧妙化しているサイバー攻撃に対しては、引き続き攻撃を前提とした多層防御や、サプライチェーンリスクへの対応を強化するとともに、新たな技術を活用し、従来の攻撃側優位の状況を改善するための取組を進めることが求められる。

政府機関及び独立行政法人等（以下「政府機関等」という。）における行政サービスの円滑な遂行は極めて重要な責務であり、システムへの投資を行う際には所要の IT 投資とセキュリティ関連投資を一体的に行うことが不可欠である。このような状況を踏まえ、政府機関等の IT 投資の効率化によって得られた原資をセキュリティに充てるなどセキュリティ関連投資の充実を図るために必要な予算を確保するとともに、上記

50 技術仕様の統一・監査等
51 サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（平成28年法律第31号）。平成28年４月15日成立。国による不正な通信の監視・監査・原因調査等の対象を拡大

の情報セキュリティ対策を強化していくことが重要である。

(1) 情報システムのセキュリティ対策の高度化・可視化

脅威が深刻化しているサイバー攻撃に対して、これらへの対処能力の向上に加え、被害の未然防止や、仮に被害が発生した場合にも、その拡大の防止や極小化を行うことを目指し、新たな防御技術を活用し、より効果的な取組を行う。

① 情報システムの防御能力の向上と状態の把握

政府機関等において、プログラムが動作するエンドポイント（端末等）においてマルウェアの挙動を検知することにより、被害の未然防止及び拡大防止に取り組む。IT資産管理の自動化により、情報システムの状態をリアルタイムに把握し、ソフトウェアの脆弱性への迅速な対応を可能としていく。また、全政府機関を対象としたデータ保護により、事案が発生した際にも情報を漏えいさせない取組を図る。さらに、様々な機器で発生する事象やアカウント管理情報を組み合わせて脅威を分析することにより、検知が困難な攻撃を発見する対策について検討する必要がある。この対策を効率的に行うためには、情報の分析に係る作業等の自動化を見据えたシステムを構築する必要がある。

② 政府機関等における横断的な連携の高度化による被害の発生・拡大の防止

政府機関等において、予防・検知・復旧・対処の各段階において端末等でのマルウェアの監視やIT資産管理の自動化について、導入状況等を踏まえつつ、これらから得られる情報をGSOC[52]に適切に共有するなど、政府機関等とGSOCによる効果的かつ効率的な連携の高度化による横断的な対応の発展を目指す。

(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

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、政府プライベートクラウドとしての政府共通プラットフォームへの移行を含むクラウド化を推進する。クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討し、対策を進める。

また、インターネット接続回線については、統一基準においてその接続口の統合・集約化を求めてきた。政府機関のインターネット接続口の適切な集約を更に推進することは、運用及びセキュリティ対策上、非常に効果的であるため、政府共通ネットワーク及び政府共通プラットフォームと連携しつつ、境界監視ポイントの集約を含め、

52 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

必要な検討を行う。

(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、サイバー攻撃に対する高い耐性を有するものがある。こうした新しい設計思想の下で誕生した情報技術について、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、防御側優位に向けた転換を目指す。

(4)　監査を通じたサイバーセキュリティの水準の向上

基本法に基づき、政府機関等に対して実施する監査において、組織横断的な分析により抽出される傾向や課題を政府機関等全体にフィードバックし、更なるサイバーセキュリティの水準の向上を促す。また、効率的な情報システムの状態の把握に係る取組に沿って整備される各政府機関における IT 資産管理情報を活用し、効果的かつ効率的に監査を実施することを目指す。

(5)　組織的な対応能力の充実

事案対応を行うチーム[53]を中心に、各政府機関等の事案対応能力や情報セキュリティに係る知識を向上させる。また、政府機関等に対するサイバー攻撃の発生に備え、各府省庁の知見・技能を有する職員から構成される機動的な支援が可能な体制（情報セキュリティ緊急支援チーム[54]）の強化を図るため、要員の対処能力の向上のための研修等を充実する。

4.2.4　大学等における安全・安心な教育・研究環境の確保

大学及び大学共同利用機関等（以下「大学等」という。）は、多様な構成員によって構成され、多岐にわたる IT 資産、多様なシステムの利用実態を有する。このような大学等の特性を踏まえ、安全・安心な教育・研究環境を確保するためには、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することが重要である。

(1)　大学等の多様性を踏まえた対策の推進

大学等の経営層は、自らサイバーセキュリティ対策の重要性を認識した上で、サイバーセキュリティ対策を経営上の重要課題と位置付け、対策を推進するための計画等に基づき自律的かつ組織的に取り組むとともに、フォローアップを実施することによりサイバーセキュリティ対策を一層推進する必要がある。

53　CSIRT（Computer Security Incident Response Team）
54　CYMAT（Cyber Incident Mobile Assistant Team）

こうした取組に当たっては、様々な教育・研究を実施している大学等の多様性を踏まえつつ、守るべき IT 資産を特定し、サイバーセキュリティに係るリスクの評価を行い、リスクに応じて重点的に実施するべきマネジメント面・技術面における対策を検討することが求められる。また、事案に適切かつ迅速な対処をするための能力の向上に向けた取組や、これらの対策を組織的かつ着実に実施するための体制についても検討する必要がある。

国は、大学等に対して、サイバーセキュリティに関するガイドライン等の策定・普及、リスクマネジメントや事案対応に関する各層別研修及び実践的な訓練・演習の実施、事案発生時の初動対応への支援を通じて、大学等における自律的かつ組織的な取組を促進する。

(2) 大学等の連携協力による取組の推進

大学等は、共通の情報基盤を利用しており、共通性が見られるサイバーセキュリティ上の課題を有している。こうした大学等の実態を踏まえたサイバーセキュリティ対策の強化が重要であり、各々の相互協力による取組の一層の促進が求められている。

このため、学術情報ネットワークを運営する機関は、国立大学及び大学共同利用機関と連携し、サイバー攻撃を観測・検知・分析するシステムを構築し、情報提供を行うとともに、監視能力の機能維持・強化及び戦略マネジメント層の育成に向けた共同研究や技術職員への研修を実施する。

さらに、国は、大学等の事案対応体制を強化するため、複数の大学等の事案対応を行うチームにおいて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取組を支援する。

4.2.5 2020 年東京大会とその後を見据えた取組

オリンピック・パラリンピック競技大会は、世界中から多数のアスリート、要人、観客等が集まり、国際的にも最高度の注目を集めて開催される行事であることから、サイバー攻撃のターゲットとなるおそれがある。

過去の大会を振り返ると、ロンドン大会では、大会の運営には影響はなかったものの、膨大な数のサイバー攻撃があったとされるほか、リオデジャネイロ大会においても平昌大会においても、相当数のサイバー攻撃が行われ被害を受けたとの報道がある。2020 年東京大会においても、過去の大会以上のサイバー攻撃が予想され、その特性上各種サービス分野にまたがるような攻撃も想定される。このため、以下のとおり、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する。

また、2020 年東京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していく。

(1) 2020 年東京大会に向けた態勢の整備

引き続き、「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[55]に基づき大会の安全に関する情報の集約等の取組を進めるとともに、物理的なセキュリティとの連携も考慮してリスク源を分析し、その結果を踏まえたリスクシナリオの検討を含め、大会運営に影響を与える可能性のある重要サービス事業者等におけるサイバーセキュリティ上のリスク評価及びそれにより明確となる分野横断的なリスクを含めた各種リスクへの対策を促進する。また、関係府省庁、大会組織委員会、東京都、競技会場のある地方公共団体、重要サービス事業者等、大会関係組織間でサイバーセキュリティに係る脅威情報を共有するとともに、事案発生時に大会関係組織が皆で力を合わせて対応するために国が調整役となるための組織である「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)」の構築を推進し、緊密に連絡調整を図るための態勢を整備する。

(2) 未来につながる成果の継承

2020 年東京大会の態勢整備のための各種施策を引き続き推進し、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、2020 年東京大会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していく。また、構築した「サイバーセキュリティ対処調整センター」を、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（ナショナル CSIRT）として活用し、サイバーセキュリティの基本的な在り方でも掲げた「リスクマネジメント」の手法については、広く全国の事業者等に適用できるよう整備・普及を促進していく。

4.2.6 従来の枠を超えた情報共有・連携体制の構築

本来、サイバーセキュリティの確保は、保有する情報資産の価値、情報通信技術の利活用の状況等を踏まえ、各組織が自主的に取り組むものである。一方、攻撃態様の変化により、自組織のみでサイバー攻撃への効果的な対策を講じることには限界が生じてきている。このため、他の組織との連携を重視する意識が官民ともに着実に広がっており、行政機関や重要インフラ事業者に限らず、幅広い主体が情報共有に取り組

55 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)」（平成29年３月21日2020年東京オリンピック競技大会・パラリンピック競技大会関係府省庁連絡会議セキュリティ幹事会決定）

み始めている。

サイバー空間と実空間の一体化が進展し、サイバー空間と密接に関連する分野が一層増加する中、サイバーセキュリティに資する情報の共有に取り組むべき分野や関係者の範囲は、更に広がり続けることが予想される。

そのため、サイバーセキュリティの基本的な在り方で掲げた「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[56]を含む既存の情報共有における取組の推進を支援するとともに、新たな役割を果たしていく必要がある。

(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・分析や各主体との迅速な調整を担う役割の重要性が増している。一方で、共有した情報が適切に取り扱われず、社会的評価・信頼の低下を引き起こすおそれがあることから、自らが保有する情報の共有に各主体が積極的に取り組むことができないという課題がある。

これを踏まえ、情報共有に十分な知見を有する専門機関を含む官民の多様な主体が、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新たな体制を構築する。その際、基本原則に掲げる「自律性」の観点から、各々の主体の自主性を尊重することが重要である。このような取組を進めることで、官と民、業界、国内外といった枠を超えた情報の共有・連携を推進していく。

また、官民で既に複数組織されている情報共有体制において、関係者の更なる負担が生じることのないよう、各々の特色や役割を踏まえて、連携や統合について検討していく。

(2) 情報共有・連携の新たな段階へ

新たな情報共有体制を構築するに当たって、多様な主体が信頼関係を構築し、連携して積極的に情報提供に協力する者ほど恩恵を享受できる仕組みを検討していく。

他者との連携・協働のレベルが高まるほど、情報共有体制に参加するメリットが高まるため、まずは国から率先して自ら保有している情報を適切に提供していく。また、サイバーセキュリティインシデント等に係る、自ら保有する情報を積極的に提供する主体が評価される環境を整備していく。とりわけ、国民の生命・身体を保護するため、リコールの要因となるようなサイバーセキュリティに係る情報が迅速かつ確実に共有されることが不可欠である。さらに、寄せられる情報に対して、処理の自動化を推

56 Information Sharing and Analysis Centerの略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策に役立てられる。（出典：サイバーセキュリティ2017（平成29年８月25日））

進するなどして、適切かつ迅速な分析や、各々の主体が真に必要とする情報の共有を実現していく。

このような取組により、サイバー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していく。さらに、我が国の情報共有の仕組みを発展させつつ、国際社会との戦略的な連携を視野に入れることも肝要である。官民や業界といった従来の枠を超えて、各々の主体が共存・発展していくことのできる関係を構築できるよう、国は各主体と緊密に連携し、環境整備に積極的に取り組んでいくことで、サイバーセキュリティに関する情報共有・連携が新たな段階へ移行していく。

4.2.7 大規模サイバー攻撃事態等への対処態勢の強化

海外では、サイバー攻撃による大規模な停電や金融機関の一部機能停止といった事案が発生し、国民生活に多大な影響を与えている。サイバー空間と実空間の一体化が進展している中、我が国においても、実空間において発生する事案の原因がサイバー攻撃にあることも将来十分にあり得る。また、大規模なサイバー攻撃については、通常、関連性の薄い分野のサービスが同時多発的に被害を受けることも想定されるところであり、係る脅威から国民・社会を守るためには、国が一丸となってサイバー空間の脅威への危機管理にも臨む必要がある。

サイバー空間と実空間の双方の危機管理に臨むために、サイバー空間と実空間の横断的な対処訓練・演習を実施するとともに、当該訓練・演習を通じてサイバー攻撃への対処態勢の強化を図る。加えて、サイバー攻撃に関する分析に係る人材の育成や官民連携の枠組みを通じた情報共有、インターネット観測の高度化を推進し、サイバー空間における情報収集・分析機能及び緊急対処能力の向上を図る。

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

自由、公正かつ安全なサイバー空間は、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である。

全ての主体に開かれ、自律的で、自由な情報の流通が保障されたサイバー空間は、技術革新の源泉であり、民主主義の基盤である。サイバー空間は、産学官民の多様な関係者による技術革新や発明、取組を通じて発展してきた。国家による過度な統制は、サイバー空間の自律的・持続的な発展を阻害する。サイバー空間の健全な発展のためには、多様な主体の協力により、自由な情報の流通が確保され、開放的・自律的なサイバー空間を堅持する必要がある。

社会のあらゆる場面でサイバー空間の利用が加速的に進み、サイバー空間と実空間の一体化が進展することにより、人権、プライバシー、犯罪・テロ、国家安全保障など、実空間の問題が、サイバー空間に持ち込まれ、課題となっている。これら課題に対応し、安全・安心を確保するための取組をサイバー空間についても進める必要がある。サイバー攻撃は容易に国境を越え、また、国家の関与が疑われる事案も出てきているため、サイバー空間の安全・安定の確保のためには、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を進める必要がある。この際、サイバー空間の自律的・持続的な発展を阻害しないように留意しなければならない。

我が国は、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、既存の枠組みを活用し、我が国の安全を確保するための取組を行い、国際連携を進める。

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、国際場裡においてその理念を発信し、サイバー空間における法の支配の推進のため、積極的な役割を果たしていく。

(1) 自由、公正かつ安全なサイバー空間の理念の発信

我が国は、自律的・持続的に発展するサイバー空間のエコシステムを維持するため、情報の流通の規制などの国家による管理・統制ではなく、多様な主体が連携・協働してサイバーセキュリティの確保に取り組むことにより、サイバー空間の安全を確保することを目指す。

こうした日本型のサイバーセキュリティの基本的な在り方を国際場裡において発信するとともに、サイバー空間の発展を妨げるような国際ルールの変更等を目指す取組に対しては、同盟国・有志国、民間団体等と連携して対抗する。

この際、インターネットの資源管理に関する議論と、人権、プライバシー、犯罪・テロ、国家安全保障等のサイバー空間の利用に関して生じる問題についての議論は分けて考えなければならない。サイバー空間の利用に関して生じる問題については、既存の枠組みの存在を前提とした議論を進める必要がある。

(2) サイバー空間における法の支配の推進

国際社会の平和と安定及び我が国の安全保障のため、サイバー空間における法の支配を推進することが重要である。

サイバー空間においても、国際連合憲章を始めとする既存の国際法が適用される。我が国は、この立場から、既存の国際法の個別具体的な適用の在り方、規範の形成・普遍化についての議論に積極的に関与する。また、これまでに明らかにされた責任ある国家の行動規範[57]について、着実な履行・実践を通じ普遍化を進める。そうした規範を国際社会に広げ、国家実行を積み重ねていくことで、規範に反する行動を抑止する。

サイバー犯罪対策では、警察庁及び関係省庁が連携して、サイバー犯罪に関する条約、刑事共助条約、ICPO[58]等の枠組みを活用した国際機関、外国法執行機関、外国治安情報機関等との間における国際捜査共助や情報交換等による国際連携を更に推進する。

こうした取組により、法の支配を推進し、国際社会の平和と安定及び我が国の安全保障を実現する。

4.3.2 我が国の防御力・抑止力・状況把握力の強化

サイバー空間における安全保障を取り巻く環境は、厳しさを増している。政府機関、重要インフラ事業者、先端技術を有する企業・学術機関等への攻撃や、民主主義の根幹を揺るがしかねない事例も発生している。さらに、それらの中には国家の関与が疑われる事案も存在する。

以上の状況を踏まえ、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ことが重要である。

これら安全保障に係る取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は内閣サイバーセキュリティセンターを中心として官民を問わず全て

57 2015年第４会期国連サイバー政府専門家会合（UNGGE）報告書、2015年G20アンタルヤ・サミット首脳宣言、及び2017年サイバー空間における責任ある国家の行動に関するG７（ルッカ）宣言　等

58 International Criminal Police Organizationの略。国際刑事警察機構

の関係機関・主体、抑止は対応措置を担う省庁、状況把握は情報収集・調査を担う機関が、平素から緊密に連携して進める。また必要な場合には、国家安全保障会議で議論・決定を行う。

(1) 国家の強靭性の確保

① 任務保証

政府機関は、国民生活や経済社会を守り、支える任務を有しており、その機能停止は、安全保障上の重大な懸念事項である。政府機関の任務遂行は、重要インフラその他の社会システムを担う事業者のサービスに依存している。また、これら事業者自身も、国民や社会に不可欠なサービスを提供するという重要な任務を有している。

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、政府機関及び重要インフラ事業者等におけるサイバーセキュリティの確保を推進する。特に、防衛当局である防衛省・自衛隊においては、サイバー攻撃対処を行う部隊の能力を更に向上させ、自らの活動が依存するネットワーク・インフラの防護を引き続き強化するとともに、自衛隊の任務保証に関連する主体との連携を深化させていく。

② 我が国の先端技術・防衛関連技術の防護

先端技術は、経済的な優位性を保障するだけでなく、安全保障上も重要な国家的資産である。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人的要因によるリスク軽減も含めたサイバーセキュリティ対策を強化する。特に防衛産業が取り扱う技術情報等は、それが漏洩・流出した場合の我が国の安全保障上の影響が大きいため、安全な情報共有を確保する仕組みの導入、契約企業向けの新たな情報セキュリティ基準の策定、契約条項の改正等の取組を行う。これらについて、官民連携の下、下請け企業等を含めた防衛産業のサプライチェーン全体に適用することを前提とした検討を行う。

また、先端技術情報を保護する観点から、国立研究開発法人や先端的な技術情報を保有する大学等における対策を促進する。

③ サイバー空間を悪用したテロ組織の活動への対策

サイバー空間は、個人や団体が自由に情報をやり取りし、自らの考えを述べる場を提供するものであり、今や民主主義を支えているものの一つである。他方、テロ組織が、過激思想の伝播や示威行為、組織への勧誘活動、活動資金の獲得等の悪意ある目的でサイバー空間を利用することは防止しなければならない。このため、表現の自由を含む基本的人権を保障しつつ、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を国際社会と連携して実施する。

(2) サイバー攻撃に対する抑止力の向上

① 実効的な抑止のための対応

国際連合憲章を始めとする国際法は、サイバー空間において適用される。そして伊勢志摩サミットにおいてG7首脳が確認したとおり、一定の場合には、サイバー攻撃が国際法上の武力の行使又は武力攻撃となり得る[59]。また、G7ルッカ外相会合において確認したとおり、悪意のあるサイバー攻撃等武力攻撃に至らない違法行為に対しても、国際違法行為の被害者である国家は、一定の場合には、当該責任を有する国家に対して均衡性のある対抗措置及びその他の合法的な対応をとることが可能である[60]。

以上の認識を踏まえ、我が国は、悪意ある主体の行動を抑止し、国民の安全・権利を保障するため、国家の関与が疑われるものも含め、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、同盟国・有志国とも連携し、脅威に応じて、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる。

適切な対応を適時にとれるよう、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するとともに、法執行機関、自衛隊を始めとする関係機関の能力強化を進める。その際、悪意ある主体によるサイバー空間の利用を妨げる能力の保有の可能性についても視野に入れる。

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、国家間の信頼を醸成する。サイバー攻撃は、匿名性・隠密性が高いことから、意図せず国家間の緊張が高まり、事態が悪化するリスクがある。このように偶発的、不必要な衝突を防ぐため、国境を超える事案が発生した場合に備え、国際的な連絡体制を平素から構築しておくことが重要である。また、二国間・多国間の協議における情報交換、政策対話等を積極的に行うことを通じ、透明性を高め、国家間の信頼を醸成する必要がある。各国と協力し、サイバー空間の問題を調整するメカニズムについても検討する。

---

59 G7伊勢志摩サミット　サイバーに関するG7の原則と行動（2016年５月）「我々は、一定の場合には、サイバー活動が国際連合憲章及び国際慣習法にいう武力の行使又は武力攻撃となり得ることを確認する。また、我々は、サイバー空間を通じた武力攻撃に対し、国家が、国際人道法を含む国際法に従い、国際連合憲章第51条において認められている個別的又は集団的自衛の固有の権利を行使し得ることを認識する。」

60 サイバー空間における責任ある国家の行動に関するG７（ルッカ）宣言（2017年４月）「紛争の予防及び紛争の平和的解決のため、国際法が武力攻撃に至らない違法行為（悪意のあるサイバー活動を含み得る。）に対する国家の対応のための枠組みを提供していることに留意する。国際違法行為の被害者である国家は、一定の場合には、その違法行為について責任を有する国家に国際的な義務を遵守させるために、当該責任を有する国家に対して均衡性のある対抗措置（ICTを介して実施する措置を含む。）及びその他の合法的な対応をとることができる。」

