資料２

サイバーセキュリティ戦略（案）

資料２－１　新たなサイバーセキュリティ戦略

～政府機関等のサイバーセキュリティ対策の抜本的強化～

資料２－２　サイバーセキュリティ戦略（案）の概要

※資料２－３　サイバーセキュリティ戦略（案）

資料２－４　「サイバーセキュリティ戦略（案）」に対する

意見募集の結果の概要

※資料２－５　「サイバーセキュリティ戦略（案）」に対する

意見募集の結果

※は、席上配布省略。

資料２－１

新たなサイバーセキュリティ戦略
～政府機関等のサイバーセキュリティ対策の抜本的強化～

平成27年8月

内閣官房内閣サイバーセキュリティセンター

政府機関等のサイバーセキュリティ対策の抜本的強化（1/3）

日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策について、所要の法改正を含め、抜本的な強化を図る。

（注）「日本再興戦略」改訂2015（平成27年6月30日閣議決定）に盛り込まれた施策を含む追加的施策を新たなサイバーセキュリティ戦略に盛り込み、積極的かつ総合的に推進する。

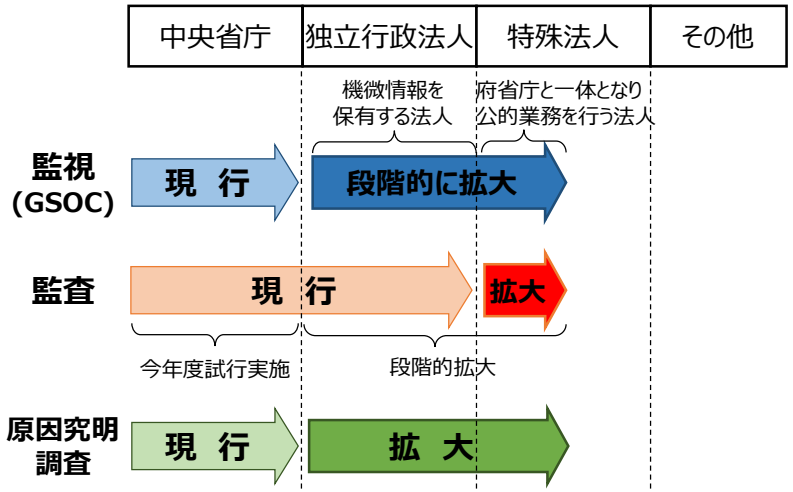
1．NISCの機能強化

■ GSOCの大幅な機能強化

- 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）システムの検知・解析機能及び運用体制の強化

■ 業務対象の拡大等

- 監視・監査・原因究明調査業務の対象について、政府機関（中央省庁）に加え、独立行政法人、政府機関と一体となって公的業務を行う特殊法人等に段階的に拡大（所要の法改正について速やかに検討）



■ 連携推進体制の強化

- 独立行政法人情報処理推進機構（IPA）及び国立研究開発法人情報通信研究機構（NICT）をはじめ、大規模なサイバー攻撃への対処等に対する知見を有する者との積極的な連携（所要の法改正について速やかに検討）

■ NISCの要員強化

- 高度セキュリティ人材の民間登用等による対処能力の一層の強化

政府機関等のサイバーセキュリティ対策の抜本的強化（2/3）

２．政府全体の取組強化

■ 政府機関における体制強化

- 政府機関等におけるインシデント対応チーム（CSIRT）体制の強化
- 初動対処に向けた組織的対応体制（幹部を含む。）の構築や政府全体の実践的訓練の実施等による危機管理体制の強化

■ 攻撃リスク低減のための対策強化（対策強化のための方針を早急に策定）

- インターネット接続口の更なる集約化
- 標的型攻撃に対する多重防御の取組の加速化
- 大量の個人情報等の重要情報を取り扱う情報システムのインターネットからの分離
- 政府機関における全面的なクラウドサービスへの移行を見据えた対策の強化

■ 人材・予算の確保

- 行政機関におけるセキュリティ人材の育成促進
- 所要の予算について行政効率化等により節減した費用等をサイバーセキュリティ対策へ振り向け（「サイバーセキュリティ関係施策に関する平成28年度予算重点化方針」に基づき、IoTセキュリティの確保、政府機関の対策強化、人材育成等に重点）

政府機関等のサイバーセキュリティ対策の抜本的強化（3/3）

3． その他の重要課題への取組強化

■ 重要インフラに関する取組強化（本年中を目途に具体策を決定）

- 社会環境の変化や既存の知見の集積等を踏まえ、重要インフラの対象範囲を見直し（継続実施）
- 情報共有環境の構築と体制の整備、及び演習・訓練の実施による継続的改善

■ セキュリティ人材の育成のための演習環境の整備（本年度中に人材育成総合強化方針(仮称)を策定）

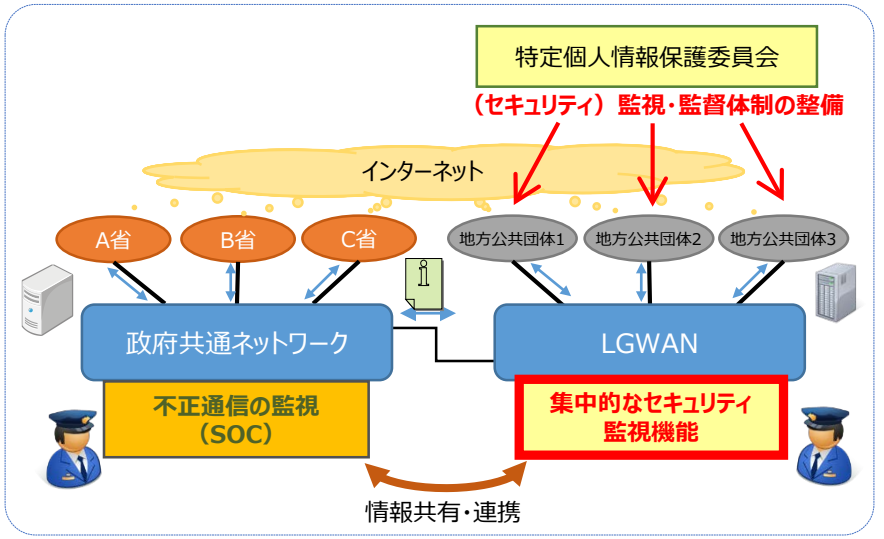
- クラウド環境の実践的な演習環境の整備等（国立研究開発法人情報通信研究機構（NICT）との積極的な連携）

■ 即応予備チームの体制整備

- 政府機関、独立行政法人、民間企業等から緊急時の対処チームへの参加等を可能とする体制の整備（法改正について速やかに検討）

■ マイナンバー制度の円滑な導入に向けた対策の強化

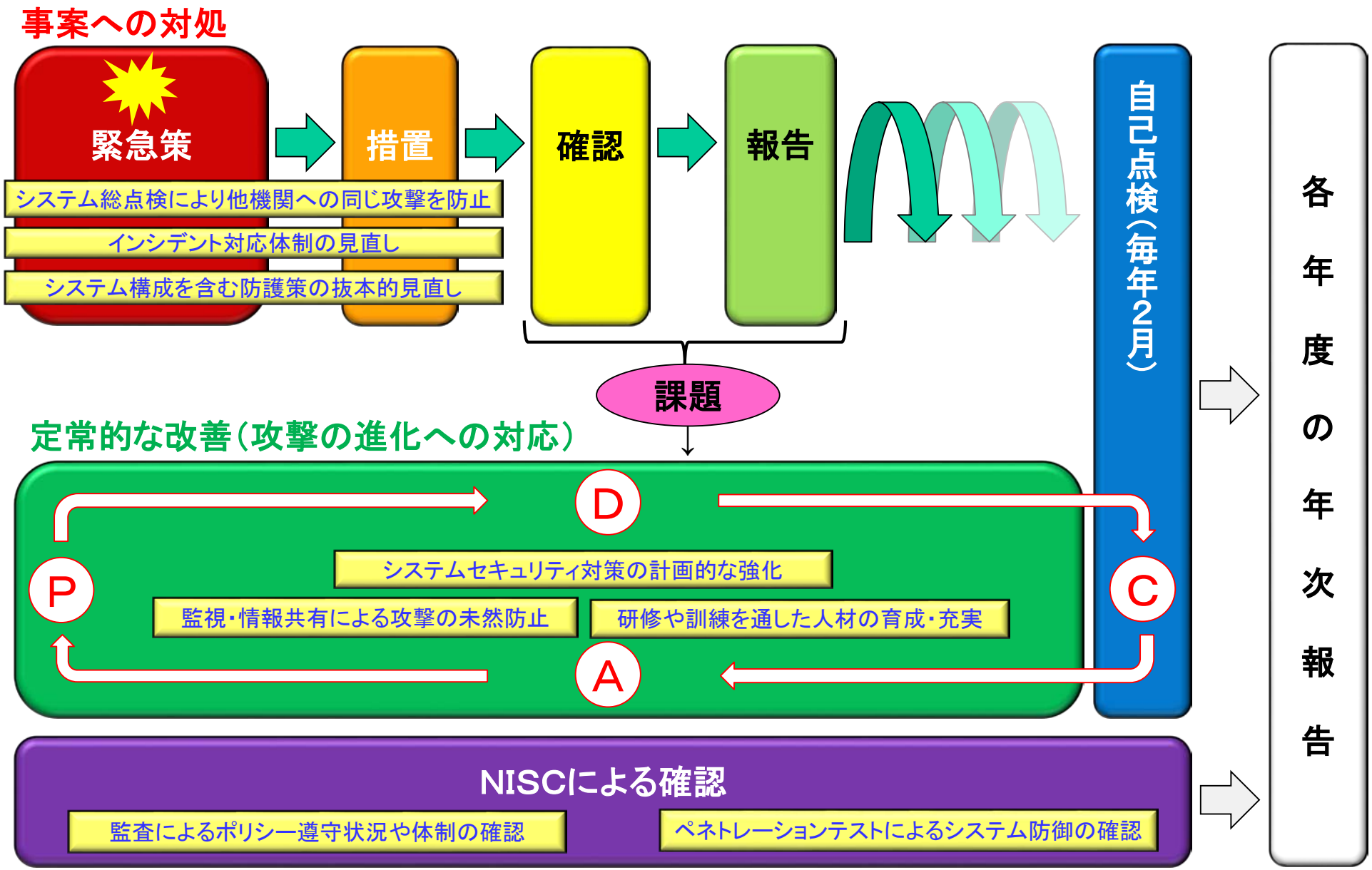
- 特定個人情報保護委員会において、関係機関と連携して監視・監督体制を整備（本年度中を目途）
- 総合行政ネットワーク（LGWAN）について集中監視機能を設ける等、GSOCとの連携による国・地方を俯瞰した監視・検知体制を整備
- 官民連携を実現する認証連携のための枠組みの取組方針を策定（本年中を目途）



■ 事案対処に関する取組強化

- サイバー攻撃を組織的に行う集団等の動向分析と捜査機関等との情報共有
- 対処機関における能力の質的・量的向上

政府機関等における継続的なセキュリティ対策強化の考え方



（参考）日本年金機構事案を踏まえた議長指示

（平成27年8月19日　サイバーセキュリティ対策推進会議資料）

	各府省庁	独立行政法人等
類似手口の点検・再発防止	① 6月1日付 ・システムの点検 ・職員及び独法等への指導指示　対応済	② 6月11日付 ・システムの点検等　対応済
連絡・対応体制	③ 6月19日付 ・CSIRT体制、対処手順等の確認　対応済 ⑤ 7月10日付 ・CSIRT体制・連絡体制等の強化　対応中	⑥ 7月22日付 ・CSIRT体制、対処・連絡手順の整備等　対応中
将来的な対策	④ 7月1日付 ・重要情報のインターネットとの分離計画等　対応済 ⑦ 8月7日付 ・インターネット接続口の集約化計画　対応中	⑥ 7月22日付 ・監視・監査の実施に向けた対応　対応中 ⑦ 8月7日付 ・インターネット接続口の集約化の慫慂　対応中
監視	GSOC	対象範囲拡大

新たな「サイバーセキュリティ戦略」について（全体構成）

資料2－2

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会**（**連融情報社会**）」が到来
  同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「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。

3 基本原則

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

4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■ **安全なIoTシステムの創出**
安全なIoT活用による新産業創出

■ **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備

■ **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■ **国民・社会を守るための取組**
事業者の取組促進、普及啓発、サイバー犯罪対策

■ **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化

■ **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■ **我が国の安全の確保**
警察・自衛隊等のサイバー対処能力強化