(3) サイバー空間の状況把握の強化

① 関係機関の能力向上

深刻化するサイバー攻撃の脅威を抑止していくためには、対応力の強化に加え、攻撃者に責任を負わせるために、サイバー攻撃を検知・調査・分析する十分な能力が求められる。このため、関係機関の情報収集・分析能力を質的・量的に向上させる。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・分析等するための技術の開発・活用等あらゆる有効な手段について幅広く検討を進める。また、カウンターサイバーインテリジェンス[61]に係る取組を進める。

② 脅威情報連携

国の関与が疑われるサイバー攻撃、非政府組織等による攻撃等多様な脅威に的確に対処し、抑止するため、政府内関係省庁及び同盟国・有志国との国内外の情報連携が不可欠である。同盟国・有志国との間で、脅威情報の共有を推進する。また、内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。

4.3.3 国際協力・連携

サイバー空間においては、事象の影響が容易に国境を越えることから、海外で生じたサイバー事案は常に我が国にも容易に影響を及ぼす可能性がある。世界各国との政府・民間様々なレベルで協力・連携することにより、サイバー空間の安全を確保し、もって国際社会の平和・安定及び我が国の安全保障を図る。

このため、様々な国際的な議論に積極的に貢献し、サイバー問題に関する情報の共有や意識の統一に向けて取り組む。また、外国との知見・経験の共有を進め、具体的な協力・連携関係を構築し、実際の行動につなげる。また、国際場裡で我が国の立場を主張できる官民の人材を確保し、育成する。

(1) 知見の共有・政策調整

サイバーセキュリティに関する二国間の協議や国際会議を通じ、互いのサイバーセキュリティ政策や戦略、体制の情報交換を行い、我が国のサイバーセキュリティ政策立案に活かしていく。また、我が国とサイバーセキュリティに係る基本的な考え方を共有する戦略的パートナー国との二国間で、サイバーセキュリティ施策に関する協力・連携を強化する。

(2) 事故対応等に係る国際連携の強化

サイバー攻撃の情報や脅威情報を平時から共有し、事故発生時に連携対処できるよ

61 情報通信技術を用いた外国の敵意ある諜報活動に対抗する情報防衛活動

う、CERT[62]間連携を強化する。また、国際サイバー演習への参加や共同訓練等を通じて、連携対処能力の向上を図るとともに、事故発生時に適切に国際連携しながら対処する。

(3) 能力構築支援

国際的な相互依存関係が進む現在、我が国の平和と安全は我が国一国のみでは確保できない。我が国の安全保障の確保に寄与するためには、全世界的に連携してサイバーセキュリティ上の脆弱性を低減し、撲滅を目指していくことが肝要である。

このような観点から、世界各国におけるサイバーセキュリティの能力構築を支援することは、対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、当該国の健全なサイバー空間の利用の進展を促すのみならず、サイバー空間全体の安全の確保と直結しており、ひいては我が国を含む世界全体の安全保障環境の向上に資する。

2016 年に公表した基本方針[63]に基づき、様々な政策手段を活用し、開発途上国における能力構築支援を積極的に実施していく。

62 CERT (Computer Emergency Response Team)。コンピュータセキュリティインシデントに対応する活動を行う組織
63 「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月サイバーセキュリティ戦略本部報告）

4.4. 横断的施策

「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」の３つの政策目標を達成するためには、その基盤として、横断的・中長期的な視点で、人材育成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していくことが重要である。

4.4.1　人材育成・確保

「Society 5.0」の実現に向けて新たな価値が創出されていく中、サイバー攻撃の脅威は広がっており、一部の専門家がサイバーセキュリティの確保に取り組むのではなく、それぞれの役割を遂行する観点から、主体的に取り組むことが求められる。

こうしたパラダイムシフトにより生じる将来を見据えつつ、各々の組織の「任務」の遂行や個人の安全な利用を支える観点から、サイバーセキュリティの確保に取り組む各人材層において保有すべき知識や技術の水準を明確化することが求められる。その上で、教育等を通じ、資格・評価基準等によって可視化された確かな知識と実践力を備えた人材が、適切な処遇を受け、更に実務経験を積み重ねることにより、人材の需要と供給が相応されるといった好循環の形成が必要である。

このため、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・確保を強化していく。その際、イノベーションを推進する観点から、人材の多様性の確保を推進していくことが重要である。

(1)　戦略マネジメント層の育成・定着

企業経営においてサイバーセキュリティ対策を進めていくためには、それが単に技術的な課題にとどまらないことから、専門家や実務者任せにすることは適切ではない。経営層が示す経営戦略や事業戦略の下、組織がマネジメントすべき様々なリスクの一つとして、業務やサービス等を実現するために必要なサイバーセキュリティに係るリスクを認識し、事業継続と価値創出に係るリスクマネジメントを中心となって支える立場として、社内外の実務者・専門家を活用・指揮しつつ、対策や事案への対応を実践する役割を果たし得る人材が求められている。このため、こうした役割を担う層を「戦略マネジメント層」と位置付け、経営層の理解の促進を含め、産業界と連携しつつ、その定着を図る。

また、業種や業態によっては、文化や慣習などの違いにより、業務やサービス等を実現するための既存のマネジメントに対し、サイバーセキュリティ対策を組み込み、実践することに困難を伴う場合がある。このため、多様なビジネスとそのマネジメン

トの実態があることを踏まえつつ、戦略マネジメント層向けの実践的な教材の開発や、指導者の発掘・育成も含め、学び直しプログラムの実践を推進する。

(2)　実務者層・技術者層の育成

戦略マネジメント層が示す方針を踏まえ、システムの企画や構築・運用時における対策等を実践する実務者層や技術者層については、これまで官民において、教育プログラムや資格・試験、演習の実施などの様々な取組が行われてきた。

こうした知識や技術の水準を高める取組は、引き続き強化を図っていく必要があるが、実務者や技術者が戦略マネジメント層に対して貢献できるよう、日々進化する情報通信技術や制御システムの技術、これらに対するサイバー攻撃について理解を深めることはもとより、経営層の方針を理解しつつ、他の専門人材と円滑にコミュニケーションをとりながらチームの一員として対処ができるようにすることが重要である。このため、実務者層・技術者層向けの育成プログラムにおいては、戦略マネジメント層が示す概念的・抽象的な考えを理解し、それを具体化するとともに、様々な関係者と円滑なコミュニケーションができるような学び直しによるスキルの開発や実践的な演習が必要である。

さらに、突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保も引き続き行っていく。例えば、サイバー攻撃に対する防御方法、攻撃手法も含む対処法、情報を収集して分析評価を行う方法の体系化を含む研究を通じ、グローバルに切磋琢磨する機会を広げ、対策を検討できる能力の育成を引き続き推進する。

(3)　人材育成基盤の整備

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させる必要がある。このため、サイバーセキュリティや情報通信技術に関する基礎的な内容については、産学官が連携して、知識・技術体系やそれに基づくモデルカリキュラムの在り方の検討を行う。

また、サイバーセキュリティや情報通信技術について若年層の教育を強化するため、初等中等教育段階では、小学校段階から必修としたプログラミング教育など、発達の段階に応じてコンピュータなどの情報通信技術の原理や仕組みなどを理解し、プログラミング的思考といった論理的思考力を育てるなど、教育課程内で情報活用能力の育成に着実に取り組む。さらに、こうした情報活用能力の育成に関する履修項目が、教員養成課程において着実に盛り込まれるようにするとともに、教員の研修を充実させる。その際、必要に応じて産業界などの人材の活用も柔軟に進めることが重要である。加えて、近年、若年層によるサイバー犯罪が発生していることから、情報モラル教育

も重要な課題である。

さらに、将来、高度なサイバーセキュリティ技術を持つ人材となることが期待される若年層向けに、教育課程外の地域や企業・団体等において、産業界などの人材の能力を柔軟に活用しつつ、自由にサイバー関連ツール、機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備を進める必要がある。同時に、こうした自己実現の環境整備は、倫理教育と併せて実施することで、若年層による興味本位のサイバー犯罪などの防止に効果があると考えられる。また、産学官連携により、大学・高等専門学校等の高等教育段階における情報技術人材の育成を引き続き推進する。

(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

政府機関における統一的な方針に基づき、セキュリティ対策を専任で担う「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、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。各府省庁の人材確保・育成計画に基づき、定員の増加による体制整備、レベルに応じて知識・能力を高められる研修や高度なセキュリティ技術者を活用した演習、適切な処遇の確保等について、着実に取り組むとともに、毎年度、計画の見直しを行い、一層の取組の強化を図る。

(5) 国際連携の推進

サイバーセキュリティの問題への対応がグローバルな規模で求められていることを踏まえ、我が国のサイバーセキュリティ人材の育成においても、国内で完結するのではなく、可能な限りグローバルな規模で切磋琢磨できるようにすべきである。このため、人材育成に取り組む大学や公的機関等のプログラムについて、国際的な基準に照らして一定の基準があると認められるものを認定し、共同演習の実施や単位互換の認定など海外の人材育成を行う組織との間での様々な連携を促すための仕組み作りを主要国との連携の下で進める。

加えて、海外におけるサイバーセキュリティ人材育成にも貢献をするため、我が国におけるサイバーセキュリティの人材育成等によって得られた知見を活かし、海外におけるサイバーセキュリティ人材の能力構築に貢献する。

4.4.2 研究開発の推進

サイバー空間と実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が必要である。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。

(1) 実践的な研究開発の推進

IoT、AI など様々な情報通信技術の組合せによって革新的製品やサービスの創出が期待されている。高いレベルのセキュリティ品質を備えた安全・安心な製品やサービスを提供していくことは、我が国の産業の成長、国際競争力の向上を目指していく上で不可欠である。

一方で、こうした技術の活用は、これまでになかった新たな脆弱性を生む可能性がある。このため、AI、ブロックチェーンなどの先進的な技術を用いたサイバーセキュリティ確保の技術、製品・サービスを構成するシステムの中に組み込むセキュリティ技術や、その組み込みの方法に関する実践的な研究開発について重点的に取り組む。特に、サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発を進めるほか、機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発を行う。

また、我が国が、サイバー攻撃に対する検知・解析能力を含むサイバー空間の状況把握能力を高め、防御等の対処能力や強靭性の確保等サイバー空間における安全保障の確保にも資する研究開発を推進する。具体的には、政府機関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、攻撃活動を把握することや、ネットワーク上の脆弱な IoT 機器の調査のための広域ネットワークスキャンの軽量化を目指した研究開発等を進める。こうした研究開発の実施においては、セキュリティを運用する現場のサイバー攻撃に関する知見をいち早く共有することによって、その知見を研究開発に活かすとともに、研究開発の成果をいち早くセキュリティを運用する現場で活かすといった好循環のサイクルを形成することが重要である。このため、セキュリティ運用を行う事業者と、国の研究機関等とのリアルタイムでの情報共有を推進する。

さらに、政府機関や重要インフラ事業者等のシステムに組み込まれている機器やソフトウェアについて、必要に応じて、不正なプログラムや回路が仕込まれていないことを検証できる手段を確保することが重要である。このため、国が中心となって、必要な技術的検証を行うための体制の整備を図るとともに、そのために必要となる研究開発に取り組む。加えて、計算機技術の発展（例：量子コンピュータ、AI）を意識した暗号技術など安全保障の観点から国として維持することが不可欠な基盤技術についても研究開発を推進する。

加えて、これらの技術的な研究開発にとどまらず、例えば、サイバーセキュリティに関する法令解釈の明確化等、サイバーセキュリティ対策における制度上の課題に関

する調査・研究を推進する。

これらのサイバーセキュリティの研究開発の取組については、その成果の普及や社会実装を推進する。また、海外のイベント等への積極的な参加等を通じ、国際的な情報発信を行いつつ、我が国と基本的な価値観を共有する有志国との間で、共同研究の実施や研究成果の国際標準化等の研究開発に係る官民の国際連携の強化を図る。

(2) 中長期的な技術・社会の進化を視野に入れた対応

サイバー空間と実空間が一体化していく中、AI や VR といった情報通信技術の進展によって、個々人の異なる価値観を承認しながら、多様な体験を、それらが形成されるプロセスを含めて共有することが実現できるようになってきている。こうした技術が人間にもたらす大きな変化の中で、中長期的には、現在の社会システムや倫理の常識が未来において根本的に変化し、これまでの技術進歩を外挿して、サイバーセキュリティの研究開発を考えるアプローチには限界が来る可能性がある。新しい価値を創出していくためには、サイバー空間と実空間との一体化が進む現状から将来を見据え、行為主体としての人間を含むエコシステムとの視点から社会全体を設計していくような新しいアプローチが必要となっていくことが考えられる。このため、中長期を視野に入れて、サイバーセキュリティと、法律や国際関係、安全保障、経営学等の社会科学的視点、さらには、哲学、心理学といった人文社会学的視点も含めた様々な領域の研究との連携、融合領域の研究を促進する。その際、科学技術を始め各種研究開発の成果が人間社会に悪影響を及ぼすものであってはならないということは言うまでもない。

4.4.3 全員参加による協働

スマートフォンを始めとする端末や公衆無線 LAN の普及によって、国民一人一人が、サイバー空間につながり、多大な恩恵を享受している。IoT の進展によって、今後、その動きは加速していく。一方で、サイバー攻撃の脅威が広がる中、安全・安心にサイバー空間を利用していくためには、実空間における防犯対策や交通安全対策と同様に、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対する意識・理解を醸成し、サイバー空間における様々なリスクに対して対処できることが不可欠になっている。

サイバーセキュリティに対する意識・理解を広く醸成していくためには、国による従来の普及啓発の取組だけでは限界がある。むしろ、国は、地域、企業、学校など様々なコミュニティの自主的な活動を尊重しつつ、各々の関係者が、お互いの役割分担の下で、連携・協働をできるような仕組みを構築し、その仕組みを下支えしていくというかたちでリーダーシップを発揮していく必要がある。

このため、内閣サイバーセキュリティセンターが中心となって、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、国は、サイバーセキュリティの普及啓発に向けた総合的な戦略及び具体的なアクションプランを策定するとともに、必要な情報発信や国民からの相談対応を行う。また、産学官民の様々なコミュニティの代表が参加する協議会の場を活用しながら、関係者による実践を推進していく。さらに、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的期間として、「サイバーセキュリティ月間」の更なる充実を図るとともに、国民向けのわかりやすい解説書の作成・普及や、学校教育での情報活用能力の育成を通じて、サイバーセキュリティについての教育を推進する。

スマートフォンやパソコン等の機器の製造・販売事業者、通信キャリアやインターネットサービスプロバイダー等の通信事業者は、セキュリティに配慮した製品・サービスの提供や、利用者への説明、相談への対応などを通じて、利用者がサイバーセキュリティの取組を適切に実施できるよう対応することが期待される。このため、国においては、必要に応じて、これらの事業者や関係団体等の取組が促進される環境を整備するとともに、利用者のニーズや利用形態等を踏まえつつ、サイバーセキュリティの確保に資するガイドラインの整備とその着実な実施を推進する。

5. 推進体制

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[64]し、経済・社会活動の基盤とする[65]こと、我が国の安全保障を万全のものとする[66]ことは、従来からの我が国政府の方針である。この方針の下、政府においては、関係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することが肝要である。このため、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、同センターにおいては、本戦略に基づく諸施策が着実に実施されるよう、本戦略を国内外の関係者に積極的に発信しつつ、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ものとする。また、危機管理対応についても一層の強化を図る必要がある。とりわけ、2020 年東京大会を控える中、産学官民における参加・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である。

本部は、サイバーセキュリティに関する重要事項については高度情報通信ネットワーク社会推進戦略本部と緊密な連携により対応する。加えて、必要に応じて、重大テロ対策本部など危機管理体制と情報共有・連携する。さらに、本部は安全保障に関わる問題については国家安全保障会議との緊密な連携により対応し、内閣官房国家安全保障局による全体取りまとめの下、関係省庁が連携して対応する。

また、本部は、本戦略で示された方向性に基づき、各府省庁の施策が着実かつ効果的に実施されるよう、経費の見積もり方針を定め、政府としての必要な予算の確保と執行を図る。さらに、情報収集・分析機能の強化や、サイバー攻撃の速やかな検知・分析・判断・対処を一体的サイクルとして行う機能を有する体制の整備に向けて、官民連携を促進する。

今後、本部は、本戦略を的確に実施するため、３年間の計画期間内において、別紙の担当府省庁一覧を含む各年度の年次計画を作成するとともに、各府省庁はこれに基づき施策を着実に実施する。また、本部はその施策の進捗状況を検証して、年次報告として取りまとめ、次年度の年次計画へ反映することとする。さらに、サイバー空間に係る情勢や技術動向が非連続的に変化することもあり得ることから、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することとする。

64　世界最先端IT国家創造宣言・官民データ活用推進基本計画（平成29年５月30日閣議決定）は、「データ利活用の促進に当たっては、個人情報やプライバシーの保護、サイバーセキュリティ対策、知的財産権の在り方、データの品質や信頼性・安全性の確保、AI、ロボット時代の倫理の在り方など、同時並行的に対策を講じておくことは言うまでもない」としている。

65　未来投資戦略2017は、「あらゆる場面で快適で豊かに生活できる超スマート社会、Society 5.0では、安全なサイバー空間の確保が経済・社会活動の重要な基盤」としている。

66　国家安全保障戦略（平成25年12月17日閣議決定・国家安全保障会議決定）は、「情報の自由な流通による経済社会やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠」としている。

別紙

担当府省庁一覧（注）

項目	担当府省庁 （◎：主担当、○：関係府省庁）
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[67]、経済産業省 ○：金融庁
(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
(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
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
(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）
(3)　中小企業の取組の促進	◎：NISC、総務省、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
(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
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）
(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

67　National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015年１月９日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長には、内閣官房副長官補（事態対処・危機管理担当）を充てている。

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
(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
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
(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
(3)　先端技術の活用による先取り対応への挑戦	◎：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
(5)　組織的な対応能力の充実	◎：NISC、総務省 ○：人事院
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
(2)　大学等の連携協力による取組の推進	◎：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
(2)　未来につながる成果の継承	◎：NISC、警察庁、総務省、法務省
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
(1)　多様な主体の情報共有・連携の推進	◎：NISC
(2)　情報共有・連携の新たな段階へ	◎：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
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
(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
(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
4.3.2　我が国の防御力・抑止力・状況把握力の強化	
(1)　国家の強靭性の確保	◎：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
(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

(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
4.3.3 国際協力・連携	◎：NISC ○：その他の府省庁
(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
(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
(3) 能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省
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
(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
(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
(3) 人材育成基盤の整備	◎：総務省、文部科学省、経済産業省
(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
(5) 国際連携の推進	◎：NISC、経済産業省
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）
(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
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
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）

注：2018 年度の年次計画に基づいた担当府省庁の一覧であり、次年度以降、新たな年次計画が本部決定された時点から、これに代わり、同計画の担当府省庁一覧が効力を生ずるものとする。

資料１－７

サイバーセキュリティ２０１８（案）

2018 年　月　日

サイバーセキュリティ戦略本部

目　次

はじめに 1

1.　経済社会の活力の向上及び持続的発展 2

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 2
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 4
1.3.　安全な IoT システムの構築 6

2.　国民が安全で安心して暮らせる社会の実現 9

2.1.　国民・社会を守るための取組 9
2.2.　官民一体となった重要インフラの防護 12
2.3.　政府機関等におけるセキュリティ強化・充実 17
2.4.　大学等における安全・安心な教育・研究環境の確保 21
2.5.　2020 年東京大会とその後を見据えた取組 22
2.6.　従来の枠を超えた情報共有・連携体制の構築 23
2.7.　大規模サイバー攻撃事態等への対処態勢の強化 25

3.　国際社会の平和・安定及び我が国の安全保障への寄与 27

3.1.　自由、公正かつ安全なサイバー空間の堅持 27
3.2.　我が国の防御力・抑止力・状況把握力の強化 28
3.3.　国際協力・連携 32

4.　横断的施策 36

4.1.　人材育成・確保 36
4.2.　研究開発の推進 40
4.3.　全員参加による協働 43

5.　推進体制 46

参考 1　用語解説 47

参考 2　担当府省庁一覧 56

はじめに

本書は、我が国のサイバーセキュリティ政策に関する国家戦略であり、今後閣議決定する予定の次期「サイバーセキュリティ戦略」（以下「2018年戦略」という。）に基づく最初の年次計画である。

自由、公正かつ安全なサイバー空間を創出・発展させ、もって「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」に寄与することを目的として、政府が2018年度に実施する具体的な取組を戦略の体系に沿って示すものである。

本書に示す取組を推進するに当たっては、政府機関における連携は元より、重要インフラ事業者や企業、個人といった多様な主体とも連携しつつ、取組を推進していく。

なお、本書は、2018年戦略が閣議決定された時点から効力を生じるものとする。また、本書の記載にかかわらず、我が国を取り巻くサイバーセキュリティに関する情勢に変化が生じた場合には、その内容に応じて、必要な範囲で迅速に相応の取組を策定・実施することとする。

1. 経済社会の活力の向上及び持続的発展

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

- 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による、経営層の意識改革
- 対策の可視化など、経営層に訴求するための施策の推進
- 企業が参照すべき法制度に関する整理

（2018 年戦略より）

(ア)内閣官房において、2016年に決定した「企業経営のためのサイバーセキュリティの考え方」及び2018年に決定した「サイバーセキュリティ人材育成取組方針」を踏まえ、関係府省庁と協力し、サイバーセキュリティ対策の推進に関する以下の取組を行う。

- サイバーセキュリティ対策について経営層が果たすべき役割、持つべき認識についての考え方の共有を図るため、「企業経営のためのサイバーセキュリティの考え方」の見直しを検討する。
- サイバーセキュリティ対策の取組を分かりやすく表現・普及するため、マークやスローガンなどのツールについて検討を行う。
- サイバーセキュリティ対策に関して、経営層が果たすべき役割・認識について、経営層の視点で、経営層自身に分かりやすく説明する人材、いわゆる伝道師の発掘と派遣や産業界と連携した経営層向けのセミナーについて検討を行う。

(イ)経済産業省において、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、コーポレート・ガバナンス・システムに関するガイドラインのとりまとめに向け、サイバーセキュリティを位置付けることを検討する。

(ウ)経済産業省において、取締役会のサイバーセキュリティへの関与を促すとともに、投資家に対するサイバーセキュリティの啓発を行う観点から、上場企業において行われる「取締役会の実効性評価」の評価項目について、サイバーセキュリティへの経営層の関与をその評価項目として組み込むことを促進する。

(エ)経済産業省において、経営層がサイバーリスクを経営上の重要課題として把握し、設備投資、体制整備、人材育成等経営資源に係る投資判断を行い、組織能力の向上を図るために、説明会等を通じて、「サイバーセキュリティ経営ガイドライン」の普及を図る。

(オ)内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う。

(2) サイバーセキュリティに対する投資の推進

- 企業の積極的な情報発信・開示に向けたベストプラクティスの共有やガイドラインの策定
- 情報発信・開示の状況についての継続的な把握・評価
- 投資家が企業経営層のサイバーセキュリティに関する取組を評価できるような仕組みづくり
- 企業に対するサイバーセキュリティの促進策のフォローと措置の検討
- サイバーセキュリティ保険の活用を推進するための方策についての検討

（2018 年戦略より）

（ア）経済産業省において、「サイバーセキュリティ経営ガイドライン」の実践的な定着を図るために、具体的な対策事例や情報共有活動事例等を示すプラクティスを作成する。また、企業がどの程度サイバーセキュリティ対策を実施するかの目安として活用できる可視化ツールを作成する。

（イ）総務省において、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、公表する。

（ウ）経済産業省において、一定のセキュリティ品質を有するセキュリティサービスを審査登録する体制を整備することにより競争力強化や活用促進を図るなど、サイバーセキュリティの成長産業化に取り組む。

（エ）総務省及び経済産業省において、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により生産性を向上させる取組について、それに必要となるシステムやサイバーセキュリティ対策製品等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の活用を促すことで、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する。

（オ）経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る。

（カ）総務省において、サイバーセキュリティ保険も活用した、関係者間のセキュリティに関する情報開示・共有を促進するためのモデル事業について検討を行う。

(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

- 先端技術の利用に伴うサイバーセキュリティリスクの分析・明確化とそれに基づくガイドラインの策定や普及等
- 先端技術のリスク分析や脅威への対策に係る研究開発の推進
- セキュリティ・バイ・デザインの考え方を基本とした取組
- 先端技術の利用を支えるためのサイバーセキュリティ技術・サービスの供給者とのマッチング、サイバーセキュリティ技術・サービスの適切な評価に係る仕組みの構築
- 我が国の高いサイバーセキュリティが確保されたモノやサービス等のトップセールスや展示会等を活用したアピール、国際展開をしやすいビジネス環境の整備

（2018 年戦略より）

(ア)経済産業省において、IPAを通じ、営業秘密保護に関する対策等を推進するため、組織における内部不正防止のためのガイドラインや営業秘密保護ハンドブックの普及推進を図る。

(イ)経済産業省において、企業の情報漏えいの防止に資するため、「秘密情報の保護ハンドブック～企業の価値向上に向けて～」及び「秘密情報の保護ハンドブックのてびき～情報管理も企業力～」についての普及啓発を図る。

(ウ)総務省及び経済産業省において、「クラウドサービス提供における情報セキュリティ対策ガイドライン」、クラウドセキュリティ監査制度等の普及促進を行う。

(エ)経済産業省において、IPAを通じ、サイバーセキュリティビジネスの振興・活性化を図るため、サイバーセキュリティ対策におけるニーズの明確化・具体化、シーズの発掘やビジネスマッチングを行うメンバーを限定しない情報交流の場（コラボレーション・プラットフォーム）を設置する。

(オ)経済産業省において、日本のセキュリティニーズに応じた日本発のサイバーセキュリティ製品・サービスの創出・活用を推進するため、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を整備するための検討を行う。

(カ)経済産業省において、IPAを通じ、組込みソフトウェア産業の抱える課題、開発技術動向、人材育成状況などの実態と動向を把握するための調査・分析を行うとともに、組込みソフトウェアが組み込まれた製品やシステム開発の高信頼化を目的として、システムアプローチによる安全性解析手法の開発・セキュリティ分析手法の検討、コーディング規約策定及びそれらの普及を図る。

(キ)経済産業省において、ASEANをはじめとした新興国に対し、電力をはじめとした重要インフラ分野におけるサイバーセキュリティに関する意識啓発、知見・能力の構築支援を通じて、日本製のセキュリティを備えた質の高いインフラ輸出に向けた環境整備を行う。

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

- サプライチェーンにおいて、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の策定
- IoT 機器や組織等に求められる具体的な対応策の産業分野毎の提示

（2018 年戦略より）

(ア)経済産業省において、産業サイバーセキュリティ研究会の下に設置したWG1(制度・技術・標準化)において、Society5.0の実現に必要なセキュリティ対策を示す「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定する。また、産業分野毎に設置したSWGにおける検討を通じて、産業分野毎に守るべきもの・リスク・必要な対策について整理する。

(イ)経済産業省において、情報システム開発・運用に係るサプライチェーン全体のセキュリティ向上のため、リスクの高い丸投げ下請や多様化するセキュリティ対策費用の増加に応じた適切な価格設定に向け、セミナー等を通した下請ガイドラインの更なる浸透を図るとともに、業界団体と連携したフォローアップなどを実施し、情報システム開発・運用に係る取引の適

正化を図る。

(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

- 要件の確認等による信頼を創出する仕組みの構築
- 信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築
- トレーサビリティを確認するための仕組みと、創出された信頼そのものに対する攻撃を検知・防御するための仕組みの検討

（2018 年戦略より）

(ア)内閣府において、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、社会全体の安全・安心を確立するため、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を推進する。本プロジェクトでは、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、業務データを安全に流通させるためのトレーサビリティ確保技術、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。また、本プロジェクトが目指す『サイバー・フィジカル・セキュリティ対策基盤』の実現には、様々な産業分野が関係することから、総務省、経済産業省をはじめとした府省庁及び産学とが分野横断的に連携して推進する。

(イ)経済産業省において、業界横断的な指針及び産業ごとの対策を整理した上で、セキュリティ対策が講じられているかどうかを確認するための、認証を含む確認の仕組みを検討する。

(3) 中小企業の取組の促進

- 中小企業を対象としたサイバーセキュリティ対策の事例集の作成
- サイバーセキュリティ保険の活用促進
- 中小企業がサイバーセキュリティに関するトラブル等について相談できる仕組みの強化
- 中小企業が自主的に宣言できる仕組みなどの可視化の取組促進、インセンティブの仕組みとの連携

（2018 年戦略より）

(ア)内閣官房において、中小企業における実態を踏まえつつ、ITやセキュリティの知識がなくとも理解できるような対策集の作成に向けた取組を行う。

(イ)総務省において、サイバーセキュリティ保険も活用した、関係者間のセキュリティに関する情報開示・共有を促進するためのモデル事業について検討を行う。（再掲）

(ウ)経済産業省において、中小企業のサイバーセキュリティ対策の促進を図るため、身近な相談窓口の整備等の支援体制の強化を検討するとともに、サイバーセキュリティ保険の普及を図る。（再掲）

(エ)経済産業省において、営業秘密保護や事業継続性の観点からも経営層がサイバーリスクを重

要課題として把握し、人材育成等経営資源に係る投資判断を行い、組織能力の向上を図るために、説明会等を通じて、「サイバーセキュリティ経営ガイドライン」の普及を図る。またIPAを通じて、中小企業における情報セキュリティ対策の実施を促すため、説明会等において「中小企業の情報セキュリティ対策ガイドライン」の普及を図る。

(オ)中小企業における情報セキュリティ投資を促進するため、経済産業省において、以下の取組を実施する。

- 中小企業等の生産性向上に資するIT導入の促進とあわせて、セキュリティに係る意識向上やその対策に向けた具体的な取組を促す。
- 認定されたITベンターに対してサイバーセキュリティの情報提供などを実施するとともに、当該ITベンダーが取り組むセキュリティ対策に関する情報を中小企業向けに開示する仕組みの構築を進める。
- 財政投融資制度において、中小企業で導入が進んでいないネットワークセキュリティの更なる普及促進に向けて、特別利率による融資を実施する。

(カ)経済産業省において、IPAを通じ、中小企業における情報セキュリティ教育担当者や中小企業を指導する立場にある者等を対象とした「中小企業情報セキュリティ講習講師養成セミナー」を実施するとともに、中小企業団体、関係機関等との連携により、当該団体等が主催する情報セキュリティ対策セミナーに協力する取組を実施する。さらに、IPAが2017年度に創設した、対策ガイドラインに基づき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で、中小企業のセキュリティレベルの向上、IPA等の作成する啓発資料や情報セキュリティ対策支援サイト等のツール等の利用促進等を図る。

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

- 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の、協働した取組の推進
- 官民の各主体が抱える課題やそれぞれの取組の可視化と情報共有を行うための仕組みの構築
- 安全な IoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組

（2018 年戦略より）

(ア)内閣官房において、IoTシステムに係る新規事業がセキュリティ・バイ・デザインの考え方に基づき取り組まれるよう、経費の見積もりの方針にこうした考え方を盛り込むとともに、各府省庁等において、こうした考え方に基づく取組が行われるよう働きかけを引き続き行う。さらに着実にこの考え方に基づく取組が行われているか適時確認をする。

(イ)内閣官房において、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。その際、各主体の間で共通認識や役割の明確化を図るため、「安全なIoTシステムのためのセキュリティに関する一般的枠組」を踏まえた取組(IoTの分野個別の課題だけでなく、その範囲や定義、物理安全対策、責任分界点（既知の脆弱性への対応に関する製造者責任や運用者等の安全管理義務などインシデント発

生時における関係者の責任を含む）やプライバシーの問題などの共通課題の検討を含む。）を推進する。

（ウ）安全なIoTシステムの構築に向けて、総務省及び経済産業省において、以下の取組を実施する。

- 総務省及び経済産業省において、専門機関と連携し、情報セキュリティ分野の国際標準化活動であるISO/IEC JTC1/SC27、ITU-T SG17等が主催する国際会合等に参加し、我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえて国際標準化を推進する。
- 総務省及び経済産業省において、IoT推進コンソーシアムを通じて、IPA及びNICTと連携しつつ、「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に反映させるべく、普及展開に努めるとともに、IoTセキュリティに関する研究開発、実証実験及びIoTセキュリティの確保に向けた総合的な対策の実施を通じ、IoT製品やシステムにおける「セキュリティ・バイ・デザイン」の国際的展開に向けた活動を行う。
- 経済産業省において、IPAを通じて、「IoTセキュリティガイドライン」の考え方の基本となった「つながる世界の開発指針」、又はその他関連ガイド等を様々な産業分野や団体の標準仕様等に反映させるべく、引き続き提案活動を実施する。また「IoTセキュリティガイドライン」を基本とする考え方の国際標準化に向けた取組を進める。
- 経済産業省において、産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下に設置したスマートホームSWG（一般社団法人電子情報技術産業協会スマートホームサイバーセキュリティWG）の場を活用して、家電など家庭で使われるIoT機器のサイバーセキュリティの確保のための必要な対策について、関連する事業者と連携しながら検討を進める。

（エ）内閣官房において、IoTシステムの設計・開発・運用に係る概念について、国内で官民が連携してモノ・ネットワーク、システム等に関する各種基準等への組込みを促進するため、情報技術に関わる国際標準化を担うISO/IECの分科委員会にて2017年11月に日本が提案した「安全なIoTシステムのためのセキュリティに関する一般的枠組」を基本とした国際規格案の標準化に向け、積極的に取り組む。

(2) 脆弱性対策に係る体制の整備

- IoT 機器に必要なサイバーセキュリティに関する要件の整理と、その要件を満たす IoT 機器の利用の推奨
- 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
- 我が国の対策をモデルとして、国際的な連携や標準化等を通じて海外に展開し、安全なネットワークの環境整備に貢献

（2018 年戦略より）

（ア）内閣官房及び関係省庁において、サイバー環境をよりクリーンなものに保つため、官民が連携して「ボット撲滅」に向けた体制を構築し対策を推進するための検討を行う。

（イ）総務省及び経済産業省において、IoT推進コンソーシアムを通じて、IPA及びNICTと連携しつつ、「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に反映させるべく、普及展開に努める。

（ウ）総務省において、NICTを通じ、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。また、「IoTセキュリティ総合対策」を踏まえ、2018年度中にIoT機器に対する脆弱性対策に関する実施体制を整備する。

2. 国民が安全で安心して暮らせる社会の実現

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

・ 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」の推進
（2018 年戦略より）

(ア)経済産業省において、経済産業省告示に基づき、IPA（受付機関）とJPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度を着実に実施するとともに、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）などを通じて、脆弱性関連情報をより確実に利用者に提供する。さらに、能動的な脆弱性の検出とその調整に関わる取組を行う。また、海外の調整機関や研究者とも連携し、国外で発見された脆弱性について、国内開発者との調整、啓発活動をJPCERT/CCにおいて実施する。

(イ)経済産業省において、情報システム等がグローバルに利用される実態に鑑み、IPA等を通じ、脆弱性対策に関するSCAP、CVSS等の国際的な標準化活動等に参画し、情報システム等の国際的な安全性確保に寄与する。

(ウ)経済産業省において、JPCERT/CCを通じて、ソフトウェア等の脆弱性に関する情報を、マネジメントツールが自動的に取り込める形式で配信する等、ユーザー組織における、ソフトウェア等の脆弱性マネジメントの重要性の啓発活動及び脆弱性マネジメント支援を実施する。

(エ)経済産業省において、IPAを通じ、情報システムの脆弱性に対して、プロアクティブに脆弱性を検出する技術の普及・啓発活動を行う。

(オ)経済産業省において、フィッシング対策協議会及びJPCERT/CCを通じて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等を実施する。

(カ)経済産業省において、IPAを通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。また、各種セミナーやイベントで利用方法を紹介することにより「icat」の普及を図る。

(キ)経済産業省において、IPAを通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。

(ク)経済産業省において、IPAを通じ、ウェブサイト運営者や製品開発者が脆弱性対策の必要性及び対策手法等を自ら学習することを支援するため、「安全なウェブサイトの作り方」を引き続き公開するとともに、体験的かつ実践的に学ぶツール「AppGoat」についてセミナー等を開催することで更なる普及啓発を図る。

(ケ)経済産業省において、JPCERT/CCを通じて、ソフトウェア製品や情報システムの開発段階において、製品開発者が情報セキュリティ上の観点から配慮すべき事項を、解説資料やセミナーの形で公開し、普及を図る。

(コ)総務省において、高度化・巧妙化するマルウェアの被害を防止するため、「ICT-ISAC」が中心となって実施している、マルウェアに感染した端末が不正サーバと通信しようとする場合に、当該通信を遮断することで、被害を未然に防止するなどの取組（ACTIVE）を促進する。

(サ)総務省において、2018年５月に成立した電気通信事業者間のサイバー攻撃に関する情報共有の促進のための制度整備を含む「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」を踏まえ、その施行に向けた省令等の整備を行う。

(シ)総務省において、いわゆる「なりすましメール」への技術的対策の一つである送信ドメイン認証技術（SPF、DKIM、DMARC等）の普及を図る。

- サービスの全体の基盤となる信頼できる情報インフラの整備の促進
- 仮想通貨交換業者との連携及び対応の推進
- 自動運転車やドローンに関するセキュリティ対策の推進

（2018 年戦略より）

(ス)内閣官房、総務省及び経済産業省において、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を評価するとともに、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行う。

(セ)重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、国際海底ケーブル等の情報インフラ設備の物理的セキュリティや機器の特性（使用期間等）も考慮しつつ、継続的に安全基準等を改善する。加えて、内閣官房及び重要インフラ所管省庁は、情報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必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化すること、人的要因によるリスク軽減の在り方の検討など、制度的枠組みを適切に改善する取組を継続的に進める。内閣官房は、重要インフラ事業者等における安全基準等の浸透状況等及び重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。

(ソ)金融庁において、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、認定された自主規制団体との意見交換等を通じて、実効性ある自主規制機能の確立を促していく。

(タ)国土交通省において、独立行政法人自動車技術総合機構交通安全環境研究所と連携し、自動車の安全基準の国際調和等を審議する唯一の場である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議長国として主導するとともに、基準適合性に係る審査体制の構築を図る。

(チ)経済産業省及び国土交通省において、自動運転車両外部からの通信が車内ネットワークにつながることによるサイバーセキュリティリスクへの対応に向けて、2018年度中に車両内の電子システムを模擬した評価環境（テストベッド）を構築し、2019年度以降、人材育成等に活用する。

(ツ)内閣府SIP（戦略的イノベーション創造プログラム）を中心に、経済産業省、総務省をはじめとする関係省庁と連携し、2017年度に作成したセキュリティ評価ガイドライン案を踏ま

え、実証実験を実施する。

(テ)様々な用途への活用が進むドローンのサイバーセキュリティについて、内閣官房及び関係省庁等による「小型無人機に係る環境整備に向けた官民協議会」等の場において、「空の産業革命に向けたロードマップ2018～小型無人機の安全な利活用のための技術開発と環境整備～」(2018年６月小型無人機に係る環境整備に向けた官民協議会決定）に基づき、空の産業革命に向けた総合的な検討の一環として論点整理を行う。

(2) 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
- 官民が連携したサイバー犯罪対策の推進
- サイバー空間における事後追跡可能性の確保に必要な取組の実施

（2018 年戦略より）

(ア)警察庁及び都道府県警察において、教育機関、地方公共団体職員、インターネットの一般利用者等を対象として、情報セキュリティに関する意識・知識の向上、サイバー犯罪による被害の防止等を図るため、サイバー犯罪の現状や検挙事例、スマートフォン等の情報端末やSNS等の最新の情報技術を悪用した犯罪等の身近な脅威等について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施する。さらに、関係省庁との連携によるスマートフォンに関する青少年に対する有害環境対策の徹底等、スマートフォンの安全利用のための環境整備に向けた取組を実施する。

(イ)警察庁、総務省及び経済産業省において、不正アクセス行為の禁止等に関する法律に基づき、不正アクセス行為、フィッシング行為、他人の識別符号を不正に取得・保管する行為等の取締りを強化するとともに、事業者団体に対する不正アクセス行為の手口に関する最新情報の提供や、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況の公表等を通じ、不正アクセス行為からの防御に関する啓発及び知識の普及を図るなど、官民連携した不正アクセス防止対策を更に推進する。

(ウ)警察庁において、サイバー防犯ボランティアの結成を促すとともに活動の支援を強化することにより、安全で安心なインターネット空間の醸成に向けた取組を推進する。

(エ)警察庁において、警察大学校サイバーセキュリティ対策研究・研修センターを通じ、サイバー犯罪等の取締りのための情報技術の解析に関する研究及びサイバー犯罪等の取締りに必要な専門的知識・技術に関する研修を実施する。

(オ)警察庁において、高度な情報通信技術を用いた犯罪に対処するため、情報技術の解析に関する資機材の強化、関係会合への参加、技術協力を通じた関係機関との協力、不正プログラムの解析等を推進する。また、警察大学校サイバーセキュリティ対策研究・研修センターを通じ、新たな電子機器や技術に係る解析手法の確立に向けた研究を推進する。

(カ)法務省において、検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査・公判上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査・公判能力の充実を図る。

(キ)検察当局及び都道府県警察において、サイバー犯罪に適切に対処するとともに、サイバー犯

罪に関する条約を締結するための「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）の適正な運用を実施する。

(ク)総務省において、NICTを通じ、能動的・網羅的なサイバー攻撃観測技術の開発に取り組むとともに、運用するサイバー攻撃観測網（NICTER）における観測・分析結果をNISCをはじめとする政府機関等への情報提供等を通じた連携強化を図る。