■ **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進

■ **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

横断的施策

■ **研究開発の推進**
攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■ **人材の育成・確保**
ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

新たな「サイバーセキュリティ戦略」について（総論）

1.サイバー空間に係る認識　2.目的　3.基本原則

➢ 本戦略は、2020年オリンピック・パラリンピック東京大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後3年程度の基本的な施策の方向性を示すもの。

1　サイバー空間に係る認識

➢ サイバー空間は「国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」である人工の空間で、経済社会の活動基盤である。

➢ 実空間のモノやヒトが、サイバー空間により物理的制約を超えて連接することで、実空間とサイバー空間の融合が高度に深化した「連接融合情報社会(連融情報社会)」が到来しつつある。

➢ 一方、国民生活・経済社会活動への重大な被害や我が国の安全保障に対するサイバー脅威も高まっている。今後、こうした脅威が更に深刻化することが予想される。

2　目的

➢ 「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。

3　基本原則

本戦略の目的達成のための施策の立案及び実施に当たり、以下に示す基本原則に従う。

① 情報の自由な流通の確保：サイバー空間発展の基盤として、情報の自由な流通が保証された空間を維持

② 法の支配：実空間と同様にサイバー空間に対しても「ルールや規範」の適用を徹底

③ 開放性：常に参加を求める者に開かれ、新たな価値を生み出す空間として保持

④ 自律性：各者の主体的な行動により、悪意ある行動を抑止する自律的メカニズムを推進

⑤ 多様な主体の連携：様々な主体の適切な連携関係構築とダイナミックな対処策実現

我が国は、上記の５つの基本原則に従うとともに、国民の安全・権利の保障のため、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。

新たな「サイバーセキュリティ戦略」について（各論①）

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 ～費用から投資へ～

■安全なIoTシステムの創出

- 企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン(SBD)の考え方に基づき、安全なIoT(モノのインターネット)システムを活用した事業を振興
- IoTシステムに係る大規模な事業について、サイバーセキュリティ戦略本部による総合調整等により、必要な対策を整合的に実施するための体制等を整備
- エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドライン等を整備
- IoTシステムの特徴(長いライフサイクル、処理能力の制限等)、ハードウェア真正性の重要性等を考慮した技術開発・実証事業の実施

■セキュリティマインドを持った企業経営の推進

- 企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築(経営ガイドライン等の発信含む)
- 経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成
- 民民間・官民間における脅威・インシデント情報の共有網の拡充

■セキュリティに係るビジネス環境の整備

- 政府系ファンドの活用等により、サイバーセキュリティ関連産業を振興(ベンチャー企業の育成等を含む)
- 中小企業等のクラウドサービス活用に有効なセキュリティ監査の普及促進
- サイバーセキュリティ産業の振興に向けた制度の見直し(リバースエンジニアリング等)
- IoTシステムのセキュリティに係る国際的な標準規格や相互承認枠組み作りの国際的議論を主導
- 知財漏えい防止強化など、公正なビジネス環境を整備

▲自動運転車の実証実験

新たな「サイバーセキュリティ戦略」について（各論②）

4.目的達成のための施策

国民が安全で安心して暮らせる社会の実現 ～2020年・その後に向けた基盤形成～

■国民・社会を守るための取組

- ソフトウェア等の脆弱性関連情報の収集やインターネット上の各種のサイバー攻撃等観測システムの連携・強化の推進
- 攻撃を受けた端末の利用者に対する注意喚起等の推進
- 整備が進む公衆無線LAN等のセキュリティ確保のための対策検討
- 地域における普及啓発活動の促進、中小企業や地方公共団体への啓発・支援
- サイバー犯罪への対処能力・捜査能力の向上に向けた取組の強化
  （通信履歴の保存の在り方についての関係事業者における適切な取組の推進を含む）

▲双方向型の普及啓発セミナー（サイバーセキュリティカフェ）

■重要インフラを守るための取組

- 重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し
- より効果的かつ迅速な官民の情報共有、政府機関内での必要な連携、訓練・演習の実施の推進
- マイナンバー制度の円滑な運用確保のため地方公共団体に必要な政策を実施し、国・地方の全体を俯瞰した監視・検知体制や、専門的・技術的知見を有する監視・監督体制を整備
- スマートメーター等の制御系について、国際標準に即した第三者認証制度の活用等を推進


▲サイバー攻撃等に対する対応能力向上のための演習
（重要インフラ分野横断的演習）

■政府機関を守るための取組

- ペネトレーションテスト等を通じたセキュリティ対策を徹底、サプライチェーン・リスクへの対応、政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能強化、 標的型攻撃に対する多重防御の取組加速等による防御力の強化
- マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化
- 新たなIT製品・サービスの特性を踏まえた政府統一的なセキュリティ対策の策定・推進
- 独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等への監視・監査・原因究明調査の実施等による総合的な対策強化

新たな「サイバーセキュリティ戦略」について（各論③）

4.目的達成のための施策

国際社会の平和・安定及び我が国の安全保障 ～サイバー空間における積極的平和主義～

■我が国の安全の確保

- 警察や自衛隊を始めとする対処機関の能力の質的・量的な向上
- 安全保障上重要な先端技術（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）に係るサイバーセキュリティの確保
- 政府機関や重要インフラ事業者等によるサービスの持続的提供のための情報の共有・分析・対応に向けた官民連携の一層の強化

▲日ASEAN情報セキュリティ政策会議

■国際社会の平和・安定

- 国連等におけるサイバー空間に係る国際的なルール等の形成に向けた積極的な貢献
- サイバー空間を悪用する国際テロ組織に対する国際社会と連携した対処
- 各国の能力構築（キャパシティビルディング）への積極的な協力の推進

▲我が国で開催したサイバーセキュリティに関する国際カンファレンス（Meridian Conference 2014）

■世界各国との協力・連携

- アジア大洋州 ： 日・ASEAN間の協力関係の更なる深化・拡大並びに地域の戦略的パートナーとの協力・連携の強化
- 北米 ： 同盟国たる米国とあらゆるレベルでの緊密な連携・対応（日米サイバー対話、インターネットエコノミーに関する日米政策協力対話、日米サイバー防衛政策ワーキンググループ等）
- 欧州・中南米・中東アフリカ ： 基本的価値観を共有する国々とのパートナーシップの構築・強化

新たな「サイバーセキュリティ戦略」について（各論④・推進体制）

4.目的達成のための施策　　5.推進体制

横断的施策

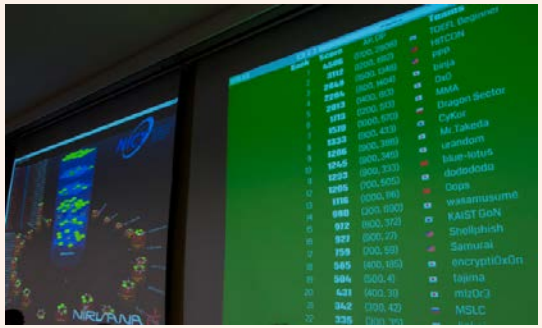
■研究開発の推進

- 関係者間の情報・データの共有等によるサイバー攻撃の検知・防御能力の一層の向上
- 融合領域の研究促進、及び安全保障のためのコア技術(暗号技術等)の保持
- 各国が強みを有する技術を有機的に組み合わせた国際連携による研究開発の推進

▲ 合宿形式で知識・技能を学ぶセキュリティキャンプ

■人材の育成・確保

- 他分野の知識も併せ持つハイブリッド型人材の育成促進
- 高等教育等における産学官連携の推進・実践的演習の充実
- 初等中等教育段階からの教育の充実
  (論理的思考力やモノの基礎的動作原理の理解促進、教員の指導力向上に向けた研修等の改善・充実)
- サイバー演習環境のクラウド環境における整備、産学官共同による教材開発の支援
- 国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保
- 実践的能力を評価する資格制度の創設、標準的なスキルの基準の整備等の推進



▲ 58ヶ国が参加したセキュリティコンテスト(2014年度)

5 推進体制

- NISC対処能力の一層の強化や産学官及び関係省庁間の連携強化によるサイバー攻撃の検知・分析・判断・対処の機能強化
- 国家の関与が疑われる高度な攻撃に対し、戦略本部とNSC(安全保障)・重大テロ対策本部(危機管理)と緊密に連携
- オリンピック・パラリンピック東京大会等に向け、リスクの明確化、組織・施設・協力関係の構築・維持、十分な訓練を実施

- 戦略本部は、各年度の年次計画及び年次報告を作成するとともに、経費見積り方針を策定する。

資料２－３

サイバーセキュリティ戦略（案）

2015 年〇月

目次

1. 策定の趣旨

20 世紀後半から 21 世紀初頭にかけて、世界は不可逆的に大きな変革を遂げた。あたかもグーテンベルクの活版印刷が知の爆発を引き起こしたように、コンピュータとインターネットの発明と普及により、人々は、場所や時間の制約にとらわれずに、世界中の人と議論し、おもいを共有することができるようになった。無数のコンピュータ、センサー、駆動装置が情報通信技術（IT）によりネットワーク化されることで創出されるサイバー空間は、実空間における人間の行動を大いに拡張した。サイバー空間を通じた世界各地における情報発信とそれに基づく自由闊達（かったつ）な議論は、世界の自由主義社会と民主主義の基盤である。また、このデジタル空間は、新たなビジネスモデルと技術革新を生み出し続けており、経済成長のフロンティアとなっている。

しかし、このサイバー空間という新たな領域において、悪意ある行動が広がっている。例えば、人々や企業・組織の情報・財産が次々と窃取されている。また、人々の日常生活・経済活動に必要不可欠な基盤を提供する政府機関・事業者が、業務の遂行や事業の継続を脅かされるようなサイバー攻撃にさらされるなど、我が国の安全に対する脅威も高まってきている。今、このような脅威に対処し、人々や企業の創意と発想の結晶である知的創造物や、民主主義の「屋台骨」として社会を支える情報の自由な流通、人々の安全・安心な暮らし、経済社会の繁栄と平和を維持し続けなければならない。

こうした状況を背景に、2014 年 11 月、我が国においてサイバーセキュリティ基本法が制定された。同法は、サイバーセキュリティという概念を法的に位置付け、国や地方公共団体といった関係者の責務を明確化するとともに、サイバーセキュリティ政策に係る政府の司令塔としてサイバーセキュリティ戦略本部を位置付け、国の行政機関に対する勧告権等の権限を付与した。政府は、同法の規定に基づき、サイバーセキュリティ戦略を定めることとされており本文書がこれに該当する。

本戦略は、2020 年オリンピック・パラリンピック東京大会の開催、そしてその先の 2020 年代初頭までの将来を見据えつつ、今後３年程度の基本的な施策の方向性を示すものである。本戦略の中で、サイバー空間に対する我が国の方針を内外に明確化するとともに、本戦略の実践により、積極的に「自由、公正かつ安全なサイバー空間」の創出に努め、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・安定と我が国の安全保障」に寄与する。

本戦略は、こうした目的の達成のため、関係者の共通の理解と行動の基礎として作成するものである。

2. サイバー空間に係る認識

2.1. サイバー空間の恩恵

サイバー空間は「国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」である人工の空間である。こうしたサイバー空間は、主に民間主体の投資や英知の集約により急速な拡大を遂げてきており、差別や排除なく誰もが容易に参加できることから多くの人々によって利用され、いまや欠くことのできない経済社会の活動基盤となっている。

しかし、情報通信革命が生み出す地殻変動は、いまだ黎明期（れいめいき）の段階にある。近年、センサーデバイス等のハードウェアの進化、低廉かつ高速なインターネットの普及、ビッグデータ解析技術の進歩等を背景に、パソコンのみならず、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始めている。こうした状況が進展し、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。連接融合情報社会は、革新的なサービスを創出し、新たな価値を幾何級数的に産み出すことができる社会である。

こうした経済社会の活力の向上及び持続的発展につながるサイバー空間の恩恵は、「自由かつ公正なサイバー空間」の上に成り立つものである。

2.2. サイバー空間における脅威の深刻化

サイバー空間が人々の生活に恩恵をもたらす一方、サイバー空間がもたらす利益を損なう活動も増加してきている。場所・時間の制約を受けず誰もが容易に参加できるサイバー空間は、悪意ある攻撃者に対し、防御側と比べて非対称な優位性を与えている。また、経済社会のサイバー空間への依存度の高まりや、国家の関与が疑われるような組織的かつ極めて高度な攻撃手法の登場が、国民生活・経済社会活動に重大な被害を生じさせ、また影響を及ぼしており、我が国の安全保障に対する脅威も年々高まってきている。