(ケ)経済産業省において、産業界及び関係省庁と連携し、企業情報の漏えいに関して、サイバー攻撃など今後ますます高度化・複雑化が予想される最新の手口や被害実態などの情報の共有を行う場として、「営業秘密官民フォーラム」を開催するとともに、参加団体等に営業秘密に関するメールマガジン「営業秘密のツボ」を配信し、判例分析や逮捕情報等に関する情報共有を行う。

(コ)警察庁において、新たな手口の不正アクセスや不正プログラム（スマートフォン等を狙ったものを含む。）の悪用等急速に悪質巧妙化するサイバー犯罪の取締りを推進するため、サイバー犯罪捜査に従事する全国の警察職員に対する部内研修及び民間企業への講義委託の積極的な実施、官民人事交流の推進、技術的に高度な民間資格の活用等、サイバー犯罪への対処態勢を強化する。

(サ)警察庁において、サイバー空間の脅威に対処するため、日本版NCFTAである一般財団法人日本サイバー犯罪対策センター（JC3）や、都道府県警察と関係事業者から成る各種協議会等を通じた産学官連携を促進するとともに、サイバーセキュリティ政策会議等において官民連携による取組を推進する。

(シ)経済産業省において、フィッシング詐欺被害の抑制のため、フィッシング対策協議会を通じて、海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を行う。

(ス)警察庁において、公衆無線LANを悪用したサイバー犯罪に対する事後追跡可能性の確保に必要な対策が適切に講じられるよう、必要な対応を行う。

(セ)警察庁及び総務省において、安全・安心なサイバー空間を構築するため、通信履歴等に関するログの保存の在り方については、「電気通信事業における個人情報保護に関するガイドライン」の解説を踏まえ、関係事業者における適切な取組を推進するなど必要な対応を行う。

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

- 重要インフラ行動計画に基づく取組の推進及び同計画の見直し
- 面としての防護の強化及び情報共有の促進・拡充

（2018 年戦略より）

(ア)内閣官房及び重要インフラ所管省庁等において、「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」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化の５つの施策を実施する。

- 「安全基準等の整備及び浸透」については、重要インフラ各分野に横断的な指針の策定とそれに基づく、各分野の「安全基準」等の整備・浸透を促進する。
- 「情報共有体制の強化」については、連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化を行う。
- 「障害対応体制の強化」については、官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化を行う。
- 「リスクマネジメント及び対処態勢の整備」については、リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの支援を行う。
- 「防護基盤の強化」については、重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等を推進する。

(イ)総務省において、重要インフラにおけるサービスの持続的な提供に向け、重要無線通信妨害事案の発生時の対応強化のため、申告受付の24時間体制を継続して実施するとともに、妨害原因の排除を迅速に実施する。また、重要無線通信への妨害を未然に防ぐための周知啓発を実施するほか、必要な電波監視施設の整備、電波監視技術に関する調査・検討を実施する。

(ウ)経済産業省において、安全・安心なクレジットカードの利用環境の整備を目的とする「割賦販売法の一部を改正する法律（平成28年法律第99号)」の成立を受け、2017年12月に改正政省令を公布し、2018年６月に改正法を施行する。また、クレジットカード取引に関係する事業者等で構成されているクレジット取引セキュリティ対策協議会において、改正法の実務上の指針として、2018年３月に改訂された「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2018-」に基づき、関係事業者等の取組を更に推進する。

(エ)厚生労働省において、「未来投資戦略」等に基づき、保健医療記録共有サービスを2020年度から本格稼働させることを目指す中で、ネットワークや医療機関のセキュリティ対策強化について、コスト負担のあり方も含めて調査・検討する。

(オ)厚生労働省において、医師等の医療従事者が資格を証明できる電子証明書である保健医療福祉分野電子証明書（HPKI）の活用・普及について一層推進していく。

(カ)厚生労働省において、医療機器の安全性を担う医療機器製造販売業者、組織としての対策を行う医療機関、脆弱性や攻撃の分析を行うセキュリティ機関、自治体等と連携・協調して対応する。

(キ)スマートメーターシステムセキュリティガイドラインに基づき電力各社が取組を強化している中で、経済産業省において、スマートメーターのセキュリティを含め電力会社を取り巻く情勢を分析し、課題の抽出及び必要な対策を検討すべく、新たに有識者が参画する専門の研究会（電力サブワーキング）を立ち上げる。

(ク)内閣官房において、重要インフラ所管省庁の協力の下、第４次行動計画に基づく施策を、中小事業者へ拡大すると共に、継続的に重要インフラに係る防護範囲の見直しに取り組む。

(ケ)総務省において、NICTを通じ、標的型攻撃に関する情報の収集・分析能力の向上に向け、官公庁・大企業のLAN環境を模擬した実証環境を用いて標的型攻撃の解析を実施する。また、「ICT-ISAC」が中心となって実施している、サイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームの構築及び関係事業者等での情報共有の取組を促進する。

(コ)内閣官房において、情報セキュリティ関係機関等と協力関係を構築・強化していくと共に、引き続き、得られた情報を適切に重要インフラ事業者等に情報提供する。また、情報セキュリティ関係機関を情報共有体制のメインプレーヤの一つとして活用していくことについて、具体的な検討を行う。

① リスクマネジメントの推進
・ 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ことに資する取組の推進
（2018 年戦略より）

(サ)内閣官房において、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、重要インフラサービス障害の発生を可能な限り減らすとともに、迅速な復旧が可能となるよう、情報セキュリティ対策に関する取組を推進する。また、オリパラ大会に関係する重要なサービスについても、安全かつ持続的に提供できるよう、この取組を推進する。

- 重要インフラ事業者等における平時のリスクアセスメントに対し、「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」に基づくリスクアセスメントの実施（継続的な見直しを含む）の浸透に向けた取組を行う。
- 重要インフラ事業者等の事業継続計画及びコンティンジェンシープランに対し、盛り込まれるべき「サイバー攻撃リスクの特性並びに対応及び対策の考慮事項」の浸透に向けた取組を行う。

(シ)金融庁において、大規模な金融機関に対して、そのサイバーセキュリティ対応能力をもう一段引き上げるため、「脅威ベースのペネトレーションテスト（テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト）」等、より高度な評価手法の活用を促していく。

② 安全基準等の改善・浸透
・ 安全基準等を改善する取組の継続的な推進
・ 安全等を維持する観点を踏まえた制度的枠組みの適切な改善
（2018 年戦略より）

(ス)重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、国際海底ケーブル等の情報インフラ設備の物理的セキュリティや機器の特性（使用期間等）も考慮しつつ、継続的に安全基準等を改善する。加えて、内閣官房及び重要インフラ所管省庁は、情報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必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化すること、人的要因によるリスク軽減の在り方の検討など、制度的枠組みを適切に改善する取組を継続的に進める。内閣官房は、重要インフラ事業者等における安全基準等の浸透状況等及び重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。（再掲）

(セ)総務省において、ネットワークIP化の進展に対応して、ICTサービスのより安定的な提供を図るため、電気通信に関する事故の発生状況等の分析・評価等を行い、その結果を公表する。また、事故再発防止のため、「情報通信ネットワーク安全・信頼性基準」等の見直しの必要性について検討する。

(ソ)総務省及び経済産業省において、重要インフラ事業者等が保有する重要データがクラウドサービス等において適切に保護される仕組みの在り方について本年度中に国内外の実態調査を踏まえ技術面・法制度面から検討を開始する。

(タ)厚生労働省において、医療機関におけるサイバーセキュリティの現状について調査を行うとともに、医療情報システムの安全管理ガイドラインの普及に取り組む。

(チ)厚生労働省において、医療機器のサイバーセキュリティ対策ガイドラインの策定等により、医療機器のサイバーセキュリティ対策を推進していく。

(ツ)経済産業省において、「ガス事業法」により、ガス事業者に作成と遵守が課せられる保安規程の規定事項に「製造・供給に係る制御システムのサイバーセキュリティ対策」を追加することについて具体化を図る。

③　深刻度評価基準
・　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の策定
（2018 年戦略より）

(テ)内閣官房において、重要インフラ所管省庁の協力の下、第４次行動計画に従い、情報共有体制の強化について次のとおり検討を進める。
- サービス障害の深刻度評価基準の導入に向けた検討を進める。
- 連絡形態の多様化（連絡元の匿名化、セプター事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除、及び分野横断的な情報を内閣官房に集約する仕組みの検討を進める。
- 効果的かつ迅速な情報共有に資するため、情報共有システム構築に係る検討を行う。

④　官民の枠を超えた訓練・演習の実施
・　官民の枠を超えた様々な規模の主体間での訓練・演習の実施
（2018 年戦略より）

(ト)情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。
- 内閣官房において、重要インフラ事業者等の障害対応能力の向上を図るため、重要インフラ分野や所管省庁等が横断的に参加する演習を実施する。
- 総務省において、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、重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。
- 金融庁において、参加金融機関および金融業界全体のセキュリティレベルの底上げを図るため、攻撃の実例分析を踏まえた金融業界横断的なサイバーセキュリティ演習について、必要に応じて対象業態を拡充の上、引き続き実施する。

⑤　制御系システムのセキュリティ対策
・　制御系システムの特性を踏まえたセキュリティ対策の実施
・　制御系システムに関する人材育成及び脅威情報の収集・分析・展開等の推進
（2018 年戦略より）

(ナ)経済産業省において、JPCERT/CCを通じて、インターネット上の公開情報を分析し、国内の制御システム等で外部から悪用されてしまう危険性のあるシステムの脆弱性や設定の状況について、その保有組織に対して情報を提供する。

(ニ)経済産業省において、制御システムのテスト環境を用いシステム全体の脅威分析、リスク評価を行う技術開発を行う。

(ヌ)内閣官房において、我が国で使用される制御系機器・システムに関する脆弱性情報やサイバー攻撃情報などの有益な情報について、非制御系の情報共有体制と整合性のとれた情報共有体制により、収集・分析・展開していく。また、どのような情報が事業者等にとって有益なのかヒアリング等により調査し、情報共有がより効果的なものとなるよう検討を行う。

(ネ)経済産業省において、海外におけるルール化の動向も踏まえ、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を策定するとともに、重要産業分野を中心に産業分野毎のサプライチェーンの構造や守るべきもの、脅威の差異を考慮した、産業分野別の具体的な対策指針を策定する。

(2) 地方公共団体のセキュリティ強化・充実

・　サービス障害や人為的ミスによるマイナンバーを含む情報漏えいへの対策
・　セキュリティポリシーに関するガイドラインの更新
・　業務用ネットワークのセキュリティレベルの確保
・　セキュリティ人材の確保・育成及び体制の充実を支援する取組の推進
・　官民の認証連携に関する環境整備
（2018 年戦略より）

(ア)内閣官房及び総務省において、サイバーセキュリティ基本法等に基づいて、地方公共団体に対する情報の提供など、地方公共団体におけるサイバーセキュリティの確保のために必要とされる協力を行う。

(イ)総務省において、関係機関と協力の上、地方公共団体職員が情報セキュリティ対策について習得することを支援するため、情報セキュリティ監査セミナー、情報セキュリティマネジメントセミナーを集合研修で、その他情報セキュリティ関連研修をeラーニングで実施する。また、マイナンバー制度における情報連携の状況等を踏まえつつ、地方公共団体における情報セキュリティポリシーに関するガイドラインの改定を実施する。

(ウ)総務省において、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、総合行政ネットワーク（LGWAN）内のポータルサイトに、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。

(エ)総務省において、関係機関と協力の上、サーバやネットワーク機器等における脆弱性診断を地方公共団体自らが実施できるよう支援する。地方公共団体の対策やリソースの充実を図るべく、緊急時対応訓練の支援及びCSIRTの連携組織を設立し、地方公共団体のインシデント即応体制の強化を図る。

(オ)内閣官房及び総務省において、総合行政ネットワーク（LGWAN）に設けた集中的にセキュリティ監視を行う機能（LGWAN-SOC)などにより、GSOCとの情報連携を通じた、国・地方全体を俯瞰した監視・検知を行う。また、総務省において、地方公共団体のセキュリティ強化対策を推進するため、情報システムの強靭性の向上や自治体情報セキュリティクラウドの状況に係るフォローアップを実施するとともに、「自治体情報セキュリティ向上プラットフォーム」の利用を促進することにより、マイナンバー制度を含めたセキュリティ確保を徹底する。さらに、情報連携に利用する情報提供ネットワークシステムについて、インターネットから独立する等の対策を講じており、引き続き高いセキュリティ確保をすべく、適切な管理・監督・支援等を行う。加えて、個人情報保護委員会において、関係省庁等と連携しつつ、特定個人情報の適正な取扱いに関するガイドラインの遵守、特定個人情報に係るセキュリティの確保を図るため、専門的・技術的知見を有する体制を拡充するとともに、監視・監督機能を強化し、情報提供ネットワークシステムに係る監視を適切に行う。

(カ)総務省において、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、地方公共団体におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。

(キ)内閣府において、2017年11月に本格運用を開始したマイナポータルを活用し、官民の認証連携をより一層推進していく。

(ク)厚生労働省において、マイナンバーカードの健康保険証としての活用について、2020年度の導入を目指して準備を進めていく。

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

- 対処能力の向上に加え、新たな防御技術を活用したより効果的な取組
- 情報システムの防御能力の向上と状態の把握
- 政府機関等における横断的な連携の高度化による被害の発生・拡大の防止

（2018 年戦略より）

(ア)内閣官房において、統一基準群の改定に伴う各府省庁、独立行政法人及びサイバーセキュリティ基本法に基づく指定法人（以下「独立行政法人等」という。）の情報セキュリティポリシーの見直しについて、必要な支援を行う。また、新たに直面した脅威・課題への対応について、統一基準群の将来の改定に向けた知見の蓄積を行う。

(イ)内閣官房において、政府機関等の情報システムの調達におけるセキュリティ・バイ・デザインを推進するため、NISCが公表しているセキュリティ・バイ・デザインに関連するマニュアルの改定に着手する。

(ウ)経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPAを通じ、

「IT製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを行うとともに、政府機関の調達担当者等に対し、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を行う。

(エ)経済産業省において、IPAを通じ、CCRAなどの海外連携、セキュリティ評価に係る国際基準の作成や各国の情報収集を行うとともに、安全な政府調達のための国際共通プロテクション・プロファイル（PP）の開発、情報収集を実施する。

(オ)経済産業省において、IPAを通じ、JISEC（ITセキュリティ評価及び認証制度）の利用者の視点に立った評価・認証手続の改善、積極的な広報活動等を実施するとともに、安全な政府調達を推進するため、調達関係者に対する広報活動や勉強会、ヒアリングを実施するとともに必要に応じて手順や新たなIT製品への対応等の見直しを実施する。

(カ)経済産業省において、安全性の高い暗号モジュールの政府機関における利用を推進するためIPAの運用する暗号モジュール試験及び認証制度（JCMVP）の普及を図る。

(キ)内閣官房において、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）により、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24時間365日収集・分析し、政府機関等に対する新たなサイバー攻撃の傾向や情勢等について、分析結果を各政府機関等に対して適宜提供する。また、IPAの実施する、独立行政法人等に係る監視業務の監督を行うとともに、監視に係る能力や機能の向上の観点から、攻撃情報の共有等の連携を図る。

(ク)内閣官房において、巧妙化する情報セキュリティに関する脅威、動向等を踏まえ、各府省庁の情報システムにおける対策の実施状況の点検・改善を行うため、公開された脆弱性等への対応やサイバー攻撃に係る対策の実施状況の調査を行う。調査結果は、マネジメント監査により確認された課題等も踏まえ、統一基準群を始めとした規程への反映や改善に向けた取組について検討を行う。

(ケ)内閣官房において、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の運用等を通じて標的型攻撃に対する多重防御の取組を引き続き推進する。

(コ)内閣官房において、大規模サイバー攻撃や大規模災害発生時における、情報システムを用いる業務についての復旧対策を強化するため、政府機関におけるIT-BCPの見直しにかかる調査等を実施するとともに、規程の改定に着手する。

(サ)総務省及び経済産業省において、CRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行う。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT及びIPAを通じ、暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、暗号政策の中長期的視点からの取組の検討を実施するため、暗号技術評価委員会及び暗号技術活用委員会を開催する。

(シ)厚生労働省において、社会保険診療報酬支払基金のサイバーセキュリティ体制について、内閣官房等と緊密に連携し、迅速なサイバー攻撃からの防護の技術的な体制の強化に取り組む。

(ス)内閣官房において、2020年東京オリンピック・パラリンピック競技大会及びその後を見据え

て、インシデント発生前及び発生時の情報提供の迅速化・高度化に資するGSOCシステムの検知・解析機能を始めとした機能強化、GSOCセンサーの増強等の検討を行うなど、政府機関等における端末等での新たな監視手法等の導入状況を踏まえつつ、政府機関等と次期GSOCにおける効果的かつ効率的な連携を推進する。

(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

- 政府プライベート･クラウドとしての政府共通プラットフォームへの移行を含むクラウド化の推進
- 信頼できるクラウドの利用を促進する方策の検討
- 政府機関のインターネット接続口の適切な集約の推進とともに､境界監視ポイントの集約の検討

（2018 年戦略より）

(ア)政府機関のクラウド化を推進する観点から、以下の取組を行う。
- 内閣官房において、政府機関におけるクラウドサービスの利用状況を適宜調査し、課題等の把握に努める。
- 総務省において、政府共通プラットフォームの本格更改に向け、新たな政府のプライベート・クラウドとしての整備計画を策定する。

(イ)総務省及び経済産業省において、官民双方が一層安心・安全にクラウドサービスを採用し、継続的に利用していくため、情報資産の重要性に応じ、信頼性の確保の観点から、クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、2018年度から検討を開始する。

(ウ)内閣官房及び総務省において、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する。

(3) 先端技術の活用による先取り対応への挑戦

- 新しい設計思想の下で誕生した情報技術の活用の可能性の検討

（2018 年戦略より）

(ア)内閣官房において、近年普及してきた情報システムの基盤の中でサイバー攻撃による高い耐性を有するものについて、これらの情報技術を、政府機関等において活用できる可能性について検証する。

(4) 監査を通じたサイバーセキュリティの水準の向上

- 組織横断的な分析により抽出される傾向や課題を踏まえたサイバーセキュリティ水準向上の促進
- IT 資産管理情報を活用した効果的かつ効率的な監査の実施

（2018 年戦略より）

(ア)内閣官房において、政府機関における統一基準群等に基づく施策の取組状況について、セキュリティ対策を強化するための体制等が有効に機能しているかとの観点を中心とした検証を通じて、自律的なセキュリティ水準の向上を促す仕組みを確立するため、引き続き国の行政機関に対して監査を実施する。監査の実施に当たっては、２年間で全ての国の行政機関に対して監査を実施する計画とし、国の行政機関のサイバーセキュリティ対策及びその維持改善の体制の整備及び運用状況に係る現状を把握し、改善のために必要な助言等を行う。なお、監査を実施した国の行政機関については、フォローアップを実施する。2018年度の監査については、前回までの監査の結果を踏まえるとともに前回対象としなかった部局やシステムを対象として実施する。

(イ)内閣官房において、国の行政機関の情報システムにおけるセキュリティ対策の点検・改善を行うため、実際の攻撃手法を用いて情報システム内部への侵入及び侵入後の被害状況について検証を行うペネトレーションテストを引き続き国の行政機関に対して実施する。その結果を踏まえて、問題点の改善に向けた助言等を行う。なお、ペネトレーションテストを実施した国の行政機関については、フォローアップを実施する。加えて、情報システムのペネトレーションテストを行うに当たり、自衛隊が有する知識・経験の活用を実施していく。

(ウ)内閣官房において、独立行政法人等における統一基準群に基づく施策の取組について、セキュリティ対策を強化するための体制等が有効に機能しているかとの観点を中心とした検証を通じて、自律的なセキュリティ水準の向上を促す仕組みを確立するため、IPAとの連携等により、引き続き独立行政法人等に対して監査を実施する。監査は、2020年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し行う計画とし、独立行政法人等のサイバーセキュリティ対策及びその維持改善の体制の整備及び運用状況に係る現状を把握し、改善のために必要な助言等を行う。なお、監査を実施した法人については、フォローアップを実施する。また、独立行政法人等における情報セキュリティ対策の実施状況を明らかにし、その結果を踏まえ、所管する府省庁と協力しセキュリティ対策の強化を図る。2018年度の監査については、独立行政法人等の業務内容の多様性を踏まえ選定した部署やシステムを対象として実施する。

(エ)内閣官房において、独立行政法人等の情報システムにおけるセキュリティ対策の点検・改善を行うため、実際の攻撃手法を用いて情報システム内部への侵入及び侵入後の被害状況について検証を行うペネトレーションテストを、IPAとの連携等により、引き続き独立行政法人等に対して実施する。その結果を踏まえて、問題点の改善に向けた助言等を行う。ペネトレーションテストは、2020年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し行う。なお、ペネトレーションテストを実施した法人については、フォローアップを実施する。