また、連接融合情報社会の到来によって、悪意ある活動はあらゆるモノ・サービスに影響を及ぼすことになり、サイバー攻撃を通じて実空間にもたらされる損害が飛躍的に大きくなることから、今後、国民生活への脅威が更に深刻化することが予想される。

こうした脅威の更なる深刻化が現実のものとならぬよう、「自由かつ公正なサイバー空間」の実現は、同時に「安全なサイバー空間」を実現するものでなければならない。

3. 目的

サイバーセキュリティ基本法[1]を踏まえ、以上の現状認識の下、本戦略は、以下を目的とする。

目的:「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

(1) 目指すべきサイバー空間

サイバー空間は、表現の自由の確保、イノベーションの創出、経済社会の活力の向上に寄与するため、不必要な規制によらず、自由が保障された空間であり、かつ、参加しようとする全ての主体が正当な理由なく差別や排除をされない空間でなければならない。

また、サイバー攻撃による情報・財産の不正な窃取、社会システムの機能不全により、国民生活、さらには国際社会が危機にさらされることを防ぐため、個人や組織を問わずあらゆる主体がサイバーセキュリティに対する認識を深め、各主体の協力的かつ自発的な取組を通じて、その脅威に対処できる安全な空間でなければならない。

我が国は、以上のような「自由、公正かつ安全なサイバー空間」を創出し、発展させるため最大限の努力を行う。

(2) 戦略が寄与する政策領域

連接融合情報社会では、サイバー空間における営みが現実社会の活動と密接な関連性を持つようになる。そのような社会において「自由、公正かつ安全なサイバー空間」を創出し、発展させることは、現実社会で活動する個人が、安全かつ豊かに日々の生活を送り、また企業が活力ある経済活動を行うことを可能とするとともに、国際社会に平和と安定をもたらすことにもなる。

このように、社会全体が歴史的なパラダイム変化を迎える中、我が国は、国民の権利と安全を保障し、我が国の経済社会の発展と国際的な秩序の形成・発展を図るという理念の下、「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

1 サイバーセキュリティ基本法（平成26年法律第104号）第１条「この法律は、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及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、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）と相まって、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」

る社会の実現」、「国際社会の平和・安定と我が国の安全保障」という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、サイバーセキュリティ戦略を推進する。

なお、我が国の経済成長、危機管理、安全保障は、言うまでもなく、それを支える社会経済システムが健全に機能することに依拠しており、こうした社会経済システムに忍び寄る重大な脅威は、我が国全体の課題である。サイバーセキュリティの確保を通じて、IT の利活用を促進[2]すること、成長戦略を確固たるもの[3]とすること、そして我が国の安全保障を万全のものとする[4]ことは、従来からの我が国政府の方針である。

(3) 戦略において目指す日本の姿

我が国は、本戦略で見据える 2020 年代初頭に向けて、自動車の自動走行システムやスマートコミュニティといった高度な社会基盤構築の推進計画を有している。また、2020 年に開催が予定されているオリンピック・パラリンピック東京大会においては、大会を支える各種社会システムのセキュリティを万全に確保することが大前提であるが、これは同時に、日本の強みを対外的にアピールする絶好の機会として捉えるべきものである。情報通信技術がモノ・サービスに結びつき、浸透していくこれからの時代、我が国のみならず世界中の消費者の信頼に応える高品質で技術先端性を有するモノ・サービスの創出、これらを有機的に統合した安全・安心な社会システムの構築等、これまで地道に培ってきた我が国の強みは、世界的に認められているブランドとして確立していることを再認識し、これを我が国の競争力強化に活用していく戦略が必要である。その際、実空間と融合したサイバー空間を活用していくためには、利便性の裏に潜む脅威に的確に対処できることが必要不可欠であり、高付加価値を創出するための「投資」が必要となる。こうした積極的な「投資」は、将来にわたって国際社会における我が国の信頼を高めるとともに、一層豊かな社会へと発展することにつながるものである。

2　世界最先端IT国家創造宣言（2015年６月30日閣議決定）では、「『世界最高水準のIT社会』の実現を目指す我が国において、サイバーセキュリティの強化は、国家の安全保障・危機管理のみならず、IT・データ利活用の促進等を通じた我が国の産業競争力強化等のためにも不可欠」としている。

3　日本再興戦略改訂2015（2015年６月30日閣議決定）は、「IT利活用における安全・安心の確保は我が国の成長戦略を確固たるものとするための前提」としている。

4　国家安全保障戦略（2013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成長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。

4. 基本原則

本戦略の目的達成のための施策の立案及び実施に当たっては、以下に示す基本原則に従うものとする。

4.1. 情報の自由な流通の確保

新たな創意と発想の場としてのサイバー空間は、その内部における情報の自由な流通の確保がその発展の基盤である。このため、我が国は、サイバー空間においては、発信した情報が、その途中で不当に検閲されず、また、不正に改変されずに、意図した受信者へ届く世界が創られ、維持されるべきであると考える。

また、サイバー空間における規律を検討する際、情報の自由な流通を最大限尊重しつつ、プライバシーにも配慮し、所要の規律とプライバシーの確保の適正なバランスについて十分な吟味を行うべきである。その際、サイバー空間における情報の自由な流通については、その前提として、他者の権利・利益をみだりに害することのないよう節度・良識が求められる。

4.2. 法の支配

連接融合情報社会においては、実空間と同様に、サイバー空間においても法の支配が貫徹されるべきである。これは、サイバー空間が、全ての人々に等しく開かれ、安全で信頼できる空間として発展し続けるために不可欠である。国内においては、サイバー空間においても法令を含むルールや規範が適用されている。同様に、国際法を始めとする国際的なルールや規範についても、サイバー空間に適用され、国際的な法の支配が確立されるべきである。さらに、サイバー空間が拡大を続けて世界中の様々な主体に利用される中にあっては、国際社会の平和と安定のため、自由や民主主義といった普遍的価値にのっとった国際的なルールや規範作りが求められる。我が国は、それらのルールや規範が、国際的に確立・実践されること、また各国において、それぞれの事情を踏まえつつも着実に導入されることに積極的に寄与していく。

4.3. 開放性

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ず、常に参加を求める者に開かれたものでなければならない。その開放性の下、相互運用性が確保された状態を維持することは、アイディアや知識を結び付け、世界に新たな価値を生み出すことになる。また、少数の者の政治的利益のために、大多数の人々がサイバー空間の利用を否定されるようなことがあってはならない。

4.4. 自律性

インターネットは、長らく多様な参加主体による自律的なガバナンスにより発展を遂げてきた。サイバー空間上の脅威が、国をあげて対処すべき課題となっても、サイバー空間における秩序維持を国家が全て代替することは不可能、かつ、不適切である。我が国は、サイバー空間の秩序と創造性の共存を実現していくことを目指す観点から、インターネットが育んだこの自律性を尊重し、各者の主体的な行動による管理を基調として、サイバー空間に連接された様々な社会システムがそれぞれに持つ機能や任務を実現し、悪意ある行動を抑止していく自律的メカニズムの構築・運用を推進していく。

4.5. 多様な主体の連携

サイバー空間は、あらゆる階層で様々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。このため、政府に限らず、重要インフラ事業者、企業、個人といったサイバー空間に関係する全てのステークホルダーが、サイバーセキュリティに係るビジョンを共有し、それぞれの役割や責務を果たし、また努力する必要がある。そして、政府はこれらのステークホルダーを適切な連携関係へと促す役割を担っている。こうした連携関係の構築に当たっては、サイバー攻撃が刻々と高度化していること等の事情を踏まえ、双方向的かつリアルタイムな情報共有等の措置によるダイナミックな対処策を実現していく。

これらの諸点は、テロリズムその他の平和を脅かすような行為やそれらを支援する活動までを自由として許容するものではなく、国民の安全・安心、我が国の安全保障上の観点との調和の中で施策に反映されるべきものである。我が国は、上記の５つの基本原則に従うとともに、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。国民の表現の自由とプライバシーの保護を共存させ、適時適切な法執行・制度整備により悪意ある者の行動を抑制することによって国民の権利を保護することこそ、国民から期待されるサイバーセキュリティ政策のあるべき姿である。また、世界中で法の支配を実現することは、グローバル市場を安定させ、イノベーションを活性化させるだけでなく、悪意ある者を国際的に許容しないことを意味し、我が国の安全保障と世界の平和と繁栄に寄与するものである。

5. 目的達成のための施策

本戦略の目的を達成するため、前述の５つの基本原則に基づき、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。その際、各施策は以下の３つのスタンスに可能な限り適合したものであることが求められる。

(1) 後手から先手へ

サイバー空間における攻撃者は、その手口を常に変化させ続けている。我が国は、被害が発生してから対応するのではなく、これからの社会変化や、今後発生し得るリスクを分析し、サイバー空間は、その構成上、脆弱性（ぜいじゃくせい）が内在しているものであるという現実を認識した上で、先手を打って必要な政策を展開する。

(2) 受動から主導へ

上記⑴を実現するため、サイバー空間が、民間部門が主体となって構築・運用している空間であることを踏まえ、これらの主体が自発的かつ主導的に取り組むことを促す政策を展開する。また、我が国は、責任ある国際社会の一員としての役割を主導的に果たし、グローバルな性質を持つサイバー空間の平和と安定に積極的に貢献するよう政策を展開する。

(3) サイバー空間から融合空間へ

あらゆるモノやヒトが情報通信技術により多層的につながり、実空間とサイバー空間の融合が高度に深化している。サイバー空間における事象は、実空間も含む様々な事象と相乗して社会に影響を及ぼし得ることを考慮しなければならない。我が国は、このような、これまでに経験したことのない連接融合情報社会への移行過程にあることを認識し、その変化を的確に捉えた政策を展開する。

5.1. 経済社会の活力の向上及び持続的発展

到来しつつある連接融合情報社会においては、パソコンのみならず、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（以下「IoT[5]システム」という。）が普及してくる。そして、この IoT システムの普及により、サイバー空間と実空間の融合が高度に深化する。今後、企業は、こうした IoT システムを活用した新たなビジネスの創出や既存ビジネスの高度化を図る方向に向かうと見込まれる。このため、我が国企業がこうしたビジネスチャンスを確実に捉えることは、我が国の経済社会の活力の向上及び持続的発展にとって極めて重要である。

企業が、IoT システムを通じて新たなサービスを提供するに当たっては、市場における個人・企業が当該サービスに期待する品質の要素としての安全やセキュリティ、すなわち「セキュリティ品質」が保証されていることが前提である。例えば、サイバー攻撃によりモノが意図しない動作をするよう遠隔操作されたり、ウェアラブル端末を通じて個人に関する情報が窃取されたりといった実空間に密着したリスクや、１回のサイバー攻撃で多くのステークホルダーが関与するデータベースから数百万、数千万件の個人情報等が流出するといった経済社会に重大な影響を及ぼすリスクは、こうしたサービスの信頼性や品質を根本的に損なう。このため、IoT システムの提供するサービス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ことが、今後の社会全体としての課題（チャレンジ）となる。

連接融合情報社会において、我が国企業が、新ビジネスの創出や既存ビジネスの高度化を実現することにより我が国経済をけん引し、当該社会の恩恵を最大限発現するためには、上記の課題に対し、産学官が一体となり、先手を取って対策を進めることが必要である。また、このような時代においてこそ、我が国が長年培ってきた強みである高品質なサービスの提供や、ステークホルダーの信頼に応える企業経営、これらを支える公正な市場環境整備によって、より高いレベルのセキュリティ品質を実現していくことが求められ、こうした取組が企業価値や国際競争力の源泉となっていく。

このため、連接融合情報社会において新たなサービスを実現する IoT システム、企業経営、そしてこれらを支えるビジネス環境のそれぞれに関して、以下のような戦略的アプローチをとっていく。

5.1.1 安全な IoT システムの創出

IoT システムにおける高いレベルでのセキュリティ品質を確保するため、産学官が

5 Internet of Things の略

一体となって先んじて投資を行うことは、多くの IoT システムの利活用が見込まれる 2020 年のオリンピック・パラリンピック東京大会の成功はもとより、我が国企業による IoT システムを活用した新たなビジネス・新規雇用等の創出のため必要不可欠である。

このため、2020 年までに、市場ニーズに応える安全な IoT システムを実現し、我が国の IoT システムの国際的評価を高めることを目指し、以下の取組を実施する。