(5) 組織的な対応能力の充実

- 事案対応を行うチームを中心に事案対応能力や情報セキュリティに係る知識の向上
- 情報セキュリティ緊急支援チームの要員の対処能力の向上

（2018 年戦略より）

(ア)内閣官房において、サイバーセキュリティ基本法に基づく重大インシデント等に係る原因究明調査をより適切に実施するため、デジタルフォレンジック調査に当たる職員の技術力の向上に引き続き取り組むとともに、民間事業者の知見を活用するための方策を講じる。

(イ)内閣官房において、サイバー攻撃への対処に関する政府機関全体としての体制を強化するため、各府省庁のインシデント対処に関わる要員による情報共有及び連携の促進に資するコミュニティの更なる活性化を図る。

(ウ)内閣官房において、引き続き、府省庁及び独立行政法人等を対象に、昨今のサイバーセキュリティの動向や課題等に応じたテーマによる勉強会等を開催する。また、人事院と協力し、政府職員の採用時の合同研修にサイバーセキュリティに関する事項を盛り込むことによる教育機会の付与に取り組む。

(エ)政府機関におけるサイバー攻撃に係る対処要員の能力及び連携の強化を図るため、以下の訓練・演習を実施する。

- 内閣官房において、各府省庁における情報セキュリティインシデント対処に関わる要員を対象として、最高情報セキュリティ責任者及びサイバーセキュリティ・情報化審議官等をはじめとした幹部による指揮の下での組織的かつ適切な対処の実現を目指し、これまでの訓練や調査等により明らかになった課題や近年のサイバー攻撃動向等を踏まえた訓練を実施する。また、府省庁及び独立行政法人等における情報セキュリティインシデント対処に関わる要員を対象として、研修を年間を通じて実施する。さらに、政府機関等において自組織の環境に最適化した訓練を独自に実施できるようにするために必要な支援を行う。
- 内閣官房において、サイバー攻撃等により発生した支援対象機関等の情報システム障害又はその発生が予想される場合等、政府一体となった対応が必要となる情報セキュリティインシデントに対応できる人材を養成・維持するため、情報セキュリティ緊急支援チーム（CYMAT）要員等に対する研修と実習等を実施する。
- 総務省において、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、国の行政機関等におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。
- 内閣官房及び総務省において、昨今のサイバー攻撃やこれまでの実施結果を踏まえつつ、NATIONAL 318(CYBER) EKIDENを実施する。

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

- 大学等における計画等に基づく自律的かつ組織的な取組の促進
- サイバーセキュリティに関するガイドライン等の策定と普及
- 各層別研修及び実践的な訓練や演習の実施
- 事案発生時の初動対応への支援

（2018 年戦略より）

(ア)文部科学省において、大学等の多様性を踏まえ、大学等が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検討を行い、大学等の取組を促進する。また、当該対策の推進に資するガイドライン等について検討する。

(イ)文部科学省において、大学等におけるリスクマネジメントや事案対応に資する各層別研修及び実践的な訓練・演習の体系について検討し、試行的に実施する。

(ウ)文部科学省において、外部のセキュリティ機関等と連携し、大学等で発生した事案の初動対

応について必要に応じて支援する体制を整備する。

(2) 大学等の連携協力による取組の推進

- サイバー攻撃への監視能力の機能維持・強化
- 戦略マネジメント層の育成に向けた共同研究や技術職員への研修の実施
- 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取組への支援

（2018 年戦略より）

(ア)文部科学省において、国立情報学研究所（NII）を通じ、国立大学法人及び大学共同利用機関法人（以下「国立大学法人等」という）のインシデント対応体制を高度化するために、国立大学法人等へのサイバー攻撃の情報提供と情報セキュリティ担当者の研修を実施する。

(イ)文部科学省において、国立情報学研究所（NII）を通じ、サイバー攻撃耐性を向上させるため、国立大学法人等において、M2Mを含み学術評価に適したデータを実環境から継続的に収集し、データ解析技術の開発を促進する。

(ウ)文部科学省において、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する。

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

- 「セキュリティ幹事会」で決定された基本戦略に基づく取組の推進
- 大会の安全に関する情報の集約等の取組の推進
- リスク評価及び明らかになったリスクへの対策の促進
- 「サイバーセキュリティ対処調整センター」の構築の推進と連絡調整態勢の整備

（2018 年戦略より）

(ア)内閣官房において、「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)」(2017年３月21日セキュリティ幹事会決定）に基づくサイバーセキュリティ対策の強化を引き続き推進する。具体的には、オリパラ競技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と、情報の共有、インシデント発生時の調整役となるための組織である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）の整備を推進する。2018年度のリスク評価は、対象エリアを全国に拡大して実施するとともに特に重要なサービス事業者については国として横断的リスク評価を実施する。また、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）については、2018年度末を目途に構築し、2019年度から要員の訓練、情報共有システムのユーザーに対する操作訓練、情報共有訓練及びインシデント発生時の対応訓練支援が実施できるよう準備する。

(イ)警察庁に設置した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年東京オリンピック・パラリンピック競技大会の安全に関する情報を集約するとともに、大会の安全に対する脅威及びリスクの分析、評価を行

い、国の関係機関等に対し必要な情報を随時提供する。

(2) 未来につながる成果の継承

- 2020 年東京大会の態勢整備のための各種施策の継続推進
- 整備した仕組み、運用経験及びノウハウの活用
- 「サイバーセキュリティ対処調整センター」のナショナル CSIRT としての活用
- 「リスクアセスメント」の手法の全国の事業者等への適用とそのための整備・普及

（2018 年戦略より）

(ア)内閣官房において、2020年東京大会に向けた態勢の整備に当たっては、整備した仕組み、その運用経験及びノウハウが、レガシーとして、2020年東京大会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できることを考慮し、構築した「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（ナショナルCSIRT）へと成長・発展させ、サイバーセキュリティの基本的な在り方でも掲げた「リスクマネジメント」の手法については、広く全国の事業者等に適用できるよう検討する。

(イ)警察庁及び都道府県警察において、2020年東京大会その他の大規模国際イベントを見据えたサイバー攻撃対策を推進するとともに、態勢の運用を通じて得た情報収集・分析、管理者対策、事案対処等に関する教訓やノウハウの効果的活用を図る。また、法務省において、人的情報収集・分析を行い、対応を推進する。

(ウ)総務省において、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、2020年東京オリンピック・パラリンピック競技大会に向けた大規模演習環境「サイバーコロッセオ」を活用し、同大会のサイバーセキュリティを守る高度な人材の育成を推進し、更なる内容の拡充を図り、より実践的な環境の下でのサイバー演習の強化を図る。

2.6. 従来の枠を超えた情報共有・連携体制の構築

- ISAC を含む既存の情報共有の推進

（2018 年戦略より）

(ア)内閣官房において、情報セキュリティ関係機関等と協力関係を構築・強化していくと共に、引き続き、得られた情報を適切に重要インフラ事業者等に情報提供する。また、情報セキュリティ関係機関を情報共有体制のメインプレーヤの一つとして活用していくことについて、具体的な検討を行う。

(イ)経済産業省において、最新の脅威情報やインシデント情報等の共有のためIPAを通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう参加組織の拡大、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。また、重要インフラ事業者等における信頼性・安全性向上の取組を支援するため、IPAを通じ、障害事例等の情報を重要インフラ事業者等へ提供する。

(ウ)総務省において、ISP事業者やICTベンダー等を中心に構成されている「ICT-ISAC」を核として、国際連携を含めてサイバー攻撃に関する情報共有網の拡充を推進する。

(エ)国土交通省において、2018年４月から重要インフラ（航空、鉄道、物流分野）事業者による情報共有・分析及び対策を連携して行う体制である「交通ISAC」（仮称）の仮運用が開始されたことから、事業者等が参加する検討会を開催し、交通ISACの本格運用に向けて情報共有・知見共有の仕組みや運営形態等を検討・議論する。

(オ)金融庁において、金融機関に対し、「金融ISAC」を含む情報共有機関等を通じた情報共有網の拡充を進める。

(カ)厚生労働省において、医療分野及び水道分野のISACについて、必要な調査・情報収集を行うとともに、検討を進める。

(キ)経済産業省において、クレジットカード会社に対し、「金融ISAC」等の情報共有機関等を通じた情報共有網の拡充を進める。

(ク)経済産業省において、自動車業界の事業者に対し、「J-Auto-ISAC」等の情報共有機関等を通じた情報共有網の拡充を進める。

(ケ)経済産業省において、重要インフラ事業者等において対策が必要となる可能性のある脅威情報及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、JPCERT/CCから重要インフラ事業者等へ提供する。

(コ)警察庁において、サイバー空間の脅威に対処するため、一般財団法人日本サイバー犯罪対策センター（JC3）を通じた産学官連携した取組を進める。

(1) 多様な主体の情報共有・連携の推進

- 情報共有に十分な知見を有する専門機関を含む官民の多様な参加主体が、安心して相互に情報共有を図るための体制の構築
- 官民、業界、国内外といった枠を超えた情報共有・連携の推進
- 既存の情報共有体制についての連携や統合の検討

（2018 年戦略より）

(ア)国の行政機関、重要インフラ事業者、サイバー関連事業者等官民の多様な主体が相互に連携し、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の創設に向けて検討を進める。

(2) 情報共有・連携の新たな段階へ

- 積極的に情報提供に協力する者ほど恩恵を享受できる仕組みの検討
- 情報処理の自動化の推進
- 参加主体が従来の枠を超えて共存・発展する関係構築に向けた環境整備の推進

（2018 年戦略より）

(ア)内閣官房が中心となり構築する情報共有体制において、積極的にサイバーセキュリティインシデント等に係る情報（例えば、リコールの要因となる情報など、国民の生命・身体を保護するために提供される情報を含む。）の共有に貢献する参加者が評価される環境を整備する

ための検討を進める。また、当該体制において情報の共有や分析を迅速に行うための処理の自動化に向けた検討を進める。

(イ)内閣官房が中心となり構築する情報共有体制において、所管省庁を同じくする複数の業界が業界を跨いで情報共有の仕組みを構築する等新しい情報共有・連携を推進するための検討を進める。

2.7. 大規模サイバー攻撃事態等への対処態勢の強化

- サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化
- サイバー空間における情報収集・分析機能及び緊急対処能力の向上

（2018 年戦略より）

(ア)内閣官房において、国民の生命等に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力の強化を図るため、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を実施する。

(イ)内閣官房において、サイバー攻撃等の事象に関する政府としての一連の初動対処（検知、判断、対処、報告）を見直し、サイバーセキュリティに係る危機管理対応の一層の強化が図られるよう留意する。

(ウ)警察庁及び都道府県警察において以下の取組を推進することにより、サイバー攻撃対処態勢の強化を図る。

- 都道府県警察において、安全確保等に係る実空間の対処も考慮しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を図る。
- 警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。
- 警察庁及び都道府県警察において、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を図る。
- 警察庁において、都道府県警察のサイバー攻撃対策担当者を対象に、大規模産業型制御システムに関するサイバー攻撃対策に係る訓練を実施する。
- 警察庁において、サイバー空間の脅威への危機管理に臨むため、サイバー空間に関する観測機能の強化等に取り組むことで、サイバーフォースセンターの技術力の向上等を図る。また、サイバー攻撃の実態解明に必要不可欠な不正プログラム等の解析を推進する。

(エ)経済産業省において、JPCERT/CCを通じ、重要インフラ事業者等からの依頼に応じ、国際的なCSIRT間連携の枠組みも利用しながら、攻撃元の国に対する調整等の情報セキュリティインシデントへの対応支援や、攻撃手法の解析の支援を行う。

(オ)経済産業省において、IPAを通じ、我が国経済社会に被害をもたらすおそれが強く、一組織で対処が困難なサイバー攻撃を受けた組織等を支援するため、「サイバーレスキュー隊（J-CRAT)」の活動を増強し、被害組織における迅速な対応・復旧に向けた計画作りを支援す

る。

(カ)個人情報保護委員会において、個人情報取扱事業者における、外部からの不正アクセス等による個人データの漏えい等の事案への対応が適切に実施されるよう、個人情報サイバーセキュリティ連携会議を通じて、関係機関と緊密な連携を図り事案の詳細の把握に努めるとともに、必要に応じて指導・助言等を行う。

(キ)経済産業省において、JPCERT/CCを通じ、企業へのサイバー攻撃等への対応能力向上に向けて、国内における組織内CSIRT設立を促進・支援する。また、CSIRTの構築・運用に関するマテリアルや、インシデント対策・対応に資する脅威情報や攻撃に関する情報、所要の分析を加えた具体的な対策情報等を適切な者の間で共有することにより、CSIRTの普及や、国内外の組織内CSIRTとの間における緊急時及び平常時の連携の強化を図るとともに、巧妙かつ執拗に行われる標的型攻撃への対処を念頭においた運用の普及、連携を進める。

3. 国際社会の平和・安定及び我が国の安全保障への寄与

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、国際場裡における理念の発信、サイバー空間における法の支配の推進

（2018 年戦略より）

(ア)内閣官房、外務省及び関係府省庁において、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、戦略的な取組を進める。

(1) 自由、公正かつ安全なサイバー空間の理念の発信

・ 日本型のサイバーセキュリティの基本的な在り方の発信、サイバー空間の発展を妨げるような国際ルールの変更等を目指す取組への対抗

（2018 年戦略より）

(ア)内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省において、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に努めるとともに、越境データ規制、ソースコード開示、国家によるインターネットの資源管理等、自由な情報の流通を阻害するような動きに対抗し、自由、公正かつ安全なサイバー空間を実現する。

(イ)経済産業省及び外務省において、情報セキュリティなどを理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション規則等、我が国企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（「Forced Localization Measures」）を行う諸外国に対し、対話や意見交換を通じ、当該規制が自由貿易との間でバランスがとれたものとなるよう、民間団体とも連携しつつ働きかけを行う。

(2) サイバー空間における法の支配の推進

・ 既存の国際法の個別具体的な適用の在り方、規範の形成・普遍化についての議論への積極的な関与

（2018 年戦略より）

(ア)内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省において、各二国間協議や多国間協議に参画し、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、それらに我が国の意向を反映させる。

・ サイバー犯罪に関する条約、刑事共助条約、ICPO 等の枠組みを活用した国際機関、外国法執行機関、外国治安情報機関等との間における国際捜査共助や情報交換等による国際連携

（2018 年戦略より）

(イ)警察庁及び法務省において、容易に国境を越えるサイバー犯罪に効果的に対処するため、原則として共助を義務的なものとする日・米、日・韓、日・中、日・香港、日・EU、日・露間の刑事共助条約・協定及びサイバー犯罪に関する条約の発効を受け、これらの条約・協定の下で、中央当局を設置し、外交ルートを経由せずに直接中央当局間で共助実施のための連絡を行うことで共助の迅速化を図る。今後は、更なる刑事共助条約の締結について検討していく。

(ウ)警察庁において、迅速かつ効果的な捜査共助等の法執行機関間における国際連携の強化を目的とし、我が国のサイバー犯罪情勢に関係の深い国々の各法執行機関と効果的な情報交換を実施するとともに、G7、ICPO等のサイバー犯罪対策に係る国際的な枠組みへの積極的な参加、アジア大洋州地域サイバー犯罪捜査技術会議の主催等を通じた多国間における協力関係の構築を推進する。また、外国法執行機関等に派遣した職員を通じ、当該機関等との連携強化を推進する。さらに、証拠の収集等のため外国法執行機関からの協力を得る必要がある場合について、外国の法執行機関に対して積極的に捜査共助を要請し、的確に国際捜査を推進する。

(エ)外務省において、我が国が2012年７月にサイバー犯罪に関する条約を締結し、同年11月から我が国について同条約の効力が生じたことを受け、引き続きアジア地域初の締約国として同条約の普及等に積極的に参画する。

3.2. 我が国の防御力・抑止力・状況把握力の強化

(1) 国家の強靭性の確保

① 任務保証
・ 政府機関及び重要インフラ事業者等におけるサイバーセキュリティの確保の推進
・ 防衛省・自衛隊のサイバー攻撃対処を行う部隊の能力向上、自らの活動が依存するネットワーク・インフラの防護強化、自衛隊の任務保証に関連する主体との連携の深化
（2018 年戦略より）

(ア)都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、以下の取組を実施することにより、緊急対処能力の向上を図る。
- 重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供や保有するシステムに対する脆弱性試験を実施する。
- 事案発生を想定した共同対処訓練を実施する。
- サイバーテロ対策協議会を通じて、参加事業者間の情報共有を実施する。

(イ)防衛省において、対処機関としてのサイバー攻撃対処能力向上のため、最新技術を活用して、サイバー防護分析装置、サイバー情報収集装置、各自衛隊の防護システムの機能の拡充を図るとともに、多様な事態において指揮命令の迅速かつ確実な伝達を確保するため、防衛情報通信基盤（DII）のクローズ系及びネットワーク監視器材へ常続監視等を強化するための最新技術を適用していく。

(ウ)防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処のための官民協力関係の深化に向けた取組を実施する。また、任務保証の観点から、防衛省・自衛隊の活動が依存するネットワーク・インフラの防護を引き続き強化するとともに、自衛隊の任務保証に関連する主体との連携を深化させていく。

(エ)防衛省・自衛隊が保有する情報通信ネットワーク等に対する侵入試験（ペネトレーションテスト）について、実施に向けた所要の準備を進める。

(オ)防衛省において、サイバー攻撃等によって防衛省・自衛隊の情報通信基盤の一部が損なわれた場合においても、運用継続を実現する研究を実施する。

(カ)防衛省において、移動系システムを標的としたサイバー攻撃対処のための演習環境整備に関する研究を実施する。

② 我が国の先端技術・防衛関連技術の防護
・ 防衛産業において、安全な情報共有を確保する仕組みの導入、契約企業向けの新たな情報セキュリティ基準の策定、契約条項の改正等の取組の実施
・ 国立研究開発法人や先端的な技術情報を保有する大学等における対策の促進
（2018 年戦略より）

(キ)防衛省において、サイバーセキュリティの更なる確保のため、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とともに、引き続き調査研究等を通じて必要な関連規則等の整備を進める。

(ク)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、以下の取組を行う。
・ 内閣官房において、先端的な技術を保有する国立研究開発法人が、自立的に情報セキュリティ対策を講じていくことができるよう国立研究開発法人相互の協力の枠組みを通じ取組を促す。
・ 文部科学省において、先端的な技術情報を保有する大学等に対して、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。

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
（2018 年戦略より）

(ケ)内閣官房において、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。

(コ)警察庁及び法務省において、サイバー空間におけるテロ組織等の動向把握及びサイバー攻撃への対策を強化するため、サイバー空間における攻撃の予兆等の早期把握を可能とする態勢を拡充し、人的情報やオープンソースの情報を幅広く収集する等により、攻撃主体・方法等に関する情報収集・分析を強化するとともに、サイバー空間を悪用したテロ組織の活動への対策について、国際社会との連携を図る。

(2) サイバー攻撃に対する抑止力の向上

① 実効的な抑止のための対応
・ 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への、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た対応
・ 法執行機関、自衛隊を始めとする関係機関の能力強化

（2018 年戦略より）

(ア)適切な対応を適時にとれるよう、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する。

(イ)防衛省において、自衛隊のサイバー攻撃対処部隊の対処能力の練度を向上させるため、指揮システムを模擬した環境を構築して、攻撃・防御の機能とこれに対する統裁・評価の機能等を備えた実戦的な演習環境を整備する。その際、悪意ある主体によるサイバー空間の利用を妨げる能力の保有の可能性についても視野に入れる。

(ウ)警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進する。また、都道府県警察において、サイバー攻撃特別捜査隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進する。

② 信頼醸成措置
・ 偶発的、不必要な衝突を防ぐための、国際的な連絡体制の構築
・ 二国間・多国間協議における情報交換、政策対話等を通じた信頼醸成

（2018 年戦略より）

(エ)内閣官房、外務省及び関係府省庁において、サイバー攻撃を発端とした不測事態の発生を未然に防止するため、ARFや二国間協議等を通じて、脅威認識やサイバーセキュリティ戦略等の政策について共有し、国際的な連絡体制等を平素から構築する。

(オ)経済産業省において、JPCERT/CCを通じて、インシデント対応調整や脅威情報の共有に係るCSIRT間連携の窓口を運営するとともに、各国の窓口チームとの間のMOU/NDAに基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、JPCERT/CCのFIRST、IWWNやAPCERTにおける活動、及びアジア太平洋地域におけるインシデント対応演習等の活動等を通じた各国CSIRTとJPCERT/CCとのインシデント対応に関する連携を行う。

(3) サイバー空間の状況把握の強化

① 関係機関の能力向上
・ 関係機関の情報収集・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・分析等するための技術の開発・活用
・ 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

（2018 年戦略より）

(ア)内閣官房において、「カウンターインテリジェンス機能の強化に関する基本方針」に基づき、各府省庁と協力し、サイバー空間におけるカウンターインテリジェンスに関する情報の集約・分析を行い各府省との共有化を図る。また、政府機関が保有する機密情報が保護されるよう適切な措置を実施する。

(イ)警察庁及び法務省において、サイバーインテリジェンス対策に資する取組を実施する。

(ウ)警察庁及び都道府県警察において、以下の取組を推進することによりサイバー空間の状況把握の強化を図る。

- 警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。(再掲)
- 警察庁及び都道府県警察において、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を図る。(再掲)
- 警察庁において、システムの脆弱性の調査等を目的とした不正なアクセスが国内外で多数確認されている背景を踏まえ、こうした攻撃の未然防止活動、有事の緊急対処に係る能力向上に資する訓練、サイバー空間に関する観測機能の強化等に取り組むことで、サイバーフォースセンターの技術力の向上等を図る。また、サイバー攻撃の実態解明に必要不可欠な不正プログラム等の解析を推進する。

(エ)警察庁において、警察部内の高度な専門性を有する人材等の確保・育成を図る方策を検討する。

(オ)経済産業省において、JPCERT/CCがインシデント対応支援活動等において解析したマルウェア検体及びその解析結果について、同様の情報を有する国内外の関係機関との適切な相互共有やインターネット定点観測システム（TSUBAME）の運用との連動等の有効活用やその高度化を進める。

(カ)防衛省において、高度なサイバー攻撃からの防護を目的として、引き続き、国内外におけるサイバー攻撃関連情報を収集・分析する体制を強化するとともに、必要な機材の拡充を実施する。

(キ)防衛省において、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。

(ク)法務省において、人的情報収集・分析を強化するための高度な専門性を有する人材の確保・育成を図る方策を検討する。

② 脅威情報連携
- 同盟国・有志国との脅威情報共有の推進
- 政府内の脅威情報共有・連携体制の強化

（2018 年戦略より）

(ケ)内閣官房及び外務省において、外国関係機関との情報交換等を緊密に行い、主要国のサイバ

ー攻撃対処や国家の関与が疑われるようなサイバー攻撃の動向等の情報収集・分析に努める。

(コ)内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。

(サ)警察庁及び法務省において、サイバー攻撃対策を推進するため、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する。

3.3. 国際協力・連携

- 国際場裡での我が国の立場を主張できる官民の人材を確保し、育成する。

（2018 年戦略より）

(ア)内閣官房及び関係府省庁において、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、我が国のサイバーセキュリティ人材が海外の優秀な技術者等と切磋琢磨しながら研鑽を積む場を増やす。

(1) 知見の共有・政策調整

- サイバーセキュリティに関する二国間の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、体制の情報交換の実施
- 戦略的パートナー国とのサイバーセキュリティ施策に関する協力・連携の強化

（2018 年戦略より）

(ア)内閣官房、総務省、外務省及び経済産業省において、日ASEANサイバーセキュリティ政策会議、二国間協議等の枠組みを通じ、アジア大洋州各国とのサイバー政策における相互理解と連携を強化する。また、総務省において、ワークショップの開催等を通じて、我が国とASEAN加盟国のネットワークオペレータによって培われた知見や経験の相互共有を促進する。

(イ)警察庁、法務省及び外務省において、国境を越えるサイバー犯罪の脅威に対抗するため、特にアジア太平洋地域諸国におけるサイバー犯罪対策に関する刑事司法制度の整備等が進むよう、二国間又は多国間の枠組みを活用した技術援助活動を積極的に推進する。

(ウ)防衛省及び関係府省庁において、東南アジア各国との間で、防衛当局間のITフォーラム等の取組を通じ、サイバー分野での連携やこれらの国に対する能力構築への協力、情報の収集や発信を推進していく。また、防衛省において、諸外国とのサイバー防衛協力を推進していく。

(エ)経済産業省において、アジアでの更なる情報セキュリティ人材の育成を図るため、アジア11か国・地域と相互・認証を行っている「情報処理技術者試験」について、我が国の情報処理技術者試験制度を移入して試験制度を創設した国（フィリピン、ベトナム、タイ、ミャンマー、モンゴル、バングラデシュ）が協力して試験を実施するための協議会であるITPECがアジア統一試験を実施しているところ、ITPECの更なる定着を図る。

(オ)内閣官房、外務省及び関係府省庁において、日米サイバー対話等の枠組みを通じ、幅広い分野における日米協力について議論し、両国間の政策面での協調や体制及び能力の強化、インシデント情報の交換等を推進し、同盟国である米国とのサイバー空間に関する幅広い連携を強化する。

(カ)総務省、外務省及び関係府省庁において、米国とのインターネットエコノミーに関する日米政策協力対話にて一致した、産業界及び他の関係者と共同してサイバーセキュリティ上の課題に取り組むことが不可欠であるとの認識に基づき、引き続き米国との情報共有を強化する。また、関連して、総務省において、日米の通信分野のISAC間の連携を推進する。

(キ)経済産業省において、国際協力体制を確立するという観点から、米NIST等の各国のサイバーセキュリティ機関との連携を通じて、情報セキュリティに関する最新情報の交換や技術共有等に取組む。

(ク)防衛省において、日米サイバー防衛政策ワーキンググループ（CDPWG）の開催等を通じて、情報共有、訓練・人材育成等の様々な協力分野において日米サイバー防衛の連携を深めていく。また、新たな日米防衛協力のための指針で示された方向性に基づき、自衛隊と米軍との間における運用面のサイバー防衛協力を深化させていく。

(ケ)内閣官房、外務省及び関係府省庁において、二国間協議の枠組みを通じ、欧州各国との連携を強化する。防衛省において、日英防衛当局間サイバー協議、日NATOサイバー防衛スタッフトークスやNATO主催の演習への参加等を通じ、欧州各国とのサイバー防衛協力を引き続き推進していく。

(コ)内閣官房、外務省及び関係府省庁において、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する。

(サ)警察庁において、サイバー攻撃対策を推進するため、情報交換等国際的な連携を通じて、諸外国関係機関との連携強化を推進する。

(シ)経済産業省において、IPAを通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行うため、JIWG及びその傘下のJHAS、JEDSと定期的に協議を行う。

(ス)防衛省において、国家の関与が疑われるような高度なサイバー攻撃に対処するため、防衛省・自衛隊のサイバーセキュリティに係る諸外国との技術面・運用面の協力を推進する。

(2) 事故対応等に係る国際連携の強化

- CERT 間連携の強化
- 国際サイバー演習への参加、共同訓練等を通じた連携対処能力の向上

（2018 年戦略より）

(ア)内閣官房及び関係府省庁において、二国間協議、IWWN、日ASEANサイバーセキュリティ政策会議等のサイバー空間に関する多国間の情報共有枠組み等に参画し、それぞれの取組においてインシデント対応演習や机上演習等を通じて、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する。

(イ)経済産業省において、JPCERT/CCを通じ、各国のCSIRT連携による対応・対策を強化するため、サイバーセキュリティに関する比較可能で堅牢な定量評価の仕組み（サイバーグリーン）の検討や、効率的な対処のためのオペレーション連携を実現するための基盤構築に資する開発、運用協力体制の検討を進める。

(ウ)経済産業省において、JPCERT/CCを通じて、主にアジア太平洋地域等を対象としたインターネット定点観測システム（TSUBAME）に関し、運用主体のJPCERT/CCと各参加国関係機関等との間での共同解析やマルウェア解析連携との連動等の取組を進める。また、アジア太平洋地域以外への観測点の拡大を進める。

(エ)経済産業省において、JPCERT/CC を通じて、以下の取組を行う。

- アジア太平洋地域、アフリカ等において、各国における対外・対内調整を担うCSIRTの構築及び運用、連携の支援。JPCERT/CCの経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習の実施。
- アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、組織内CSIRT構築セミナー等の普及・啓発、サイバー演習の実施。
- 我が国企業が組込みソフトウェア等の開発をアウトソーシングしているアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施。

(3) 能力構築支援

- 様々な政策手段を活用した開発途上国における能力構築支援の実施

（2018 年戦略より）

(ア)内閣官房、警察庁、総務省、外務省、経済産業省、その他関係府省庁・機関が相互に連携、情報共有を行い、ASEAN 加盟国をはじめとする各国における能力構築支援に積極的に取り組む。取組に際しては、内閣官房を中心に、「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）」（2016 年 10 月）を踏まえ、政府及び関係機関が一体となって対応していく。

- 内閣官房において、日・ASEANサイバーセキュリティ政策会議を通じたセキュリティ人材育成の取組や一般向け意識啓発の取組を通じて、ASEAN加盟国の能力構築に貢献する。
- 警察庁において、アジア大洋州地域サイバー犯罪捜査技術会議やJICA課題別研修（サイバー犯罪対処能力向上）、JICA国別研修（サイバーセキュリティ及びサイバー犯罪対処能力強化）の開催等を通じ、アジア大洋州地域をはじめとする各国における能力構築に貢献する。
- 総務省において、日ASEAN情報通信大臣会合を通じて、情報通信分野に関してASEAN域内各国・地域との間でのネットワークセキュリティ分野における能力構築等の連携を推進する。また、APT（アジア・太平洋電気通信共同体）における取組やITU-D等の取組を通じて、研修やセミナーを開催することにより、諸外国に対する意識啓発に取り組む。
- 外務省において、警察庁等とも協力しつつ、第３回日・ASEANサイバー犯罪対策対話や日ASEAN統合基金の活用，UNODCプロジェクトへの拠出を通じて、ASEAN加盟国のサイバー犯罪対策能力構築支援を行う。その他国際機関などと連携したプロジェクトについても検討する。
- 経済産業省において、ASEAN加盟国に対し、ISMS、CSMSに関する研修・セミナー等を通じて、我が国のセキュリティマネジメントに関するノウハウを共有することで、ASEAN加盟国への能力構築支援へ貢献する。
- 経済産業省において、JPCERT/CCを通じ、アジア太平洋地域、アフリカ等において、各国

における対外・対内調整を担うCSIRTの構築及び運用、連携の支援を行う。JPCERT/CCの経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習実施を行う。また、アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、組織内CSIRT構築セミナー等の普及・啓発、サイバー演習の実施等の活動等を行う。さらに、我が国企業が組込みソフトウェア等の開発をアウトソーシングしている先のアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施する。

(イ)経済産業省及び IPA 産業サイバーセキュリティセンター（ICSCoE）が米国土安全保障省及び同省傘下の ICS-CERT と協力し、ASEAN をはじめとしたアジア太平洋地域の国々に対する産業サイバーセキュリティの共同演習実施を通じた能力構築支援を開始する。

4. 横断的施策

4.1. 人材育成・確保

・ 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

（2018 年戦略より）

(ア)内閣官房において、関係府省庁と連携しつつ、「サイバーセキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成取組方針」に基づき、普及啓発・人材育成専門調査会等を通じて、施策間連携を図りつつ、関係施策を促進していく。

(イ)内閣官房において、「サイバーセキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成取組方針」を踏まえ、さまざまな人材育成施策について、施策間の連携を強化するとともに、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」の推進を図る。

(1) 戦略マネジメント層の育成・定着

・ 「戦略マネジメント層」に関する経営層の理解の促進と産業界と連携したその定着
・ 戦略マネジメント層向けの実践的な教材の開発や、指導者の発掘・育成も含め、学び直しプログラムの実践を推進

（2018 年戦略より）

(ア)経済産業省において、IPAに設置した「産業サイバーセキュリティセンター」において、ITとOT双方のスキルを核とした上でビジネススキルやマネジメントスキル・リーダーシップをバランスよく兼ね備えた、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組む。また、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・信頼性を検証する事業も実施し、対策強化に繋げる。

(イ)経済産業省において、IPAの「産業サイバーセキュリティセンター」を通じ、高度な経営判断を補佐する戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニングを行うプログラムを2018年秋から開始する。

(ウ)経済産業省において、セキュリティ教育を提供するため、教える側の質的向上・量的拡充のため、「学」の教員向けにIPA、JPCERT/CCにより、FD（Faculty Development）等の研修機会の提供を実施していく。

(エ)文部科学省において、IT技術者等のサイバーセキュリティに係る素養の向上を図るため、高等教育機関等における社会人学生の受け入れを促進する。

(オ)内閣官房において、戦略マネジメント層を担う人材の育成に向けて、必要な知識・スキルを身に着けるための試行的取組について検討する。

(2) 実務者層・技術者層の育成

・ 学び直しによるスキルの開発や実践的な演習

（2018 年戦略より）

(ア)警察庁において、国立高等専門学校機構と連携し、高等専門学校へのサイバーセキュリティ講義を実施することで、学生のサイバーセキュリティ分野に対する興味・理解を促進し、人材育成とそれに伴う社会全体の対処能力向上を図る。

(イ)都道府県警察において、安全確保等に係る実空間の対処も考慮しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を図る。（再掲）

(ウ)総務省において、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、国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るための新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。

(エ)文部科学省において、高等専門学校におけるセキュリティ教育の強化のための施策として、企業等のニーズを踏まえた技術者のセキュリティ教育に必要な教材・教育プログラム開発を進める。また、並行して、2016年より、段階的に整備を進めてきた情報セキュリティ教育の演習拠点（10拠点）については、日々進歩しているサイバー攻撃技術に対応するため、定期的な環境更新（アップデート）を進めるなど、全国の高等専門学校生が共同で利用できるサイバーレンジ（実践的な演習環境）の提供に向けた取組を推進する。

(オ)厚生労働省において、離職者や在職者を対象として職業に必要な技能及び知識を習得させるため、サイバーセキュリティに関する内容を含む公共職業訓練を実施するとともに、離職者や在職者を対象とした教育訓練給付制度において、サイバーセキュリティに関する内容を含む教育訓練を指定する。

(カ)経済産業省において、情報セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として2016年に開始した情報処理安全確保支援士（登録セキスペ）制度の着実な実施と当該制度の普及のため、企業や団体への周知等を積極的に行う。

(キ)経済産業省において、国家試験である情報処理技術者試験において、組織のセキュリティポリシーの運用等に必要となる知識を問う「情報セキュリティマネジメント試験」の普及を図る。

(ク)内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る。

(ケ)経済産業省において、IPAを通じ、各府省庁、全国各地の関係団体と協力し、インターネットを利用する一般の利用者を対象としてSNSの安全な利用方法を含む情報セキュリティに関する啓発を行うインターネット安全教室を引き続き開催していく。

- 突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保、グローバルに切磋琢磨する機会を広げ、対策を検討できる能力の育成

（2018 年戦略より）

(コ)経済産業省において、若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的としてIPAと「セキュリティ・キャンプ協議会」にて共催しているセキュリティ・キャンプについて、サイバーセキュリティを取り巻く状況の変化への更なる対応を図る。

(サ)経済産業省において、ITを駆使してイノベーションを創出することのできる独創的なアイディア・技術を有する人材の発掘・育成に向け、「未踏IT人材発掘・育成事業」を実施する。

(シ)経済産業省において、情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト「CTF」について、NPO日本ネットワークセキュリティ協会及び企業が共同で開催地域拡大や競技内容の向上を図り、更なる人材候補者を増やすべく、大学等との連携や多様なコンテストの在り方を検討するとともに、同協会で実施するコンテスト（「SECCON 2018」）について普及・広報の支援を行う。

(ス)防衛省において、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。

(セ)防衛省において、自衛隊のサイバー攻撃対処部隊の対処能力の練度を向上させるため、指揮システムを模擬した環境を構築して、攻撃・防御の機能とこれに対する統裁・評価の機能等を備えた実戦的な演習環境を整備する。

(ソ)防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処のための具体的・実効的連携を深化するための取組を実施する。

(3) 人材育成基盤の整備

- 知識・技術体系やそれに基づくモデルカリキュラムの在り方の検討
- 教育課程内での情報活用能力の育成、情報モラル教育
- 教員の研修の充実
- 自由にサイバー関連ツール、機器を用いて興味を持って学べる機会が豊富に用意されるような環境整備
- 大学・高等専門学校等の高等教育段階における情報技術人材の育成

（2018 年戦略より）

(ア)経済産業省において、情報サービスの提供に必要な実務能力を明確化、体系化した共通指標であるITスキル標準の全面的な改訂に向け、第４次産業革命に伴い主流となる新技術に対応するIT人材に焦点を当てたスキル標準の検討を引き続き行う。

(イ)文部科学省において、新学習指導要領の実施を見据え、児童生徒の発達の段階に応じた、プログラミング的思考や情報セキュリティ、情報モラル等を含めた情報活用能力を培う教育を一層推進する。特に、各学校における指導の改善・充実に向けて、教科等横断的な情報活用

能力の育成に係るカリキュラム・マネジメントの在り方や、それに基づく指導方法・教材の利活用等について、実践的な研究を実施する。

(ウ)文部科学省において、2016年11月の教育職員免許法改正及び2017年11月の同法施行規則改正に基づき、ICTを用いて効果的な授業を行ったり、適切なデジタル教材を開発・活用したりすることができる力を教師を志す学生に身に付けさせるため、各教科の指導法を学ぶ科目について、当該教科の特性に応じた情報機器や教材の効果的な活用方法を新たに内容に加えた教員養成課程の審査を行う。

(エ)文部科学省において、独立行政法人教職員支援機構と連携し、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。

(オ)文部科学省において、動画教材や指導手引書も活用して、学校における情報モラル教育の充実を図るため、教員等を対象としたセミナーを実施する。

(カ)総務省において、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」における「SecHack365」の取組を通じて、若年層のICT人材を対象に、高度なセキュリティ技術を本格的に指導し、セキュリティイノベーターの育成に取り組む。

(キ)文部科学省において、複数の大学や産学の連携によるサイバーセキュリティに係る実践的な教育ネットワークの構築やPBL（課題解決型学習）の実施を支援する。

(ク)文部科学省及び経済産業省において、高度なITの知識と経営などその他の領域における専門知識を併せもつハイブリッド型人材の育成を進める。

(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

- 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
- 毎年度、計画の見直しを行い、一層の取組の強化

（2018 年戦略より）

(ア)各府省庁において、内閣官房の主導によりPDCAサイクルを更に充実させることにより、「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」の見直しを行い、体制の整備・人材の拡充、有為な人材の確保、一定の専門性を有する人材の育成や適切な処遇の確保を含む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する。

(イ)各府省庁において、2020年東京オリンピック・パラリンピック競技大会の成功等に向けて、サイバーセキュリティ・情報化審議官等が中心となって、「各府省庁セキュリティ・IT人材確保・育成計画」に沿って引き続き体制の整備と適切な処遇の確保に取り組む。

(ウ)各府省庁のセキュリティ・IT人材を育成・確保するため、内閣官房及び総務省において、情報システム統一研修等各コースの内容の更なる充実に向けた取組を進めるとともに、2018年１月に策定された「橋渡し人材のスキル認定の基準」に基づく橋渡し人材（部内育成の専門人材）のスキル認定が推進されるよう、各府省庁に対する支援等を行う。

(エ)内閣官房において、サイバーセキュリティ・情報化審議官等の研修等を通じて政府機関内における相互の事例共有、意見交換等の継続的な実施を促進する。また、府省庁を対象に、昨今のサイバーセキュリティの動向や課題等に応じたテーマによる勉強会を開催する。

(5) 国際連携の推進

- 国際的な基準を踏まえた人材育成プログラムの認定など海外組織との間での連携を促すための仕組み作り
- 海外におけるサイバーセキュリティ人材の能力構築への貢献

（2018 年戦略より）

(ア)内閣官房において、主要国における取組について調査の上、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を行う。

(イ)経済産業省において、今後、ますますの経済連携が求められるASEAN各国において、我が国企業が安全に活動でき、また、我が国の持つノウハウをASEAN諸国と共有できるよう、セキュリティマネジメント導入のためのノウハウ支援等を行う。

4.2. 研究開発の推進

(1) 実践的な研究開発の推進

- 先進的な技術を用いたサイバーセキュリティ確保の技術、製品・サービスを構成するシステムの中に組み込むセキュリティ技術や、その組み込みの方法に関する実践的な研究開発

（2018 年戦略より）

(ア)総務省において、NICTを通じ、巧妙かつ複雑化したサイバー攻撃や今後本格普及するIoT等への未知の脅威に対応するため、サイバー攻撃観測技術の高度化、機械学習等を応用した通信分析技術やマルウェア自動分析技術の高度化等のアドバンスト・サイバーセキュリティ技術の研究開発を行う。

(イ)文部科学省において、サイバーセキュリティを含む経済・社会的な重要課題を解決につなげることが期待される、量子コンピュータをはじめとした量子科学技術に関する研究開発を推進する。

(ウ)文部科学省において、理化学研究所革新知能統合研究センター（AIPセンター）を通じ、革新的な人工知能基盤技術の構築と、サイバーセキュリティを含む社会的課題の解決に向けた応用研究等を進めていく。あわせて、JSTの戦略的創造研究推進事業において、サイバーセキュリティを含めた研究課題を支援する。

(エ)経済産業省において、AIST等を通じ、IoTシステムに付随する脅威に対応するため、ソフトウェア工学、暗号技術などを用いてシステムのセキュリティ、品質、安全性、効率の向上、などを両立させるための革新的、先端的技術の基礎研究に取り組む。

(オ)経済産業省において、IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバ

一空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、そうした社会を支えるコア技術の調査・研究開発・実証等を行う。

- サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発
- 機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発
- 不正なプログラムや回路が仕込まれていないことの検証を行うための体制の整備とそのための研究開発

（2018 年戦略より）

(カ)経済産業省において、制御システムの挙動を解析し、サイバー攻撃を検知・予測する技術開発や、可用性を確保した脆弱性への対処技術に関する研究を行う。

(キ)内閣府において、関係府省庁と連携して、戦略的イノベーション創造プログラム（SIP）第1期「重要インフラ等におけるサイバーセキュリティの確保」により、2020年東京オリンピック・パラリンピック競技大会を支える重要インフラに導入して有効性を実証し、将来の国内インフラ産業の安定運用やインフラ輸出に貢献するための研究開発・社会実装を行う。本プロジェクトでは、制御・通信機器のセキュリティ確認（機器やソフトウェアの真正性・完全性を確かめること）技術、動作監視・解析技術、異常検知時に制御システムの可用性を重視する防御技術等を開発する。

(ク)内閣府において、戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアなSociety 5.0の実現に向けて、様々なIoT機器を守り、社会全体の安全・安心を確立するため、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を推進する。本プロジェクトでは、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、業務データを安全に流通させるためのトレーサビリティ確保技術、サイバー・フィジカル空間を跨った不正なデータを検知・防御する技術等を開発する。また、本プロジェクトが目指す『サイバー・フィジカル・セキュリティ対策基盤』の実現には、様々な産業分野が関係することから、総務省、経済産業省をはじめとした府省庁及び産学とが分野横断的に連携して推進する。(再掲)

(ケ)総務省において、スマートシティにおけるプラットフォームに係るセキュリティ要件の具体化や所用の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を進める。

(コ)総務省において、戦略的情報通信研究開発推進事業（SCOPE）のなかで、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する。

(サ)内閣官房において、関係府省と連携しつつ、政府機関や重要インフラ事業者等のシステムに組み込まれている機器やソフトウェアについて、不正なプログラムや回路が仕込まれていないことの技術的検証等を行うための体制整備を図るとともに、そのために必要となる研究開発について関係施策を促進していく。

- 政府機関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、攻撃活動を把握、ネットワーク上の脆弱な IoT 機器の調査のための広域ネットワークスキャンの軽量化を目指した研究開発、セキュリティ運用を行う事業者と、国の研究機関等とのリアルタイムでの情報共有を推進

（2018 年戦略より）

(シ)総務省において、NICTを通じ、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の高度化を図り、攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の研究開発を行う。また、サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とするサイバーセキュリティ・ユニバーサル・リポジトリ（CURE）を構築するとともに、CUREに基づく自動対策技術の確立等を行う。

(ス)総務省において、脆弱なIoT機器のセキュリティ対策のため、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャンのための研究開発を行う。

- 計算機技術の発展（例：量子コンピュータ、AI）を意識した暗号技術など安全保障の観点から国として維持することが不可欠な基盤技術の研究開発
- サイバーセキュリティ対策における制度上の課題に関する調査・研究

（2018 年戦略より）

(セ)内閣府において、革新的研究開発推進プログラム(ImPACT)「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」により、機密情報を安全に伝送・保管できる通信ネットワークの構築を目指して量子暗号技術の研究開発を行う。

(ソ)総務省において、NICTを通じ、情報理論的安全性（暗号が情報理論的な意味で無条件に安全である性質）を具備した量子暗号等を活用した量子情報通信ネットワーク技術の確立に向け、研究開発を実施する。

(タ)総務省において、盗聴や改ざんが極めて困難な量子暗号通信を、超小型衛星に活用するための技術の確立に向け、研究開発を実施する。

(チ)内閣官房において、企業が積極的なサイバーセキュリティ対策を講じる上で事業者が特に認識しておくべき関係法令集の作成を念頭に、その体制について検討を行う。(再掲)

(ツ)総務省及び経済産業省において、CRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行う。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT及びIPAを通じ、暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、暗号政策の中長期的視点からの取組の検討を実施するため、暗号技術評価委員会及び暗号技術活用委員会を開催する。(再掲)

- サイバーセキュリティの研究開発の成果の普及や社会実装の推進、海外のイベント等への積極的な参加等を通じた、国際的な情報発信、共同研究の実施や研究成果の国際標準化等の研究開発に係る官民の国際連携の強化

（2018 年戦略より）

(テ)総務省及び経済産業省において、専門機関と連携し、情報セキュリティ分野の国際標準化活動であるISO/IEC JTC1/SC27、ITU-T SG17等が主催する国際会合等に参加し、我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえて国際標準化を推進する。(再掲)

(ト)総務省において、サイバーセキュリティ関連産業の国際展開及びサイバーセキュリティ関連の研究開発の国際的な発信等のため、我が国の関係組織の主要な国際展示会への出展に資する事業を実施する。

(ナ)経済産業省において、IPAを通じ、情報セキュリティ分野と関連の深い国際標準化活動であるISO/IEC JTC1/SC27が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。

(2) 中長期的な技術・社会の進化を視野に入れた対応

- 人文社会学的視点も含めた様々な領域の研究との連携、融合領域の研究を促進

(2018 年戦略より)

(ア)内閣官房において、各府省庁と連携し、信頼性工学、心理学等の様々な社会科学的視点も含めて策定した「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する。

4.3. 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総合的な戦略及び具体的なアクションプランの策定

(2018 年戦略より)

(ア)内閣官房において、「新・情報セキュリティ普及啓発プログラム」の改訂を行い、普及啓発施策の方向性と具体的な行動計画をとりまとめる。

- 必要な情報発信や国民からの相談対応
- 産学官民の様々なコミュニティの代表が参加する協議会の場を活用しながら、関係者による実践を推進

(2018 年戦略より)

(イ)内閣官房において、家庭や教育現場、企業内等でのセキュリティ意識向上のため、緊急時における注意・警戒情報やサイバーセキュリティに関する役立ち情報等について、SNS等を用いた発信を引き続き行うとともに、より効果的な手段について検討を行う。

(ウ)経済産業省において、IPAを通じ、「情報セキュリティ安心相談窓口」、さらに、高度なサイバー攻撃を受けた際の「標的型サイバー攻撃の特別相談窓口」によって、サイバーセキュリティ対策の相談を受け付ける体制を充実させ、一般国民や中小企業等の十分な対策を講じることが困難な組織の取組を支援する。

(エ)内閣官房において、主体的に普及啓発活動を行う動きが地域レベルでも促進されるよう、「情報セキュリティ社会推進協議会」等を活用しつつ、産学官民の連携・協力を通じて、必要な取組について検討を進める。

(オ)総務省、法務省及び経済産業省において、電子署名などのトラストサービスの利活用等に関するセミナーの開催及びHPを活用した情報提供を行うことで、国民による安全なサイバー空間の利用をサポートするとともに、認定認証事業者に対する説明会の開催、民間事業者等からの電子署名に関する相談対応等を行うことで、企業における電子署名の利活用の普及促進策を検討・実施する。

(カ)経済産業省において、IPA、JPCERT/CCを通じて、情報漏えいの新たな手法や手口の情報収集に努め、一般国民や中小企業等に対し、ウェブサイトやメーリングリスト等を通じて対策情報等、必要な情報提供を行う。

(キ)経済産業省において、IPAを通じ、広く企業及び国民一般に情報セキュリティ対策を普及するため、地域で開催されるセミナーや各種イベントへの出展、普及啓発資料の配布、セキュリティプレゼンター制度の運用などにより情報の周知を行い、セキュリティ啓発サイトや各種ツール類を用いて、対策情報の提供を行う。

- 「サイバーセキュリティ月間」のさらなる充実

(2018 年戦略より)

(ク)内閣官房において、行動計画に基づき、NISCが中核的役割を担いつつ、各府省庁や民間の取組主体と協力して、「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進める。

- 国民向けのわかりやすい解説書の作成・普及
- 学校教育を通じた、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

(2018 年戦略より)

(ケ)内閣官房において、サイバーセキュリティに関する基本的な知識を紹介したハンドブックについて、引き続き内容の見直しを行うとともに、普及及び活用を促す取組を行う。

(コ)経済産業省において、個人情報も含む情報漏えい対策に取り組むため、IPAを通じ、ファイル共有ソフトによる情報漏えいを防止する等の機能を有する「情報漏えい対策ツール」を民間の配布サイトも活用して一般国民に提供する。

(サ)総務省において、文部科学省と協力し、青少年やその保護者のインターネットリテラシー向上を図るため、多くの青少年が初めてスマートフォン等を手にする春の卒業・進学・新入学の時期に特に重点を置き、関係府省庁と協力して啓発活動を集中的に展開する「春のあんしんネット・新学期一斉行動」の取組や、「e-ネットキャラバン」等の青少年や保護者等に向けた啓発講座の実施等を行う。また、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通し、インターネット利用における注意点に関する周知啓発の取組を行う。

(シ)文部科学省において、ネットモラルキャラバン隊を通じ、スマートフォン等によるインターネット上のマナーや家庭でのルールづくりの重要性の普及啓発を実施する。

(ス)文部科学省において、独立行政法人教職員支援機構と連携し、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。(再掲)

(セ)文部科学省において、動画教材や指導手引書も活用して、学校における情報モラル教育の充実を図るため、教員等を対象としたセミナーを実施する。(再掲)

(ソ)経済産業省において、IPAを通じ、各府省庁と協力し、情報モラル/セキュリティの大切さを児童・生徒が自身で考えるきっかけとなるように、IPA主催の標語・ポスター・４コマ漫画等の募集及び入選作品公表を行い、国内の若年層における情報モラル/セキュリティ意識の醸成と向上を図る。

(タ)経済産業省において、IPAを通じ、各府省庁と協力し、家庭や学校からインターネットを利用する一般の利用者を対象として情報セキュリティに関する啓発を行う安全教室について、全国各地の関係団体と連携し引き続き開催していく。

- 利用者がサイバーセキュリティの取組を適切に実施できるよう事業者や関係団体等の取組が促進される環境の整備、サイバーセキュリティの確保に資するガイドラインの整備とその着実な実施を推進

(2018 年戦略より)

(チ)総務省において、安全に無線LANを利用できる環境の整備に向けて、引き続き利用者・提供者において必要となるセキュリティ対策に関する検討を行うとともに、利用者・提供者に対する周知啓発を実施する。特に、セキュアな公衆無線LAN環境の実現に向けて、各種ガイドラインの改定や教育コンテンツを活用した周知・啓発、データ利活用施策との連携、セキュアな公衆無線LAN環境の優良事例の調査・整理及びこれを踏まえた所要の政策支援等の取組を行う。

(ツ)経済産業省において、IPAを通じて、サイバーセキュリティに関する現状把握及び対策を実施する際の参考となる最新の動向の収集・分析・報告書の公表等により、サイバー空間利用者への啓発を推進する。

5. 推進体制

(ア) 内閣官房において、関係機関の一層の能力強化に向けて、JPCERT/CCと締結した国際連携活動及び情報共有等に関するパートナーシップの一層の深化を図るため、2015年度に構築した情報共有システムの機能向上を図るとともに連携体制についても逐次見直しを実施する。また、総合的分析機能の強化を図る。さらに、NICTと締結した研究開発や技術協力等に関するパートナーシップに基づいてNICTとの協力体制を整備し、サイバーセキュリティ対策に係る技術面の強化を図る。

(イ) 内閣官房において、2018年戦略に基づく諸施策が着実に実施されるようにするとともに、全ての主体によるサイバーセキュリティに関する自律的な取組を促進するため、各種イベント等における説明会の開催などを通じて、国内外の関係者への2018年戦略の発信を積極的に行い、周知を図る。

(ウ) 内閣官房において、国民の生命等に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力の強化を図るため、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を実施する。（再掲）

(エ) 内閣官房において、「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）」（2017年3月21日セキュリティ幹事会決定）に基づくサイバーセキュリティ対策の強化を引き続き推進する。具体的には、オリパラ競技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と、情報の共有、インシデント発生時の調整役となるための組織である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）の整備を推進する。2018年度のリスク評価は、対象エリアを全国に拡大して実施するとともに特に重要なサービス事業者については国として横断的リスク評価を実施する。また、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）については、2018年度末を目途に構築し、2019年度から要員の訓練、情報共有システムのユーザーに対する操作訓練、情報共有訓練及びインシデント発生時の対応訓練支援が実施できるよう準備する。（再掲）

参考１　用語解説

	用　　語	解　　説
A	AIST	national institute of Advanced Industrial Science and Technologyの略。国立研究開発法人産業技術総合研究所（産総研）。2001年１月６日の中央省庁再編に伴い、通商産業省工業技術院及び全国15研究所群を統合再編し、通商産業省及びその後継の経済産業省から分離して発足した独立行政法人。
	APCERT	Asia Pacific Computer Emergency Response Teamの略。各国・地域におけるCSIRTの活動と連携し、アジア太平洋地域におけるコーディネーションの実施等を行う。
	AppGoat	IPAが無償提供する脆弱性体験学習ツール。学習教材と演習環境がセットになっており、脆弱性の検証手法から原理、影響、対策までを演習しながら学習できる。
	APT	Asia-Pacific Telecommunityの略。アジア太平洋電気通信共同体。アジア・太平洋地域の電気通信の開発促進及び地域電気通信網の整備・拡充を目的として1979年に設立。
	ARF	ASEAN Regional Forumの略。政治・安全保障問題に関する対話と協力を通じ、アジア太平洋地域の安全保障環境を向上させることを目的としたフォーラム。
	ASEAN	Association of South East Asian Nationsの略。東南アジア諸国連合。
B	BCP	Business Continuity Planの略。緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。BCPのうち情報（通信）システムについて記載を詳細化したものがIT-BCP（ICT-BCP）である。
C	CC	Common Criteriaの略。ISO/IEC 15408のこと。情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。
	CCRA	Common Criteria Recognition Arrangementの略。CCに基づいたセキュリティ評価・認証の相互承認に関する協定。
	CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略（セプター）。重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。2005年以降順次構築が進められ、2017年３月末現在、13分野で18セプターが活動。
	CERT/CC	Computer Emergency Response Team/Coordination Centerの略（サートシーシー）。サイバー攻撃情報やシステムの脆弱性関連情報を収集・分析し、関係機関に情報提供等を行っている非営利団体の一般的な名称。複数の国で設立されており、日本にはJPCERT/CCが設置されている。
	CISO	Chief Information Security Officerの略。最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。なお、「政府CISO」は内閣サイバーセキュリティセンター長である。
	CRYPTREC	Cryptography Research and Evaluation Committeesの略。電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT及びIPAが共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成される。
	CSIRT	Computer Security Incident Response Teamの略（シーサート）。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。
	CSMS	Cyber Security Management Systemの略。制御システムのセキュリティマネジメントシステム。
	CTF	Capture The Flagの略。情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト。
	CURE	国立研究開発法人情報通信研究機構（NICT）において研究開発している、サイバーセキュリティ研究及びセキュリティ・オペレーションの遂行に不可欠な各種通信、マルウェア、脆弱性情報、イベント情報、インシデント情報等のサイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする仕組み。
	CVSS	Common Vulnerability Scoring Systemの略。情報システムの脆弱性の深刻度に対するオープンで汎用的な評価手法。

	CYMAT	CYber incident Mobile Assistance Teamの略（サイマット）。我が国の機関等において大規模なサイバー攻撃等により政府として一体となって迅速・的確に対応すべき事態等が発生した際に、機関の壁を越えて連携し、被害拡大防止等について機動的な支援を行うため、2012年６月に内閣官房に設置した体制のこと。
D	DII	Defense Information Infrastructureの略。防衛省の基盤的共通通信ネットワーク。
	DKIM	Domain Keys Identified Mailの略。電子署名を利用した電子メールの送信ドメイン認証技術の一つ。スパムメール、フィッシングメールなどの迷惑メールへの対策の一つとして利用可能。
	DMARC	Domain-based Message Authentication, Reporting &Conformanceの略。電子メールにおける送信ドメイン認証技術の一つであり、SPF・DKIMのドメイン認証技術を利用し、メールの正当性を送信者と受信者間で確認する仕組み。
E	eラーニング	electronic learningの略。情報通信技術を用いた教育、学習のこと。
F	FIRST	Forum of Incident Response and Security Teamsの略。各国のCSIRTの協力体制を構築する目的で、1990年に設立された国際協議会であり、2017年５月現在、世界80ヶ国の官・民・大学等369の組織が参加している。
G	G7	Group of Seven（主要７か国首脳会議）の略。
	GSOC	Government Security Operation Coordination teamの略（ジーソック）。政府機関情報セキュリティ横断監視・即応調整チーム。政府機関等に設置したセンサーを通じた政府横断的な監視、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うためのGSOCシステムを運用する体制のこと。内閣官房内閣サイバーセキュリティセンターにおいて、2008年４月から運用開始。 　近年のサイバー攻撃の複雑・巧妙化を踏まえ、2017年４月に運用開始した第３期GSOCでは、検知・解析機能の強化、センサーの増強等を図っている。また、2017年４月からは、独立行政法人等に対する監視体制（第二GSOC）の運用を開始し、従前からの政府機関に対する監視体制（第一GSOC）と連携を図り、監視体制を強化している。
I	icat	IPAの運営するサイバーセキュリティ注意喚起サービス。ソフトウェア等の脆弱性に関する情報をタイムリーに発信する。
	ICPO	International Criminal Police Organizationの略（インターポール）。国際刑事警察機構。
	ICT	Information and Communications Technologyの略。情報通信技術のこと。
	IoT	Internet of Thingsの略。あらゆる物がインターネットを通じて繋がることによって実現する新たなサービス、ビジネスモデル、又はそれを可能とする要素技術の総称。従来のパソコン、サーバ、携帯電話、スマートフォンのほか、ICタグ、ユビキタス、組込システム、各種センサーや送受信装置等が相互に情報をやり取りできるようになり、新たなネットワーク社会が実現すると期待されている。
	IoT推進コンソーシアム	IoT推進に関する技術の開発・実証や新たなビジネスモデルの創出を推進するための体制を構築することを目的として、2015年10月に設立された産官学が参画・連携する組織。
	IoTセキュリティガイドライン	IoT推進コンソーシアム IoTセキュリティワーキンググループにおいて、2016年７月に策定。IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT機器やシステム、サービスについて、その関係者がセキュリティ確保の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ、明確化することによって、産業界による積極的な開発等の取組を促すとともに、利用者が安心してIoT機器やシステム、サービスを利用できる環境を生み出すことにつなげるもの。
	IPA	Information-technology Promotion Agencyの略。独立行政法人情報処理推進機構。ソフトウェアの安全性・信頼性向上対策、総合的なIT人材育成事業（スキル標準、情報処理技術者試験等）とともに、情報セキュリティ対策の取組として、コンピュータウイルスや不正アクセスに関する情報の届出受付、国民や企業等への注意喚起や情報提供等を実施している独立行政法人。
	ISAC	Information Sharing and Analysis Centerの略。サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。
	ISMS	Information Security Management Systemの略。情報セキュリティマネジメントシステム。
	ISO	International Organization for Standardizationの略。電気及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）における国際標準の策定を行う国際標準化機関。

	ISO/IEC JTC1 SC27	セキュリティコントロールとサービスの分野を対象に、国際規格を策定するISO/IEC JTC1配下の分科委員会。
	ISO/IEC JTC1 SC41	インターネット・オブ・シングスと関連技術の分野を対象に、国際規格を策定するISO/IEC JTC1配下の分科委員会。
	ISP	Internet Service Providerの略。インターネット接続事業者。
	ITPEC	IT Professionals Examination Councilの略。アジア統一共通試験実施委員会。我が国の情報処理技術者試験制度を移入して試験制度を創設した国（６カ国）が協力して試験を実施するための協議会。
	ITU	International Telecommunication Unionの略。国際電気通信連合。国際連合の専門機関の一つ。国際電気通信連合憲章に基づき無線通信と電気通信分野において各国間の標準化と規制を確立することを目的とする。
	ITU-D	International Telecommunication Union Telecommunication Development Sectorの略。ITUの電気通信開発部門。
	ITU-T	International Telecommunication Union Telecommunication Standardization Sectorの略。ITUの電気通信標準化部門。
	IT製品の調達におけるセキュリティ要件リスト	経済産業省及びIPAの共同により、2014年５月に策定。安全性・信頼性の高いIT製品等の利用推進の取組の一つとして、従来の「ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」を改訂したもの。
	ITセキュリティ評価及び認証制度	IT製品・システムについて、そのセキュリティ機能や目標とするセキュリティ保証レベルを、情報セキュリティの国際標準ISO/IEC 15408に基づいて第三者が評価し、結果を公的に検証し、原則公開する制度。
	IWWN	International Watch and Warning Networkの略。サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組の促進を目的とした会合。
J	JC3	Japan Cybercrime Control Centerの略。一般財団法人日本サイバー犯罪対策センター。産学官連携によるサイバー犯罪等への対処のため、日本版NCFTAとして設立された。
	JCMVP	Japan Cryptographic Module Validation Programの略。「暗号モジュール試験及び認証制度」を参照。
	J-CSIP	Initiative for Cyber Security Information sharing Partnership of Japanの略。サイバー情報共有イニシアティブ。IPAを情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取組。
	JHAS	Joint Interpretation Library（JIL）Hardware-related Attacks SWGの略。欧州の認証機関、評価機関、スマートカードベンダ、ユーザーなどからなる作業部会。
	JISEC	Japan Information Technology Security Evaluation and Certification Schemeの略。ITセキュリティ評価及び認証制度を参照。
	JIWG	Joint Interpretation Library（JIL）WGの略。欧州における、スマートカードなどのセキュリティ認証機関からなる技術ワーキンググループ。
	JPCERT/CC	Japan Computer Emergency Response Team/Coordination Centerの略。インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生の状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている機関。特定の政府機関や企業からは独立した組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。 1996年10月に「コンピュータ緊急対応センター」として発足。
	JVN	Japan Vulnerability Notesの略。JPCERT/CCとIPAが共同で管理している脆弱性対策情報提供サイト。
	JVNiPedia	IPAが運営する脆弱性情報データベース。
L	LAN	Local Area Networkの略。企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。
	LGWAN	Local Government Wide Area Networkの略。総合行政ネットワーク。地方公共団体の組織内ネットワークを相互に接続する行政専用ネットワークであり、安全確実な電子文書交換、電子メール、情報共有及び多様な業務支援システムの共同利用を可能とする電子自治体の基盤。