(1) 安全な IoT システムを活用した新規事業の振興

IoT システムに係る新たな事業を成功させるためには、競争力の源泉となる高いレベルでのセキュリティ品質の実現が不可欠である。しかし、セキュリティを後付けで導入しても、IoT システムが本質的に安全になるものではない。むしろ単にコストの大幅な増加の要因となる。このため、連携される既存システムを含めて、IoT システム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。具体的には、IoT システムに係る事業について、セキュリティ・バイ・デザインの考え方に基づき所要のセキュリティ対策を業態横断的に推進し、メリハリをもって、積極的に新規事業の振興を図る。

(2) IoT システムのセキュリティに係る体系及び体制の整備

経済社会の活力の向上及び持続的発展のためには、IoT システムに係る大規模な事業について、業態横断的に産学官の主体が適切に連携することで、ビジネスイノベーションを巻き起こしていくことが重要である。そして、こうした事業の推進は、セキュリティ・バイ・デザインの考え方に基づいて実施されることが不可欠である。こうした関係主体間において相互信頼に基づく連携と各主体の自律的な取組による協働を実現するためには、当該事業に求められるセキュリティ対策に係る目標、方法、期限等について共通認識を醸成し、その上で、各関係主体の任務を明確化する必要がある。

例えば、高信頼度の ITS（Intelligent Transport Systems）の開発・実現においては、関係府省庁、産業界、研究機関等、数多くの産学官の主体が関係する。これらの関係主体は、まず、ITS 導入によってもたらされるメリットとリスクは不可分であり、その両面を客観的に捉え、採られるべきセキュリティ対策やその実装方法、期限等の認識を共有し、その上で、各主体の任務を明確化する。こうすることによって、関係主体間の相互信頼に基づく連携と各主体の自律的な対策実施による協働が加速化され、効果的で付加価値の高い事業の実現に結び付けることができる。

このため、国が推進する IoT システムに係る大規模な事業のうち、経済社会への影響が大きいと考えられるものについては、サイバーセキュリティ戦略本部が、横断的

な対策のために必要な企画・立案・総合調整を行い、関係府省庁や関係機関の間における有機的・一体的な連携を働きかけるなど、必要な取組が整合的かつ遺漏なく実施されるよう促していく。

(3) IoT システムのセキュリティに係る制度整備

市場が期待する高いレベルのセキュリティ品質の IoT システムを適時に市場に投入していくためには、IoT システムのサプライチェーン全体で適切な対策が講じられていることが求められる。すなわち、関係主体が IoT システムの全体及び各構成要素に求められるセキュリティ対策についての共通認識を形成するための基盤が必要である。また、企業が、新たな IoT システムを積極的に市場に投入していこうとする際にセキュリティの観点を含めて求められる安全性や信頼性の指針があると、新たなビジネスにチャレンジしやすい。このため、産学官で連携しつつ、IoT システムの構成要素である M2M（Machine to Machine）機器やウェアラブル端末等の機器を含め、エネルギー分野、自動車分野、医療分野等における IoT システムのセキュリティに係る総合的なガイドラインや基準の整備を行う。

また、安全な IoT システムの提供を実現するためには、サイバー空間において、どのような技術的問題が生じているのかをいち早く把握して、修正プログラムの配布・適用等の必要な措置を講じることが求められる。このため、関係者が連携し IoT システムや、その構成要素である機器等の脆弱性を調査し、供給者への修正を促すとともに、利用者に着実に対策が行き届くような仕組みを検討し、構築していく。さらに、IoT システムの使用段階において把握したセキュリティ品質や脅威に係る情報を集約・分析し、IoT システムの開発者等の関係者にフィードバックし、一層安全かつ高品質なサービスを実現し、提供していくための取組を促す。

(4) IoT システムのセキュリティに係る技術開発・実証

IoT システムを活用した新ビジネスの創出等を促進していくためには、信頼のおけない安価な機器の調達・導入のリスクに対処しつつ、設計から廃棄までのライフサイクルが長かったり、処理能力に制限があったりするといった、従来の情報通信機器とは異なる IoT システムの構成要素の特徴を踏まえ、セキュリティを担保するための技術開発等を進める必要がある。このため、IoT システムの構成要素の特徴を加味した情報通信技術の開発・実証事業を行う。

様々なモノがネットワークに接続されることにより構成されたシステムから高付加価値のサービスが提供されていくためには、システム全体としてのセキュリティ確保のための対策が必要である。このため、テスト環境の構築や、システム全体の脅威分析・リスク評価手法の開発、IC チップを含むハードウェアの真正性の検証等、社会

科学的な研究も含め、IoT システムにおける対策検討等に必要な技術開発・実証事業を行う。

5.1.2　セキュリティマインドを持った企業経営の推進

連接融合情報社会における企業経営に当たっては、従前からのサイバーセキュリティ確保のための取組はもとより、新たなビジネスの創出等のためにも、これまで以上に、セキュリティリスクの把握や経営資源に係る投資判断を適切に行い、製品・サービスへのセキュリティ機能の実装の推進、セキュリティ人材の育成、組織能力の向上等を図ることが必要となってくる。

このため、我が国企業において、セキュリティマインドを持った企業経営を浸透させることを目指し、以下の取組を実施する。

(1)　経営層の意識改革

企業の経営層が、事業の基盤として用いるシステムや営業秘密の事業戦略上の価値・役割を認識して活用することは、企業経営において不可欠なものである。また、高いレベルのセキュリティ品質が確保された製品・サービスを市場に投入し、新たなビジネスを創出する経営判断に当たり、サイバーセキュリティに関する素養が企業経営層の必須能力となりつつある。こうした社会の変化をより多くの企業経営層が的確に認識し、セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことは、我が国の経済社会の活力の向上及び持続的発展のために必要である。このため、サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成のための官民が一体となった啓発活動を実施する。

また、各企業が、事業戦略としてサイバーセキュリティを確保していくためには、経営層において、セキュリティに関する最高責任者を置くことが必要となる。このため、CISO（Chief Information Security Officer）の機能が各企業の経営層に確実に位置付けられるよう、官民で連携して促す。

(2)　経営能力を高めるサイバーセキュリティ人材の育成

サイバーセキュリティの考え方や能力を、企業経営において使いこなすためには、経営層と実務者層の双方が、経営戦略やサイバーセキュリティに関する課題や解決の方向性を共有する必要がある。このため、経営層の示す経営方針を理解し、サイバーセキュリティに係るビジョンの提示や、実務者層との間のコミュニケーションの支援を行う橋渡し人材層の育成を推進する。

また、企業経営や事業戦略において、サイバーセキュリティ確保のための取組が不可欠になるにつれ、企業の内部人材としてサイバーセキュリティ人材を育てていく必要性が高まっている。このため、サイバーセキュリティを担う実務者層、橋渡し人材層、セキュリティリスクを含む企業のリスクマネジメントに責任を有する経営層といったキャリアパスを考慮した長期的な人材育成や人事評価の在り方について検討し、経営層に訴求する取組を展開する。

(3) 組織能力の向上

連接融合情報社会においては、製品・サービスにセキュリティを取り込んでいくことが、企業の競争力強化に貢献し、企業活動の維持・発展の基盤となることから、企業における製品・サービスの関係者がセキュリティ・バイ・デザインを共通の価値として認識することを促していく。また、営業秘密保護や事業継続の観点から、リスク分析に基づく組織運営を行うよう促していくなど、有効な経営の在り方を発信・推進する。組織の壁を越えたサプライチェーン全体でセキュリティを向上するための方策を講じていく。

さらに、企業における深刻な事業リスクであるサイバー攻撃等の事象への対応能力の向上に当たっては、インシデントの検知・対応の窓口機能を有するCSIRT（Computer Security Incident Response Team）の設置・運用、迅速な対応・復旧に向けた計画やツールの整備、演習の実施、対外説明機能の強化等が有用であることから、こうした取組を促し、名実ともに充実を図る。

加えて、経営層のリーダーシップの下での体制整備、最新のサイバー攻撃の手口や被害の状況等を踏まえた有効な対策、情報開示等の在り方についてサイバーセキュリティに係る経営のガイドライン等により企業に対して発信していくとともに、それを踏まえた企業の取組が第三者認証等により客観的に評価される仕組みを確立していく。また、対策の際の課題、ベストプラクティス、最新の脅威情報やインシデント情報等の共有のため、サイバーセキュリティについて知見を有する独立行政法人、ISAC（Information Sharing and Analysis Center）を含むインシデント情報共有・分析機能を有する機関等を積極的に活用しつつ、情報共有のためのプラットフォーム構築等、民民間・官民間における一層の情報共有網の拡充を進める。

5.1.3 セキュリティに係るビジネス環境の整備

我が国のIoT産業[6]を含む情報通信技術を利活用した関連産業が国際競争力を有し、もって我が国経済をけん引していくとともに、我が国が自立的にサイバーセキュリティの確保を行う能力を有していくためには、我が国において、サイバーセキュリティ

6 機器やサービスの提供を含めIoTシステムに係る産業をいう。

関連産業が成長産業となるよう必要な環境整備を行っていくほか、あらゆるビジネスの基盤となる公正な市場環境の整備を行っていく必要がある。このため、我が国企業のセキュリティ確保及び国際競争力強化の基盤となるビジネス環境の整備に向けて、以下の取組を実施する。

(1) サイバーセキュリティ関連産業の振興

IoT 産業等の関連産業の成長に伴い、今後、コンサルティングや人材育成ビジネスを含むサイバーセキュリティ関連産業に対する需要が一層増加することが見込まれる。このため、我が国において、サイバーセキュリティ産業がこうした需要を捉え、成長産業となるよう、国内外で大規模に活躍できる企業やベンチャー企業の育成等によりこれを振興していく。

まず、サイバー関連情報に係るグローバルな情報収集網や、こうした情報の分析・提供能力を有する産業の振興のため、政府系ファンドの活用によりサイバーセキュリティ分野への大規模かつ集中的な投資を行うなどにより、我が国のサイバーセキュリティ関連産業のリーディングケースを確立する。

また、単独で十分なセキュリティ環境を実現することが困難な中小企業等についてはセキュリティが確保されたクラウドサービスを活用することが有効であると考えられるため、クラウドサービスに関するセキュリティ監査等の普及を促進させていく。

加えて、変化が激しく機動性の求められるサイバーセキュリティ分野においては、革新的な新規事業や技術開発に挑戦するベンチャー企業等の活性化が重要である。このため、サイバーセキュリティ分野において、政府系ファンドの活用によるベンチャー企業同士の国際的な交流を含む共同研究開発等の促進、公的研究機関とベンチャー企業との共同研究開発の促進、研究開発成果を活用したベンチャー企業の育成等の取組を行う。

さらに、サイバーセキュリティに関連する産業の振興に向けて制度の見直しを柔軟に検討していく必要がある。このため、例えば著作権法におけるセキュリティ目的のリバースエンジニアリング[7]に関する適法性の明確化や、所要の制度の見直しについて検討を行う。

(2) 公正なビジネス環境の整備

イノベーションが絶えず生まれ、企業収益につながる経済システムを構築するためには、企業における基幹技術、製造ノウハウといった技術情報の価値を守ることが必

7 Reverse engineering。ソフトウェアやハードウェアなどを解析・分解し、その仕組みや仕様、目的、要素技術などを明らかにすること。

要不可欠である。このため、企業の知的財産の漏えい防止及びこれが侵害された場合の措置を強化するための法整備、啓発活動、実践的な訓練・演習等を実施していく。また、セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置に対しては、国際的な連携の下、厳格に対処する。

(3) 我が国企業の国際展開のための環境整備

我が国の IoT 産業やサイバーセキュリティ関連産業が、国際競争力を有し、もって成長産業として我が国経済をけん引していくためには、国際的なルール等に我が国の立場を十分に盛り込んでいくことが重要である。このため、制御装置等を含む IoT システムのセキュリティに係る国際的な標準規格や評価・認証制度の国際的な相互承認への枠組み作りについて、産学官が一体となり、国際的議論を主導していくほか、我が国のベストプラクティスの国際的な共有・展開を図る。

また､我が国の IoT 産業やサイバーセキュリティ関連産業の国際展開に当たっては、IoT システムで生成・流通されるデータのセキュリティを始め、海外の社会基盤におけるセキュリティの確保が不可欠となる。このため、我が国と経済的結びつきの深い東南アジア諸国連合（ASEAN）諸国等において必要な制度整備の支援、普及啓発活動等を行う。

加えて、近年、我が国企業の国際展開等に伴い、いわゆるサプライチェーン・リスク[8]への対策も重要となってきている。このため、サプライチェーン・リスクへの対策として、例えば必要な研究開発や、ASEAN 諸国等の国・地域との協力を推進する。

8 機器（ICチップを含む。）やシステムの設計・製造・調達・設置・運用段階におけるリスクであって、これらの段階においてウィルスを含む悪意のあるプログラムを埋め込まれるなどのリスクを含む。

5.2. 国民が安全で安心して暮らせる社会の実現

昨今、サイバー空間に起因して、国民の個人情報や財産を始め、実生活に悪影響を及ぼす事例が頻繁に報告されており、被害が深刻化している。今後 IoT システム等の拡大やマイナンバー制度の運用開始など、サイバー空間を取り巻く環境がより一層大きく変化する中、国民が安全・安心に暮らせる社会を実現するためには、政府機関や地方公共団体、サイバー関連事業者、一般企業、そして国民一人一人に至るまで、関係する様々な主体において、多層的なサイバーセキュリティの確保が必要となる。

また、重要インフラや政府機関の機能やサービスは、それ自体が国民生活・経済社会活動を支える基盤となっており、支障が生じると国民の安全・安心に直接的かつ重大な悪影響が生じる可能性があり、対策に万全を期す必要がある。業務責任者（任務責任者）がシステム責任者（資産責任者）と重要インフラや政府機関の機能やサービスを全うするという観点からリスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証（任務保証）」の考え方に基づく取組が必要である。

2020 年のオリンピック・パラリンピック東京大会を始めとする国際的なビッグイベントに向けて、我が国は、国際的に大きな注目を集める一方で、悪意ある者の関心の対象ともなり、サイバー攻撃等のリスクの高まりも考えられる。我が国は、各関係主体が密に連携しつつ、国の威信を懸けて、集中的な対策を推進する。そして、そこから得られる知見やノウハウを、国民の安全・安心に資する財産として、将来にわたり持続・発展させていく。

こうした認識の下、サイバー空間の脅威に対応し、もって国民が安全で安心して暮らせる社会を実現していくため、以下の取組を実施する。

5.2.1　国民・社会を守るための取組

国民・社会がサイバー空間に起因する脅威にさらされないようにするためには、その利用環境が安全なものとなるよう、サイバー空間を構成する機器やサービスが安全かつ安定的に提供され続けることが不可欠である。さらに、利用者たる個人や企業・団体が、自ら進んで意識・リテラシーを高め、主体的に対策に取り組む努力も欠かすことはできない。加えて、サイバー空間における悪意ある振る舞い等の脅威を無効化するため、事後追跡・再発防止及び今後生じ得る犯罪・脅威への対策を積極的に強化していく必要がある。

(1)　安全・安心なサイバー空間の利用環境の構築

サイバー空間を構成する機器やネットワーク、アプリケーション等の各要素は、端

末製造事業者やインターネットアクセス提供事業者、ネットワーク管理事業者、ソフトウェア開発事業者等の民間企業を中心として提供されている。また、サイバー空間を取り巻くリスクに対応するためのツールについても、民間企業が中心となり提供されている。

これらのサイバー関連事業者は、自らが提供するあらゆる製品・サービスについて、単に利便性を追求するだけでなく、その脆弱性を排除する責任を負うことを自ら認識し、システムの企画・設計段階からセキュリティの確保を盛り込む（セキュリティ・バイ・デザイン）とともに、それを利用者の視点に立って適切に説明することが求められる。また、国や関係機関と緊密に連携し、サイバー攻撃に関するインシデントの認知・解析機能を向上させるとともに、一般利用者等への効果的な注意喚起等の措置を図る。

このため、国は、ソフトウェア等の脆弱性関連情報の収集やインターネット上の各種のサイバー攻撃等観測システムの連携・強化を推進する。

また、マルウェア感染や、脆弱な端末がサイバー攻撃の踏み台にされるといったサイバー空間上の差し迫った危険から利用者を保護し、安心してインターネットの恩恵を享受できる環境を整えるため、攻撃を受けた端末の利用者に対する注意喚起のほか、感染によって引き起こされる被害を未然に防ぐ方策の検討の取組を進める。

さらに、2020 年に向けて、公衆無線 LAN を始めとする訪日客向けのインターネット通信環境の整備が進められているが、利便性のみならずサイバーセキュリティの観点からも十分な取組がなされるよう、必要な対策について検討を進める。

(2)　サイバー空間利用者の取組の促進

パソコンやスマートフォン等のデバイスによるインターネットの利用に関し、セキュリティに対する意識や知識が国民全体に十分に浸透しているとは言い難い。一方、リスクの複雑化・多様化が進む昨今、サイバーセキュリティを意識していない利用者は被害を受けるばかりか、自らが加害者になる可能性もはらんでいる。

こうした状況に対応し、サイバー空間の利用者たる国民の自助努力をサポートするため、国は、各種啓発主体と連携し、「サイバーセキュリティ月間」を始めとし、不正プログラムや不審なメールへの対処の方法等に係る普及啓発活動を推進する。とりわけ、サイバー空間に接し始める青少年やその保護者に対し、情報モラル教育を含めた啓発活動に重点的に取り組む。加えて、企業や学校のような組織に所属せず、サイバー空間の脅威や対策について学ぶ機会の少ない者に配慮した啓発活動を推進する。さらに、インターネット利用における悩みや不安に関する相談に応じられる人材を育成

し、活動を促す取組についても、引き続き着実に推進する。

さらに、政府や関係機関による広く国民全体に向けた普及啓発活動に加え、年齢層や所属、ライフスタイルが異なる多様な国民のニーズにきめ細やかに対応していくためには、地域コミュニティによる主体的な普及啓発活動の活性化が望まれる。このため、産学官民の様々な立場の主体が有機的に連携し、一体となって行う普及啓発活動が地域レベルでも促進されるよう、各地で実施されている草の根的な活動に対し、国も積極的な支援等を行う。

国民の安全・安心を担保するためには、個人への啓発はもとより、多種多様な経済活動を営む民間事業者・団体や、住民に直結した行政サービスを担う地方公共団体、学生・児童生徒や保護者の情報を多く扱う教育機関等の公的機関におけるサイバーセキュリティ確保に向けた啓発も極めて重要である。特に、中小の企業や地方公共団体のように、十分な対策を講じることが困難な組織については、国、関係機関、業界団体等の関係者が連携し、各種セミナーや対策ガイドラインの策定・普及、最新の攻撃の手口等の情報共有体制の整備、実践的な訓練・演習の実施等の取組を通じた支援が必要であることに配慮し、必要な取組を推進する。

(3) サイバー犯罪への対策

サイバー空間と実空間の結びつきが強まるにつれ、インターネットバンキングを悪用した不正送金事件や標的型攻撃による情報窃取、フィッシング行為等、国民一人一人や企業に身近な被害事例が多発している。また、大規模な個人情報流出事案を始めとして、個人情報や機微情報を流出させる犯行も後を絶たず、社会問題化している。悪意あるサイバー犯罪の実態を把握し、法令に従って適切に取り締まるとともに、サイバー空間において今後起こり得る新たな手口にも対処できるようにするため、犯罪対処能力・捜査能力の向上が不可欠である。

このため、国は、サイバー空間の脅威に関する実態把握のための情報収集の強化やサイバー犯罪に係る捜査能力の向上、取締り、国際連携等のための体制強化を進める。また、捜査・取締り及び被害拡大防止において、高度な技術的知見が必要となっていることから、不正プログラムの解析等のための技術力の向上、インターネット観測の高度化等、情報技術の解析の体制を強化することにより、必要なノウハウ・技術の蓄積等を推進する。さらに、必要な人材育成や技術開発を着実に推進する。加えて、サイバー犯罪の捜査や未然防止に向け、民間の知見の積極的な活用や、官民の人事交流を始め、官民連携を強化する。

サイバー犯罪に対する事後追跡可能性を確保するためには、サイバー関連事業者の協力が不可欠であることから、その事業活動に関し、適切な取組がなされるよう必要

な対応を行う。特に、通信履歴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[9]」の解説の改正を踏まえ、関係事業者における適切な取組を推進する。

5.2.2　重要インフラを守るための取組

国民生活及び経済活動は、様々な社会インフラによって支えられており、その機能を実現するために情報システムが幅広く用いられている。こうした中で、特に情報通信、電力、金融など、その機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり重点的に防護していく必要がある。その際、民間は全てを政府に依存するのではなく、政府も民間だけに任せるのではない、緊密な官民連携が求められる。また、重要インフラはその性質上、持続的なサービス提供が求められていることから、その防護に当たっては、サービス提供に必要な情報システムについて、サイバー攻撃等による障害の発生を可能な限り減らすとともに、障害発生の早期検知と、障害の迅速な復旧を図ることが重要である。

このため政府では、「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」[10]を策定し、重要インフラ分野を特定[11]するとともに、同計画に基づいて安全基準等の整備・浸透、演習・訓練の実施、官民の情報共有体制の強化などの諸施策を実施している。

こうした既存の取組は、我が国の重要インフラ防護において一定の効果を上げているところであり、引き続き継続する。一方で、重要インフラを取り巻く社会環境や技術環境が刻々と変化する中で、従前の取組を漫然と続けるだけでは、有効性を喪失し形骸化しかねない。このため、以下に示すような取組内容の見直しを継続的に図ることとし、当該取組に向けた更なるセキュリティ強化等の具体的内容について取りまとめ、これを推進する。また、重要インフラ事業者及びその所管省庁は、強制基準やガイドラインなどの安全基準を定めてサイバー攻撃に対する防護を行っているが、重要インフラの中でも業法によってサービスの維持及び安全確保に係る水準が求められているものについては、昨今のサイバー空間を取り巻く環境変化を踏まえ、安全基準について不断の見直しを行っていく。

(1)　重要インフラ防護の範囲等の不断の見直し

社会環境の変化や既存の知見の集積等により、これまで重要インフラと位置付けら

9　平成16年８月31日総務省告示第695号。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、電気通信サービス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して策定されている。

10　2014年５月19日情報セキュリティ政策会議決定。2015年５月25日サイバーセキュリティ戦略本部改訂。

11　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の13分野。

れていなかった分野であっても、情報システムが障害に至った場合の影響が大きいと判断されるものがあれば、新たに重要インフラ分野とする必要がある。このため、重要インフラ分野そのものの見直しを継続的に行う。この際、新規の分野は必ずしも既存の分野と一律に全て同じ取組を行う必要性がなく、また、分野数の増加により全分野一律の対策が難しくなることも考えられるため、重要インフラ分野をクラス分けするなど、分野間の相互依存性や提供するサービスといった各分野の特性や業法の有無を踏まえた対応を行う。

一方、既存の重要インフラ分野においても、そのサービス提供をより確実なものとしていくには、個々の限られた重要インフラ事業者による「点での防護」ではなく、分野全体での「面としての防護」を確保する必要がある。このため、これまで主要事業者に対して重点的に行ってきた取組を中小事業者に拡大していくことや、重要インフラ事業者が提供するサービスに間接的に関わる外部委託先や主要関係先といった周辺事業者に対しても取組を広げるなど、各分野内において実際に取組を行う対象である「重要インフラ事業者」の範囲についても継続的に見直しを行う。

加えて、サイバー攻撃は重要インフラ分野に対してだけ発生するわけではないことから、重要インフラ分野以外の民間企業を対象とした取組についても検討する必要がある。特に我が国を代表するような企業や核物質防護等の措置が要求される安全保障上重要な企業については、重要インフラの定義いかんに関わらず、情報共有体制整備などの検討を進めていく。

(2) 効果的かつ迅速な情報共有の実現

サイバー攻撃は複雑・巧妙化し続けており、多様な脅威に的確に対抗するためには、官民が連携してサイバー攻撃の可能性がある障害情報を共有していくことが重要である。情報共有の活性化には、重要インフラ事業者が情報を提供する際に、自身の信頼や評判を損なうといった心理的障壁を排除すること、及び提供のメリットを感じることが必要である。このため、情報共有の際には提供源の秘匿や共有範囲の設定など適切な加工を行うことを共通認識とするとともに、情報提供したことによって不利益が生じない環境を構築していく。さらに、情報集約側は、十分な分析能力を保有した上で、提供情報を基に注意喚起等を適時適切に実施するとともに、提供情報を収集・分析・共有する基盤となるプラットフォーム構築などの双方向で高度な情報共有環境を実現することで、重要インフラ事業者がサイバー攻撃防御に必要な情報を速やかに入手できるようにする。

2020 年に向けて、世界に誇れるサイバー攻撃対処体制を構築するためには、より効果的な情報を、より迅速に共有していくことが必要となる。このため、業法等の規定

により報告対象となる一定規模以上の障害だけでなく、小規模な障害情報や予兆情報はサイバー攻撃の脅威に対抗する上で有効であるとの認識の下、関係者の共通理解として情報収集を行っているが、内閣サイバーセキュリティセンター（NISC）と所管省庁がより緊密に連携し、積極的な情報収集に取り組む。また、NISC と重要インフラ事業者との間のホットライン構築や、情報共有の様式・手順の改良、処理の自動化などの取組により、情報を速やかに共有できる体制を整備するため、NISC への必要な情報の集約を含め、政府機関内での必要な連携を高めていく。