M	M2M	Machine-to-Machineの略。ネットワークに繋がれた機器同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるシステムのこと。例としては、情報通信機器（情報家電、自動車、自動販売機等）や建築物等に設置された各種センサー・デバイスを、ネットワークを通じて協調させ、エネルギー管理、施設管理、経年劣化監視、防災等の多様な分野のサービスを実現するなど。より広義の概念でIoT（Internet Of Things）と呼ばれることもある。
	MOU/NDA	Memorandum Of Understanding/Non-Disclosure Agreementの略。覚書及び秘密保持契約。
	MyJVN	JVNiPedia で配布されている脆弱性チェックツール。PCのソフトウェアが最新か、セキュリティ設定に問題がないか等を確認し、対策が必要な場合は情報へのリンクを提供する。
N	NATIONAL 318(CYBER) EKIDEN	府省庁職員を対象とした、１府12省庁対抗による競技形式のサイバー攻撃対処訓練のこと。
	NCFTA	National Cyber-Forensics and Training Allianceの略。FBI、民間企業、学術機関を構成員として米国に設立された米国の非営利団体。サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。
	NICT	National Institute of Information and Communications Technologyの略。国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を実施するとともに、民間や大学が実施する情報通信分野の研究開発の支援の実施等を行う独立行政法人。
	NII	National Institute of Informaticsの略。国立情報学研究所。大学共同利用機関法人情報・システム研究機構の一員。情報学という新しい学問分野での「未来価値創成」を目指すわが国唯一の学術総合研究所として、ネットワーク、ソフトウェア、コンテンツなどの情報関連分野の新しい理論・方法論から応用までの研究開発を総合的に推進している。
	NISC	National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015年１月９日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長には、内閣官房副長官補（事態対処・危機管理担当）を充てている。
	NIST	National Institute of Standards and Technologyの略。アメリカ国立標準技術研究所。
O	OS	Operating Systemの略。多くのアプリケーションソフトが共通して利用する基本的な機能を提供し、コンピュータシステムを管理する基本ソフトウェア。
P	PBL	Project Based Learningの略。課題解決型学習。
	PDCAサイクル	Plan-Do-Check-Act cycle。事業活動における生産管理や品質管理などの管理業務を円滑に進める手法の一つ。Plan（計画）→Do（実行）→Check（評価）→Act（改善）の４段階を繰り返すことによって、業務を継続的に改善する。
	PP	Protection Profileの略。IT製品のセキュリティ上の課題に対する要件をCCに従って規定したセキュリティ要求仕様。主に調達要件として用いられる。
S	SCAP	Security Content Automation Protocol の略。情報セキュリティにかかわる技術面での自動化と標準化を実現する技術仕様。
	SECCON 2018	SECCON：SECurity CONtest 2018の略。情報セキュリティをテーマに多様な競技を開催する情報セキュリティイベントの2018年における名称。競技を通じた実践的情報セキュリティ人材の発掘・育成、技術実践の場の提供を目的とする。
	SIP	cross-ministerial Strategic Innovation promotion Programの略。戦略的イノベーション創造プログラム。内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。国民にとって真に重要な社会的課題や、日本経済再生に寄与できるような課題に取り組み、基礎研究から実用化・事業化（出口）までを見据えて一気通貫で研究開発を推進する。
	SNS	Social Networking Serviceの略。社会的ネットワークをインターネット上で構築するサービスのこと。友人・知人間のコミュニケーションを円滑にする手段や場を提供したり、趣味や嗜好、居住地域、出身校、「友人の友人」といったつながりを通じて新たな人間関係を構築したりする場を提供する。

	SOC	Security Operation Centerの略。セキュリティサービス及びセキュリティ監視を提供するセンター。
	Society5.0	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。（出典：未来投資戦略2017（平成29年6月9日閣議決定））
	SPF	Sender Policy Frameworkの略。電子メールにおける送信ドメイン認証の一つ。差出人のメールアドレスが他のドメインになりすましていないかどうかを検出することができる。
	STARDUST	国立研究開発法人情報通信研究機構（NICT）において研究開発している、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サイバー攻撃誘引基盤。
T	TSUBAME	JPCERT/CCが運営するインターネット定点観測システム。Internet上に観測用センサーを分散配置し、セキュリティ上の脅威となるトラフィックの観測を実施。得られた情報はウェブサイト等を通して提供されている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	安全なIoTシステムのためのセキュリティに関する一般的枠組	NISCにおいて、2016年８月に策定。従来の情報セキュリティの確保に加え、新たに安全確保が重要なIoTシステムは、セキュリティ・バイ・デザインの思想で設計、構築、運用されることが不可欠であるため、安全なIoTシステムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにしたもの。
い	イノベーション	新技術の発明や新規のアイデア等から、新しい価値を創造し、社会的変化をもたらす自発的な人・組織・社会での幅広い変革のこと。
	インシデント	中断・阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
か	カウンターインテリジェンス	外国の敵意ある諜報活動に対抗する情報防衛活動のこと。
	可用性	情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること（Availability）。
	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity）。
き	機密性	情報に関して正当な権限を持った者だけが、情報にアクセスできること（Confidentiality）。
く	クラウドサービス	インターネット等のブロードバンド回線を経由して、データセンタに蓄積されたコンピュータ資源を役務（サービス）として、第三者（利用者）に対して遠隔地から提供するもの。なお、利用者は役務として提供されるコンピュータ資源がいずれの場所に存在しているか認知できない場合がある。
	クラウドサービス提供における情報セキュリティ対策ガイドライン	総務省において、2014年４月策定。2018年７月改定。クラウドサービス利用の進展状況等に対応するため、クラウドサービス提供事業者が留意すべき情報セキュリティ対策に関するガイドライン。
こ	高度サイバー攻撃対処のためのリスク評価等のガイドライン	2016年10月７日サイバーセキュリティ対策推進会議（CISO等連絡会議）決定。政府機関等における情報及び情報システムに係る情報セキュリティ水準の一層の向上及びサイバー攻撃への対処体制の充実・強化に資するために策定されたもの。
	コーポレート・ガバナンス・システム	会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組みに関するシステム。
	コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ定めたもの。
さ	サイバーインテリジェンス	情報通信技術を用いた諜報活動のこと。
	サイバー攻撃特別捜査隊	サイバー攻撃対策の強化のため、14都道府県警察に設置。サイバー攻撃に関する情報収集、被害の未然防止及び犯罪捜査に専従している。
	サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、戦略の策定その他当該施策の基本となる事項等を定めた法律。2014年11月12日公布・一部施行、2015年１月９日完全施行。

	サイバーセキュリティ経営ガイドライン	経済産業省及びIPAの共同により、2015年12月にVer1.0を策定。大企業および中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためのガイドライン。
	サイバーセキュリティ月間	サイバーセキュリティについて国民に広く普及啓発するため、2009年より毎年２月に実施してきた「情報セキュリティ月間」を、2015年より、２月１日から３月18日（「サイバーの日」）までに期間を拡大したもの。月間の期間中、サイバーセキュリティについて、「知る・守る・続ける」をキャッチフレーズに、普及啓発に関する行事や関連キャンペーン等を行っている。
	サイバーセキュリティ研究開発戦略	情報通信技術の進化や、人間と情報の関わり方が変化していることを意識しつつ、近い将来及び中長期的な将来における、サイバーセキュリティ研究開発の方向性についてビジョンを提示した文書。
	サイバーセキュリティ人材育成プログラム	サイバーセキュリティ関連人材の育成の方向性を示した「サイバーセキュリティ人材育成プログラム」を2017年４月18日にサイバーセキュリティ戦略本部にて決定。
	サイバーセキュリティ戦略（2018年戦略）	我が国のサイバーセキュリティ政策に関する国家戦略であり、2015年９月４日に閣議決定された前戦略からのサイバー空間に係る現状認識を踏まえ、目指すサイバーセキュリティの基本的な在り方として、「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」を位置づけており、今後３年間の諸施策の目標及び実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるもの。
	サイバーセキュリティ戦略本部	2015年１月９日、サイバーセキュリティ基本法に基づき内閣に設置された。我が国における司令塔として、サイバーセキュリティ戦略の案の作成及び実施の推進、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を事務としてつかさどる。本部長は、内閣官房長官。
	サイバーテロ対策協議会	警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等との間で構成する組織。全国の都道府県に設置されており、サイバー攻撃の脅威や情報セキュリティに関する情報共有のほか、サイバー攻撃の発生を想定した共同対処訓練やサイバー攻撃対策セミナー等の実施により、重要インフラ事業者等のサイバーセキュリティや緊急対処能力の向上に努めている。
	サイバーフォースセンター	サイバー攻撃対策の技術的基盤として、警察庁情報通信局に設置。サイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析を実施するほか、事案発生時には技術的な緊急対処の拠点として機能する。
	サプライチェーン	取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。
	産業サイバーセキュリティ研究会	経済産業省において設置された研究会。我が国の産業が直面する、深刻度を増しているサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される。
し	事業継続計画	BCPを参照。
	重要インフラサービス	重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続のうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに定めるもの。
	重要インフラサービス障害	重要インフラの情報セキュリティ対策に係る第４次行動計画において新設した用語。システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。
	重要インフラ所管省庁	重要インフラの情報セキュリティ対策に係る第３次行動計画及び同第４次行動計画における関係主体の一つ。金融庁、総務省、厚生労働省、経済産業省及び国土交通省。
	重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書	2018年４月４日サイバーセキュリティ戦略本部決定。情報セキュリティ確保に係るリスクアセスメントの考え方や具体的な作業手順に関するフレームワークを提供することにより、重要インフラ事業者等におけるリスクアセスメントの理解を深め、その精度や水準の向上に寄与するとともに、重要インフラ事業者等による自律的な情報セキュリティ対策を促進することを目的としているもの。
	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	2017年４月18日サイバーセキュリティ戦略本部決定。昨今のサイバー攻撃による急速な脅威の高まりや、2020東京オリンピック・パラリンピック競技大会も見据え、安全かつ持続的なサービスの提供に努めるという機能保証の考え方に基づき、第３次行動計画を見直したもの。「重要インフラ行動計画」、「第４次行動計画」と略称を使うことがある。

	重要インフラ分野	情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット及び石油。重要インフラの情報セキュリティ対策に係る第４次行動計画において記載。
	情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。（JIS Q 27000:2014）
	情報セキュリティ関係機関	重要インフラの情報セキュリティ対策に係る第３次行動計画及び同第４次行動計画における関係主体の一つ。警察庁サイバーフォースセンター、国立研究開発法人情報通信研究機構（NICT）、国立研究開発法人産業技術総合研究所（AIST）、独立行政法人情報処理推進機構（IPA）、一般社団法人ICT-ISAC、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）。
	情報セキュリティ政策会議	2005年５月、IT総合戦略本部の下に設置された会議。内閣官房長官を議長とし、我が国の情報セキュリティに関する諸問題に係る対策等を決定する。サイバーセキュリティ戦略本部に業務が引き継がれ、2015年６月に廃止。
	情報セキュリティ普及啓発プログラム	今後推進すべき新たな普及啓発の進め方についてまとめたプログラム。2011年７月８日情報セキュリティ政策会議決定。改定版である新・情報セキュリティ普及啓発プログラムは2014年７月10日情報セキュリティ政策会議改定。
	情報通信ネットワーク安全・信頼性基準	1987年２月14日郵政省告示第73号。情報通信ネットワークのうち社会的に重要なもの又はそれに準ずるものを対象とし、その安全・信頼性対策の指標としての基準を定めることにより、安全・信頼性対策の普及を促進し、もって情報通信ネットワークの健全な発展に寄与することを目的としているもの。
す	スマートフォン	従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末。従来の携帯電話端末とは異なり、利用者が使いたいアプリケーションを自由にインストールして利用することが一般的。
せ	制御系	センサーやアクチュエータなどのフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPCなどをネットワークで接続した機器群をさす。
	セキュリティ・キャンプ協議会	次代を担う日本発で世界に通用する若年層のセキュリティ人材を発掘・育成するため、産業界、教育界を結集した講師による「セキュリティ・キャンプ」（22歳以下を対象）を実施し、それを全国的に普及、拡大していくことを目的とした協議会。なお、同協議会は2018年４月24日に「一般社団法人セキュリティ・キャンプ協議会」となったことが発表されている。
	セキュリティ・バイ・デザイン	システムの企画・設計段階から情報セキュリティの確保を盛り込むこと。
	セプター	CEPTOAR （Capability for Engineering of Protection, Technical Operation, Analysis and Response）を参照。
た	大規模サイバー攻撃事態	国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態。例えば、サイバー攻撃により、人の死傷、重要インフラサービスの重大な供給停止等が発生する事態。
つ	つながる世界の開発指針	IPAにおいて、2016年３月に策定、2017年６月に第２版へ改訂。様々なモノがつながって新たな価値を創出していく『つながる世界』ならではの機器やシステムに関わる企業が安全安心に関して最低限考慮すべき事項をとりまとめたもの。
て	デジタルフォレンジック	不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
	テストベッド	技術や機器の検証・評価のための実証実験、又はそれを行う実験機器や条件整備された環境のこと。
	電気通信事業における個人情報保護に関するガイドライン	2017年４月18日総務省告示第152号。同年９月14日総務省告示第297号最終改正。電気通信事業の公共性及び高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、通信の秘密に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めることにより、電気通信役務の利便性の向上を図るとともに、利用者の権利利益を保護することを目的とするもの。
	電子署名	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。

と	統一基準群	国の行政機関、独立行政法人及び指定法人の情報セキュリティを確保するため、これらのとるべき対策の統一的な枠組みについて定めた一連のサイバーセキュリティ戦略本部決定文書等のこと。「政府機関の情報セキュリティ対策のための統一規範」、「政府機関等の情報セキュリティ対策の運用等に関する指針」、「政府機関の情報セキュリティ対策のための統一基準」（2016年８月31日サイバーセキュリティ戦略本部決定）及び「府省庁対策基準策定のためのガイドライン」（2016年８月31日内閣官房内閣サイバーセキュリティセンター決定）。
な	内閣サイバーセキュリティセンター	NISCを参照。
	ナショナルサイバートレーニングセンター	2017年４月、実践的なサイバートレーニングを企画・推進する組織としてNICTに設置されたもの。
	なりすまし	他の利用者のふりをすること。または、中間者（Man-in-the-Middle）攻撃など他の利用者のふりをして行う不正行為のこと。例えば、その当人であるふりをして電子メールを送信するなど、別人のふりをして電子掲示板に書き込みを行うような行為が挙げられる。
に	日米サイバー対話	サイバー空間を取り巻く諸問題についての日米両政府による包括対話。（第１回：2013年５月、第２回：2014年４月、第３回：2015年７月、第４回：2016年７月、第５回：2017年７月）
は	ハッキング	高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。不正にコンピュータを利用する行為全般のことをハッキングと呼ぶこともあるが、本来は悪い意味の言葉ではない。そのような悪意のある行為は、本来はクラッキングという。
ひ	ビッグデータ	利用者が急激に拡大しているソーシャルメディア内のテキストデータ、携帯電話・スマートフォンに組み込まれたGPS（全地球測位システム）から発生する位置情報、時々刻々と生成されるセンサーデータなど、ボリュームが膨大であるとともに、従来の技術では管理や処理が困難なデータ群。
	秘密情報の保護ハンドブック～企業の価値向上に向けて～	経済産業省において、2016年２月に策定。秘密情報の漏えいを未然に防ぐため、企業が対策を行う際の参考となる対策例を紹介するもの。
	秘密情報の保護ハンドブックのてびき～情報管理も企業力～	経済産業省において、2016年12月に策定。「秘密情報の保護ハンドブック～企業の価値向上に向けて～」について、活用しやすいようにわかりやすくまとめたもの。
	標的型攻撃	特定の組織や情報を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）などを窃取、又は、組織等のシステムを破壊・妨害しようとする攻撃。標的型攻撃の一種として特定のターゲットに対して様々な手法で持続的に攻撃を行うAPT（Advanced Persistent Threat）攻撃がある。
ふ	フィッシング	実在の金融機関、ショッピングサイトなどを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、銀行口座番号、クレジットカード番号やパスワード、暗証番号などの重要な情報を入力させて詐取する行為のこと。
	フィッシング対策協議会	フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策を促進することを目的として、2005年４月28日に設立された協議会。
	不正アクセス	ID・パスワード等により利用が制限・管理されているコンピュータに対し、ネットワークを経由して、正規の手続を経ずに不正に侵入し、利用可能とする行為のこと。
	不正プログラム	情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称。
へ	ベストプラクティス	優れていると考えられている事例やプロセス、ノウハウなど。

	ペネトレーションテスト	情報システムに対する侵入テストのこと。「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015年５月25日サイバーセキュリティ戦略本部決定）においては、「インターネットに接続されている情報システムについて、疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。なお、インターネットとの境界を突破できた場合を仮定して、内部ネットワークについても、サイバーセキュリティ対策上の問題を検証し、改善のために必要な助言等を行う。」とされている。
ほ	ボットネット	マルウェアに感染したコンピュータ等により構成されたネットワークであり、攻撃者はネットワークを構成するコンピュータ等に対して一斉に指令を与えることができる。
	ポータルサイト	インターネットにアクセスする際の入口となるウェブサイト。
ま	マイナポータル	政府が運営するオンラインサービス。子育てに関する行政手続きがワンストップでできたり、行政機関からのお知らせを確認できたりするポータルサイトのこと。
	マルウェア	malicious software の短縮された語。不正かつ有害な動作を行う、悪意を持ったソフトウェアのこと。
み	未踏IT人材発掘・育成事業	2000年度から「未踏ソフトウェア創造事業」として開始し、2008年度により若い人材の発掘・育成に重点化すべく「未踏IT人材発掘・育成事業」として再編したもの。
り	リスクマネジメント	リスクを組織的に管理し、損失などの回避・低減等を図るプロセスのこと。
	リテラシー	本来、文字を読み書きする能力を意味するが、「情報リテラシー」のように、その分野における知識、教養、能力を意味することに使われている。
	量子暗号	量子力学の原理を用いた暗号技術。原理的に盗聴の有無を検知できる特性を持つ。

参考 2　担当府省庁一覧

項目	担当府省庁 （◎：主担当、○：関係府省庁）
1.　経済社会の活力の向上及び持続的発展	
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
(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
(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
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
(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）
(3)　中小企業の取組の促進	◎：NISC、総務省、経済産業省
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
(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
2.　国民が安全で安心して暮らせる社会の実現	
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）
(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
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
(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
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
(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
(3)　先端技術の活用による先取り対応への挑戦	◎：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
(5)　組織的な対応能力の充実	◎：NISC、総務省 ○：人事院
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
(2)　大学等の連携協力による取組の推進	◎：文部科学省
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
(2)　未来につながる成果の継承	◎：NISC、警察庁、総務省、法務省
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
(1)　多様な主体の情報共有・連携の推進	◎：NISC
(2)　情報共有・連携の新たな段階へ	◎：NISC
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
3.　国際社会の平和・安定及び我が国の安全保障への寄与	
3.1　自由、公正かつ安全なサイバー空間の堅持	◎：NISC ○：外務省
(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
(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
3.2　我が国の防御力・抑止力・状況把握力の強化	
(1)　国家の強靭性の確保	◎：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
(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
(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
3.3　国際協力・連携	◎：NISC ○：その他の府省庁
(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
(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
(3)　能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省
4.　横断的施策	
4.1　人材育成・確保	◎：NISC ○：総務省、文部科学省、経済産業省
(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
(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

		(3)　人材育成基盤の整備	◎：総務省、文部科学省、経済産業省
		(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
		(5)　国際連携の推進	◎：NISC、経済産業省
	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）
		(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
	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
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）