また、重要インフラ事業者がサイバー攻撃の発生を事案対処省庁に通報した場合、政府機関は連携しながら、重要インフラ事業者の支援を行うとともに、実態解明を進める。その結果得られたサイバー攻撃の手口等に関する情報について、被害の拡大を防止するため、政府機関及び重要インフラ事業者等との間で積極的に共有する。

こうした情報共有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・訓練を実施し、必要な改善を継続的に加えていく。

(3) 各分野の個別事情への支援

地方公共団体については、サイバーセキュリティ基本法において、独自の責務やサイバーセキュリティ戦略本部の協力がうたわれている。そして、大小様々な規模の団体がありながら、取り扱う情報の機微性などの事情を踏まえれば、政府機関等と同様のセキュリティ確保が求められるなどの特別な位置付けにある。こうした中、マイナンバー導入に伴う新たなシステム調達といった環境変化が予定されており、政府としてもサイバーセキュリティが確保されたものとなるよう、サイバーセキュリティ基本法等に基づき必要な支援を実施していくとともに、地方公共団体の情報システムについてマイナンバー制度の運用に係るセキュリティを強化する観点から必要な対策を検討し、講じていく。また、マイナンバー法における個人番号利用事務において使用するシステムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を含めて検討の上、必要な措置を講ずるとともに、関係機関が連携し専門的・技術的知見を有する監視・監督体制を整備する。さらに、連携・接続する国・地方の関連システム全体を俯瞰した監視・検知体制の整備に向けて、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）との情報連携も踏まえたインシデントの監視・検知を迅速に行える体制の整備を進める。加えて、マイナンバーを機とした政府内及び官民の認証連携についても、利便性の向上とセキュリティの確保が適切なバランスの取れたものとなるよう環境整備を進めていく。

また、電力分野のスマートメーターや化学・石油分野の工場生産系システムに代表されるように、情報システムの中でも制御系については、IT の不具合によって、安全

確保及び持続的なサービス提供の確保に支障を来す懸念がある。制御系のセキュリティを十全に確保していくためには、情報セキュリティによって安全確保を的確に行うことが持続的なサービス提供の確保につながることを改めて認識する必要がある。また、こうした制御系システムは、汎用製品の使用や標準プロトコルの導入といった技術のオープン化やネットワークのオープン化が進んでおり、従来機器の置換などで広く利用されるようになる一方、脆弱性や不正アクセスへの対応が急務となっている。こうした特性を踏まえ、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、その情報を収集・分析・展開していく。また、制御系システム等の調達、運用には高度な専門性が必要とされることから、セキュリティ要件への適合を客観的に判断することが可能である国際標準に即した第三者認証制度の活用を進めていく。

5.2.3 政府機関を守るための取組

政府機関等では、政府機関における統一的な基準の策定及びその運用を中心としてサイバーセキュリティの確保に取り組んでおり、これまで、主に政府機関全体としての対策水準の向上を推進するとともに、新たに直面した脅威・課題についても基準に逐次反映することによって対応してきた。

一方で、2020 年までには、政府機関等に対するサイバー攻撃の高度化・巧妙化や IT に関する製品・サービスの多機能化・多様化を始めとした社会環境の変容が一層加速することが予想され、これらに伴う脅威の急速な増大や予見困難な新たな課題に直面することを想定しておく必要がある。加えて、正にこれから設計・構築を始める情報システムには 2020 年時点で運用しているものも含まれ、将来にわたってセキュアであることが求められることや、サイバーセキュリティに関する対策の多くは特効薬的に作用するものではないことから、新たな脅威・課題に直面してから対策を講じ始める姿勢では、2020 年におけるサイバーセキュリティの確保は実現できないことに留意が必要である。

これらを踏まえ、政府機関等においては、既に顕在化している脅威や課題はもとより、未知の脅威等に直面した場合であっても柔軟かつ迅速に対応できるよう、従来から推進している対策に万全を期すことを前提としつつ、先々を見据えて以下の事項について重点的に取り組むとともに、政府機関における統一的な基準を始めとした規程に適時反映し、監査や平素からの教育などの取組によりその徹底を図る。

(1) 攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進

情報の窃取・破壊・改ざんを企図したとみられる標的型攻撃を始めとしたサイバー

攻撃に対処するため、他の機関を本来の標的とする攻撃の踏み台とするために狙われる場合も想定し、全ての政府機関等において、攻撃に直面することを前提とした多層的な対策を講ずる。また、その推進に当たっては、政府機関における統一的な基準に基づく対策を徹底するとともに、行政としての責任を全うする目的に照らしたリスク分析を行い、政府機関全体としての最適化を図る。

i. インシデントの未然防止

ソフトウェアに関する公開された脆弱性や把握された不正プログラムへの対応、電子署名・認証技術の活用といった予防的な対策を確実に実施するとともに、情勢の変化に応じて迅速・柔軟に見直していく。

具体的には、サイバーセキュリティに関する情報の収集・分析機能を強化するとともに、政府機関全体としての情報共有及び政府機関内外における連携に関する体制の強化を行う。また、サプライチェーン・リスクへの対応を始めとした情報システムの企画・設計段階からセキュリティの確保を盛り込むための取組を推進する。さらに、情勢変化に応じた運用中の情報システムにおける対策の迅速・柔軟な見直しを推進する。加えて、ペネトレーションテストを始めとした検査を通じて、情報システムにおける対策の実施状況の点検・改善に取り組む。

ii. 被害の発生・拡大の防止

ゼロデイ攻撃を含む未知の脆弱性や不正プログラムを悪用した攻撃によって情報システム内部に侵入されるなどのインシデントを全て未然に防止することは極めて困難であるため、未然防止と併せて、事態の早期把握及び被害の発生・拡大の防止に向けた迅速かつ的確な対処の実施を推進する。

具体的には、GSOC による政府機関全体における検知・解析機能の強化、並びに各機関におけるインシデント対応を行うチーム（CSIRT）の体制及び事態の把握・対処機能の強化、インシデント発生時の情報提供の迅速化・高度化に取り組む。また、インシデントの発生に備えた訓練・演習を実施し、その教訓を施策に反映させるとともに、対処要員の能力・連携の強化及び各機関幹部による指揮の下での組織的対処の徹底を図る。さらに、監視効率の向上等によりリスクを低減させるため、政府機関の情報システムにおけるインターネットの接続口の更なる集約を図る。加えて、政府機関で重大なインシデントが発生した場合等における原因究明調査のための取組を強化し、分析結果を共有することによって被害の拡大防止を図るとともに、対策の改善に反映させる。

iii. 被害の低減

インシデントの発生から応急的な対処の完了までの間における被害を低減するた

め、侵入の拡大や攻撃目的の達成を困難にするための対策を講じる。

具体的には、個人情報や機微な情報を始め、外部に流出することや改ざんされることによって国民・社会等に多大な悪影響を及ぼす機密性・完全性の高い情報への不正なアクセスをより困難なものにするため、業務の内容や取り扱う情報の性質・量に応じた情報システムの分離や運用ルールを含む情報管理の更なる強化に取り組む。また、システム破壊等可用性に関わる攻撃も含め、標的型攻撃に対する多重防御の取組を加速する。加えて、リスクや影響度に応じた対処及び情報システムの重点的な対策強化に関する優先度の評価方法の確立に取り組む。

(2) しなやかな組織的対応能力の強化

加速度的な変化への柔軟かつ迅速な対応を可能とする、しなやかな組織的対応能力の強化に取り組む。

具体的には、定期的な自己点検や第三者的視点からのマネジメント監査を始めとした点検の実施を通じて、政府機関等における対策強化のための体制・制度の検証・改善に取り組む。また、リスク評価に基づくリスク対処方針や対策水準の設定、不測の事態に備えたコンティンジェンシープラン（緊急時対応計画）の策定を関係者間の合意の下で行う制度の確立等、リスク評価に基づく組織的な情報システムの対策・管理の推進に取り組む。さらに、未知の脅威等に備えた対応に一意的な解は存在しないため、政府機関全体での事例の共有や意見交換の促進に資するコミュニティを形成する。加えて、組織的対応の要は人であることから、幹部を含む職員全体のサイバーセキュリティに関する素養の向上を確実なものとするよう取り組む。また、資格等を個人の能力を客観的に示す指標の一つとして活用しつつ、各機関における対応能力強化のけん引役となるセキュリティ人材の育成・確保を図る。

(3) 技術の進歩や業務遂行形態の変化への対応

多機能化・多様化する IT 製品・サービスの活用による行政事務の高度化・合理化や、IT の活用に係る時代の要請に応じた形態での行政事務の遂行に当たっては、サイバーセキュリティの確保に留意し、新たな IT 製品・サービスの不適切な利用に起因するインシデントの発生やセキュリティ水準の低下の防止を図る。

具体的には、政府機関全体における新たな IT 製品・サービスの導入状況及び対策状況に関する情報を集約するとともに、それらサービス等の特性を踏まえた政府統一的な対策を策定・推進する。また、IT を活用した行政事務の遂行形態の変化に際しては、関係機関間で緊密に連携し、サイバーセキュリティの確保を前提とした形態を実現する。

(4) 監視対象の拡大等による総合的な対策強化

政府機関全体としてのサイバーセキュリティを強化するため、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等における対策の総合的な強化を図る。

具体的には、当該法人におけるインシデント対処能力の向上や所管省庁による当該法人への監査の強化等を図るほか、当該法人におけるサイバーセキュリティに関する取組について、法人の特性等を踏まえつつ、政府機関の取組（上記(1)から(3)まで）に準じて推進する。とりわけ、当該法人について、公平な受益者の負担に留意しつつ段階的にGSOCの監視対象に追加するほか、サイバーセキュリティ戦略本部がNISCに実施させる監査及び原因究明調査の対象とする等の施策を推進する。また、本対策強化に際しては、専門的知見を有する関係法人との連携体制の整備を図ることを含め、所要の法改正について速やかに検討を行い、必要に応じて措置する。

5.3. 国際社会の平和・安定及び我が国の安全保障

自由、公正かつ安全なサイバー空間は、地球規模でのコミュニケーションが可能なグローバルな共通空間であり、国際社会の平和と安定の礎である。とりわけ我が国は、サイバー空間における多様な価値観を認め、自律性を重んじ、そして人々の言論や企業行動を法の支配により保障することが、国際社会の平和と安定を実現し、ひいては繁栄に導くと確信している。現に、我が国は、自由、公正かつ安全なサイバー空間を利活用することによって、平和で安定し、極めて質の高い生活と持続的発展が可能な経済・社会を実現させてきた。その反面、国際的にも国内においても、社会システムのサイバー空間への依存度は高まっており、手法の巧妙化とその影響の甚大化により、サイバー攻撃が実空間における経済社会活動に重大な影響を与える事態が生じていることも事実である。こうした状況において、サイバー攻撃に対して適切に対処し、サイバー空間の安全な利用を確保することは、国際社会の平和と安定及び我が国の安全保障上、早急かつ抜本的に取り組むべき極めて重要な課題である。

このような課題に対し、我が国の安全を確保するため、国全体の対処能力を抜本的に強化しつつ、引き続き、同盟国・有志国等との協力・連携や、各国との信頼醸成に取り組んでいく。また、自由、公正かつ安全なサイバー空間を希求する立場から、専制的な体制による情報の独占、統制、検閲、窃取、破壊及びテロリスト等の非国家主体によるサイバー空間の悪用等に強く反対し、国際協調主義に基づく「積極的平和主義」をもって国際社会の平和と安定を実現することにより、国際的な秩序の維持に積極的に貢献しながら、我が国の安全保障を確保していく。

我が国は、かかる認識の下、国際社会の平和と安定及び我が国の安全保障の確立に向け、以下のような戦略的アプローチをとっていく。また、その実施に当たっては、各府省庁及び関連機関のサイバーセキュリティ施策等に関する情報の内閣官房への集約を更に進めるとともに、我が国としての統一的な対外対応を強化する。

5.3.1　我が国の安全の確保

社会システムを始め、あらゆるものがネットワーク化され、サイバー空間と実空間との融合が進みつつあり、多くの組織がサイバー空間に深く依存している。その結果、サイバー攻撃によって、一国の政治、社会、経済、文化に強い打撃を与えることが可能となった。いまやサイバー空間は、経済活動のみならず、安全保障やインテリジェンス活動の舞台ともなり、国家の関与が疑われるものも含め、組織的かつ周到に準備された高度なサイバー攻撃による破壊行為や機密情報の窃取、データの改ざんは現実の脅威である。

こうした高度なサイバー攻撃からの防護においては、予防、検知、対処の全ての段

階において、高度な知見に基づいた迅速かつ的確な対応が必要である。このため、平素におけるサイバー空間の分析を通じて、様々な主体によるサイバー攻撃の兆候を含む状況を早期に認識・把握し、問題点を検知して迅速に対応する能力の一層の向上を図っていく。これに向けては、外国政府機関との情報共有を含む情報収集・情勢分析機能の強化を図るとともに、組織・分野横断的な取組を総合的に推進することが重要である。

また、我が国の安全保障のためには、政府や重要インフラ等が有している社会システムとしての機能をサイバー攻撃から防護することが必要である。防護に当たっては、官民を問わず、組織における縦割り、硬直的な前例主義は、攻撃者にとって好都合となる。こうした認識を多様な関係主体間で共有した上で、これまでの連携を一層強固にし、切れ目のない重層的・多層的な防護を実現する。あわせて、我が国は、あらゆる段階の事案が想定されるサイバー攻撃に対してその規模、程度に応じて的確に対処できるよう、幅広い総合的な見地から能力の一層の強化を図る。

さらに、サイバー攻撃が容易に国境を越えて行われ得ること、海外において国家の関与や実空間における軍のオペレーションと連動していることが疑われるサイバー攻撃の事例もあることを踏まえれば、同盟国及び同様の立場に立ついわゆる有志国・機関との間の脅威情報の共有や人材育成等における協力・連携の積極的な推進が不可欠であり、また、その他の国とも信頼醸成を進めていくことが重要である。

(1) 対処機関の能力強化

多様化・複雑化するサイバー脅威に対処するためには国全体の強靭（きょうじん）性と能力強化が不可欠である。このため、警察や自衛隊を始めとする対処機関の能力を質的・量的に向上させる。その際、これら対処機関の役割を十分に果たすため、人材育成・確保、最新技術の導入・習得、研究開発等を含む諸制度の見直し等、あらゆる有効な手段について、幅広く検討を進める。このほか、政府機関が保有する機密情報を標的とするサイバー攻撃に対処するため、内閣情報調査室等の関係機関においてカウンターサイバーインテリジェンスに係る取組を推進する。

(2) 我が国の先端技術の活用・防護

我が国の先端技術は、経済的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。特に宇宙関連技術や原子力関連技術、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情報を扱う主体にあっては、それらが世界のサイバー攻撃者の標的となり得るものであることを改めて意識する必要がある。これらの主体は、安全保障の確保に向け、我が国が保有する先端技術を有効に活用していくためにも、そのサイバーセキュリティの確保に万全を期する。関係する主

体は、先端技術に関与する全ての者のセキュリティ意識を更に向上させるとともに、国外からのサイバー攻撃に対する監視の強化や対処能力の向上、調達する物品・サービスに関する調査・確認の強化、官民の情報共有を始めとした連携強化等、所要の対策を講じていく。

(3) 政府機関・社会システムの防護

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持続的に提供するという重要な任務を有している。したがって、我が国の安全保障上、こうした社会システムを担う事業者のサイバーセキュリティの確保は、政府機関の任務を保証し、かつ、国民や社会に不可欠なサービスの持続的な提供を果たすためにも、極めて重要である。このため、これらの事業者は、政府機関との連携の下、サイバー攻撃によるサービス提供への影響度合いが、政府機関及び事業者自身の任務遂行にどのような影響を与えるのかを十分に認識し、十全の対策を講じていく必要がある。

この観点から、政府と重要インフラその他の社会システムを担う事業者は、平素から、必要な範囲で、脆弱性や攻撃情報を始めとする有益な情報を持ち寄り、共有し、分析し、対応していく取組を一層強化し、政府と民間との情報の双方向の流れを一層加速する。

防衛当局である防衛省・自衛隊においては、自らが保有するネットワーク・インフラの防護を引き続き強化するとともに、上記の社会システムに対するサイバー攻撃も、任務遂行上の大きな阻害要因となる可能性を踏まえ、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。

5.3.2 国際社会の平和・安定

国際社会の平和と安定のためには、サイバーセキュリティの確保とグローバル規模での情報の自由な流通を両立させる必要がある。

サイバー空間は、グローバルに活動する主体や世界各国の多様な主体が管理・運営するハードウェアとソフトウェアが、自律的・協調的なネットワークによって結ばれ、データを通信・処理することによって成立している。このような国際的性質を有する空間において、コミュニケーションや社会・経済・文化等の活動が活発に行われるためには、人々が信頼して利用できるよう、世界各国に分散する構成要素のセキュリティが適切に確保されている必要がある。

また、サイバー空間では、グローバル規模で情報が自由に流通することによって、地球上の社会・経済・文化等のあらゆる活動の基盤となり、国境を越えた相互理解が促進されている。権力による過度な規制や管理によりサイバー空間が分断されれば、このサイバー空間の持つ優れたグローバル性は毀損されてしまう。

加えて、サイバー空間に係る安全を確保するためには、我が国自身のみならず、国際社会の平和と安定にもつながるものとして、国際的に安定したサイバー環境を創出するための施策を実施することが重要である。

かかる認識の下、我が国は、国際社会の平和と安定の実現のため、以下の方針により、責任ある国際社会の一員としての役割を主導的に果たし、多様な主体との国際的な連携によるサイバーセキュリティの確保並びにサイバー空間におけるグローバル規模の情報の自由な流通の確保に向けて取り組んでいく。

(1) サイバー空間における国際的な法の支配の確立

我が国は、多種多様な主体や価値観の存在を認識しつつ、情報の自由な流通を基本原則とする立場から、サイバー空間における国際的な法の支配の確立のため、積極的な役割を担っていく。

i. 国際的なルールや規範の形成

我が国は、サイバー空間においても従来の国際法が適用されると考える。例えば、サイバー空間における安全保障については、国連総会第一委員会の下に設置された政府専門家会合に我が国も参加し、2013 年６月、「サイバー空間を利用した行為にも既存の国際法が適用される」ことなどを示した成果文書を国連総会に報告した。我が国は、今後とも、従来の国際法がサイバー空間にも適用されるとの立場から、個別具体的な国際法の適用についての議論に積極的に関与し、もってサイバー空間における国際的なルールや規範の形成に取り組んでいく。

上記以外の国連及びその専門機関の会合、経済開発協力機構（OECD）、アジア太平洋経済協力（APEC）、サイバー空間に関する国際会議等の場においても、多様な主体の参加の下、経済社会面やインターネット・ガバナンス等に力点を置いた議論が行われている。我が国は、これらの議論においても、引き続き、国内外の各主体と連携し、サイバー空間の開放性や相互運用性、自律性、情報の自由な流通を確保することが、社会・経済・文化の発展に大きく貢献するとの立場から、国際的なルールや規範の形成を積極的に進める。

ii. 国際的なルールや規範の実現

我が国は、国際的なルールや規範を形成しつつ、それらの実現についても積極的に

取組を進めていく。例えば、安全保障分野では、個別具体的な国際法の適用についての議論の成果を踏まえながら、国際機関や各国とのサイバー協議等の場において、後述する信頼醸成等を進めていく。また、サイバー犯罪対策では、我が国はサイバー犯罪条約を締結していることから、この条約の締結国の拡大を始めとして、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、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図り、国境を越える犯罪者の検挙に向けた国際捜査を推進する。我が国は、国際的なルールや規範をこうして率先して実践し、もってサイバー空間における法の支配を確立させるとともに、国際社会の平和と安定を実現していく。

(2) 国際的な信頼醸成措置

サイバー空間が、社会活動や経済活動のみならず、軍事活動を含めたあらゆる活動が依拠する場となっている中、サイバー攻撃を発端とした不測の事態の発生をいかに防ぐか等について、国連等の場において国際的な議論を推進し、多くの国で認識を共有する必要がある。このため、国連を始めとする多国間の場や各国とのサイバー協議において、我が国の基本的な立場を積極的に発信し、多くの国とそれぞれの立場を相互に共有する。加えて、国を超えるインシデントが発生した場合の、国と国、民と民といった様々なレイヤーにおける国際的な連絡体制を平素から構築し、連絡演習等を実施することにより、国際的な信頼醸成を進めていく。

(3) サイバー空間を悪用した国際テロ組織の活動への対策

サイバー空間が国際社会の平和と安定に寄与するものであり続けるためには、サイバー空間を悪用した国際テロ組織の活動を阻止する必要がある。サイバー空間の拡大に伴い、過激主義を標榜（ひょうぼう）する非政府主体が、過激思想の伝播（でんぱ）や示威行為、組織への勧誘活動、テロ資金の獲得等にサイバー空間を悪用している。このような国際テロ組織に対し、我が国としても、国連安保理決議等の国際社会の意思表明を踏まえ、国際社会と連携した対処を進めていく必要がある。このため、インターネット上でテロとの関連性の高い情報を収集する技術等の活用を含め、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・分析の強化その他の必要な措置をとる。

(4) サイバー分野における能力構築（キャパシティビルディング）への協力

我が国は、自由と民主主義を基調とする責任ある国際社会の一員として、これまでの経験と蓄積を元に、各国のキャパシティビルディングに積極的に取り組む。

国境を越えるサイバー空間の脅威は、世界各国の多様な主体が連携して対処していく必要があり、一部の国や地域において脅威に対処するための能力が不十分であることは、我が国を含む世界全体にとってのリスク要因となる。事実、我が国へのサイバ

一攻撃は、国外からの攻撃が多く確認されている。

また我が国の国民及び企業の活動はグローバル化しており、海外への渡航や企業の海外進出拠点は増加を続けている。その活動は、情報化の進展に伴い、渡航先国・進出先国の管理・運営する社会インフラ及びサイバー空間に依存する。

こうしたことから、世界各国におけるサイバーセキュリティ確保のためのキャパシティビルディングに協力することは、当該国への貢献となるのみならず、我が国と世界全体にとっても利益となる。

我が国は、これまで情報通信社会の発展に伴い、サイバーセキュリティに関する法令や政策の整備を推進するとともに、政府機関、重要インフラ事業者、その他の組織及び個人におけるサイバーセキュリティの確保やサイバー犯罪対策、サイバーセキュリティ人材の育成、サイバーセキュリティに関する技術の研究開発に取り組んできた。我が国は、これらの経験と蓄積を元に、情報の自由な流通を基本原則とする責任ある国際社会の一員として、引き続き、各国のキャパシティビルディングに積極的に協力していく。このため、政府及び関係機関は一体となってキャパシティビルディングについて検討し、その効率的・効果的な実施を図る。

(5) 国際的な人材育成

こうした国際的なサイバーセキュリティ関連の取組に当たっては、国際会議等に継続的に参加貢献して我が国の立場を主張し、外国の様々な主体とコミュニケーションを深めていくことが必要である。このため、このような人材には、サイバーセキュリティに関する十分な知識とともに、各国の社会・経済・文化等の状況についての理解も求められる。したがって、我が国は、サイバー空間に関する技術的な知見を有するとともに、各国の状況や国際安全保障、国際協力等にも精通した、国際場裡（こくさいじょうり）で十分に活躍し得る質の高い国際的な人材を官民において一層増強していく。

5.3.3 世界各国との協力・連携

我が国は、世界各国との協力・連携によって、国際社会の平和・安定及び我が国の安全保障を実現していく。国際的な連携・協力は、国家の関与も疑われるような高度なサイバー攻撃に対する国際的対応力の強化等にも資するものである。我が国は、日米同盟を基軸としつつ、相手国との地理的・経済的な関係、価値観の共有度合い等の状況を考慮し、自由と民主主義を基調とする責任ある国際社会の一員として、各国との協力関係を拡大・深化させ、また、サイバー攻撃を発端とした不測の事態の発生を回避・防止する観点から信頼醸成も図りながら、幅広い分野で国際協力体制を確立し、サイバー空間の安全を確保していく。

(1) アジア大洋州

アジア大洋州地域は、歴史的にも我が国との関係が深く、国民相互の往来や我が国企業による投資も増加を続けている。我が国は、この地域における責任ある国として、二国間や多国間の様々なチャネルを通じ、本地域におけるサイバー分野での国際連携やキャパシティビルディングへの協力、情報の収集や発信を強力に推進していく。

我が国はASEANとの間に、40年以上にわたる伝統的なパートナーシップを持つ。サイバーセキュリティ分野においても、日ASEAN情報セキュリティ政策会議を始め、複数のチャネルによる密接な協力関係を有する。我が国は、引き続き、国際会議や共同プロジェクト等の枠組み、相手国のニーズを踏まえた多様で実践的なキャパシティビルディングの継続的実施等を通じ、日・ASEAN 間のサイバー分野での協力関係を更に深化・拡大させ、強靭なASEANのサイバー空間の実現に積極的に貢献していく。加えて、ASEAN 加盟国それぞれの経済・社会・文化の状況を重視するとともに、サイバー空間に対する多様な価値観を踏まえ、各加盟国との二国間の協力関係も強化していく。

また、我が国は、我が国と基本的な価値観を共有する、地域の戦略的パートナーの国との協力・連携を強化していく。これらの国との間では、様々なチャネルを通じ、サイバー関連施策やサイバー攻撃に関する情報の平素からの共有・活用、サイバー攻撃に対する共同訓練等、サイバー分野における二国間の協力関係を深化させていくとともに、地域や国際場裡におけるサイバー空間の諸課題への対応と連携を図っていく。

アジア大洋州におけるその他の国や地域についても、サイバー空間についての認識や互いのサイバーセキュリティ戦略等の情報交換、サイバー分野における協力の可能性等を議論し、相互理解と連携を進めていく。また、APEC や ASEAN 地域フォーラム（ARF）等の地域的枠組みにも積極的に参加し、地域のサイバー空間におけるセキュリティの確保と情報の自由な流通による経済・社会・文化の発展に向けて取り組んでいく。

(2) 北米

我が国は、北米地域の両国と基本的価値観を共有しており、サイバー分野においても連携を進めていく。特に米国は、日米安保体制を基軸に、あらゆるレベルで緊密に連携する我が国の同盟国である。サイバー空間に関する価値観も同じくしており、日米サイバー対話やインターネットエコノミーに関する日米政策協力対話、日米サイバー防衛政策ワーキンググループ等、二国間における様々なチャネルにおいて緊密な情報交換と連携を図っている。我が国は、引き続き、サイバー関連施策やサイバー攻撃に関する情報の共有・活用、サイバー事案への対処、先端的技術分野における共同プロジェクトの実施等、具体的な連携を深めるとともに、サイバー空間に関する国際的

な規範やルールの形成と実現、国際安全保障、インターネット・ガバナンス等を含む、国際場裡における幅広いサイバー空間の諸課題への対応についても緊密に協力し、国際社会の平和と安定に向けて取り組んでいく。また、防衛当局間でも、脅威情報の共有やサイバー攻撃に対する共同訓練、人材育成における協力を進めつつ、新たな日米防衛協力のための指針の下、自衛隊と米軍との間の運用面における協力を一層強化させ、政府全体としての協力体制を確固たるものとすることにより、日米同盟の抑止力及び対処能力を向上させていく。

(3) 欧州

我が国と基本的価値観を共有する欧州諸国は、国際社会の平和と安定の実現に向けて、共に主導的な役割を果たすパートナーである。サイバー分野においても、各国及び関係機関と、防衛当局間を含めた様々なチャネルを通じた連携を引き続き強化し、サイバー関連施策やサイバー攻撃に関する情報の平素からの共有・活用、サイバー攻撃に対する共同訓練、先端的技術分野における共同プロジェクト等の協力を進めるとともに、国際場裡におけるサイバー空間の諸課題への対応及び協力を図っていく。

(4) 中南米、中東アフリカ

中南米、中東アフリカの両地域においても、共通の価値観を持つ国々とのパートナーシップを構築・強化するとともに、その他の多くの国とキャパシティビルディング等の連携・協力の可能性を検討していく。

5.4. 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つの政策目標の達成には、我が国において、これらを支える優れた研究や技術開発及び人材の輩出に向けたたゆまぬ努力が不可欠である。特にこうした共通基盤的な取組は、成果が出るまでに長い時間を要することに加え、多岐にわたる取組が必要となることから、横断的、中長期的な視点で取り組むとともに、官民及び関係省庁の事業・制度を柔軟に活用しつつ進める。

5.4.1　研究開発の推進

情報通信技術は、国民の社会生活に大きく浸透し、経済活動においてもイノベーションの源として一層の普及が進みつつある。ネットワークへ接続するシステムや機器は重要インフラ等での利活用を含めて大幅に拡大し、国、企業等はこれまで以上にサイバーセキュリティへの対策を講じていくことが必要になる。さらに、サイバー攻撃は日々進化し高度化・複雑化しており、その変化に対処していくため、ネットワーク、ハードウェア、ソフトウェア等の幅広い分野において、創意と工夫に満ちたサイバーセキュリティ技術を生み出すための充実した研究開発の推進が不可欠である。研究開発推進の考え方は以下のとおりであり、関係主体が連携し、それぞれが保有する情報、視点、強みを組み合わせることで推進していく。

(1)　サイバー攻撃の検知・防御能力の向上

IoT システム等が普及した連接融合情報社会において、より高度化・複雑化するサイバー攻撃等の脅威から政府、重要インフラ、企業・団体、個人を守るためには、その実態に応じて検知・防御能力の一層の向上が求められる。かかる能力向上に資するための研究開発には、現実にどのような脅威があり、具体的なニーズが何であるかを適時適切に把握して実施できるようにするための環境整備の充実が必要となる。また、サイバーセキュリティの研究開発は社会的なニーズを踏まえ実用化されることが重要であり、研究成果の社会還元の推進が重要である。このため、政府機関、研究者その他の関係者間で利用しやすい形式で必要となる情報・データの共有、例えば、サイバー攻撃耐性を向上させるため、M2M（Machine to Machine）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、解析する技術の開発を促進する。さらに、研究に係る法令、基準の検討等必要な取組を進めていく。また、政府が推進する研究開発プロジェクトにおいて、研究開発の企画段階からサイバーセキュリティを組み込むなど、防御能力の向上を進める。

(2)　サイバーセキュリティと他分野の融合領域の研究

サイバー空間は実空間と融合し、現実社会への影響も大きくなっていることから、

単に情報システム上での脅威を考えたり、学術的な研究を行ったりするだけでは、もはや脅威に対抗できない。法令等の研究や政策、情勢、技術といった様々な分野における分析手法の研究が必要である。このため、法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究促進、ビッグデータやAI（人工知能）といった社会・技術の変化を先取りした調査・研究・開発を進めていく。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。

(3) サイバーセキュリティのコア技術の保持

日々高度化・巧妙化するサイバー攻撃等を予測して対応していくためには、攻撃や防御のための技術の原理、システム等の仕組みなどを自ら考え開発するために必要なコア技術の保持が我が国として必要である。特に、コア技術を育む基礎研究については、暗号研究のように、直ちにビジネスにつながらないものの、経営力、事業開発力のある者との連携により、新たな産業創出の種となるものであり、また、安全保障の観点等から国として維持することが不可欠な技術もある。このため、公的研究機関や大学等の適切な研究機関において、研究開発を促す環境の整備を着実に進めていく。

(4) 国際連携による研究開発の強化

サイバー攻撃は国境を越えて行われることから、高度化・巧妙化するサイバー脅威に対処するための技術的な取組に当たっては、国際的に連携して、的確に対応できる、より高度な対策技術の開発に向け、各国が「強み」を有する技術を有機的に組み合わせ、発展させることが有効である。研究の内容や我が国の安全保障上の問題にも留意しつつ、国際連携による研究開発を積極的に行っていく。同時に、様々な国際標準化の取組が行われている中で、セキュリティ技術を中心とした様々な国際標準の策定・普及や相互承認の枠組み作りを進めていく。

(5) 関係機関との連携

研究開発は短い期間で成果が出るものではなく、長期的に取り組まなければならない課題である。また、研究開発を支える環境整備や研究者の育成については、サイバーセキュリティのみならず他の分野においても共通の課題である。このため、サイバーセキュリティという観点のみならず、環境の変化に留意しつつ、総合科学技術・イノベーション会議等の施策の主体となっている他の関連機関とも連携を図りながら、産学官が連携して総合的に積極的な施策を推進する[12]。

12　一例として、戦略的イノベーション創造プログラム（SIP）新規課題候補として「重要インフラ等におけるサイバーセキュリティの確保」が2015年６月18日の総合科学技術・イノベーション会議で決定された。

5.4.2　人材の育成・確保

情報通信技術が広く国民全体に拡大・浸透し、社会の基盤となっており、連接融合情報社会においては、サイバーセキュリティは、同分野の専門家はもちろん、一般的な情報通信技術者、ひいては IoT システムの利用者に至るまで、程度に差はあるものの様々な層の人材に必須の素養である。しかし、例えば、国内でサイバーセキュリティに関する業務に従事する技術者は現在、質的にも量的にも圧倒的に不足している[13]という現実に鑑みても、人材育成は喫緊の課題である。そこで、以下のとおり、サイバーセキュリティや関係する分野に係る教育の充実、突出した能力を有する人材の発掘・育成・確保、人材が将来にわたって活躍し続けるための環境整備等に取り組む。また、これらを含め、人材育成に係る施策を総合的かつ強力に推進するための方針を策定する。

なお、こうした人材においては、技術的な能力のみならず、高い倫理観も同時に身に付ける必要がある。

(1)　高等教育段階や職業能力開発における社会ニーズに合った人材の育成

今後社会で活躍できる高度な専門人材については、産学官がより一層有機的に連携し、社会のニーズに合った人材を量・質の両面から効果的に育成していくことが必要である。大学院、大学、高等専門学校等の高等教育機関においては、サイバーセキュリティに係る理論・基礎の習得と演習を通じた実践力の強化に向けた取組を推進する。この際、必要な知識や能力等の素養を十分有しているかを評価することが重要である。

また、産学官の協力体制構築に向け、緊密な連携や情報共有の促進に加え、サイバー演習の環境をクラウド環境で整備するとともに、産学官共同による教材開発を支援するなど、人材育成のための実践的な演習の取組を推進する。

また、企業等の組織経営にとってサイバーセキュリティが不可欠の課題となりつつある現状を踏まえると、経営戦略と技術的な観点の両面から思考でき、経営層と実務者層との間の橋渡しをすることで、セキュリティへの適切な経営資源配分を促すことができる橋渡し人材層が強く求められる。そのためにも、高等教育段階から、サイバーセキュリティや情報通信に関する技術的な能力とともに、法律や経営学等の社会科学を含めた様々な専門分野の知見、組織経営等に必要な知識を併せ持つハイブリッド型人材の育成を進める。

さらに、安全な製品・サービスの提供に当たっては、セキュリティの知識を備えつ

13　独立行政法人情報処理推進機構が2013年５月に行った試算によると、国内における情報セキュリティに従事する技術者は、約26.5万人と言われているが、必要なスキルを満たすと考えられる人材は10.5万人強であり、残りの16万人あまりの人材に対しては更に何らかの教育やトレーニングを行う必要があるとされる。また、潜在的には更に約８万人のセキュリティ人材が不足している状態とされている。

つ、製品・サービスの生産に関わることが必要不可欠である。情報通信技術を扱うあらゆる分野の技術者のみならず、その利用者に至るまで、様々な層の人材にサイバーセキュリティが必須の素養となりつつあることを踏まえ、高等教育機関によるリカレント教育や産学官連携による実践的な演習の機会の充実、職業訓練の活用促進等の取組が求められる。

(2) 初等中等教育段階における教育の充実

連接融合情報社会においては、個人、企業、政府機関など各主体が IoT システムを始めとする情報通信技術を存分に利活用できることが、自らの経済社会活動や生活を豊かにし、発展させていくために不可欠な基盤となる。そして、かかる社会において安全に活動していくためにも、サイバーセキュリティに関する素養は、程度の差はあるものの全ての人にとって必要なものとなる。このような素養としては、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解が必要であり、それらを初等中等教育段階から、児童生徒の発達段階に応じて培うことは不可欠である。また、高等教育の前段階においてこれらを身に付けることが、高等教育段階におけるサイバーセキュリティに係る高度な人材の育成や、一般の情報通信技術者及び利用者がサイバーセキュリティを必須の素養として身に付けるためにも欠かせない。

このため、初等中等教育段階から、児童生徒の発達段階に応じて、情報活用の実践力、情報の科学的な理解、情報社会に参画する態度を培う教育を一層推進し、情報セキュリティを含む情報モラルの理解等を促し、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解を促すようなものとなるよう取り組む。また、教員の情報通信技術を活用した指導力向上を目指した研修等の改善・充実を進める。

(3) 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

サイバーセキュリティ人材については、サイバーセキュリティに特化して高度な研究協力をする大学院等の機関による教育だけでなく、突出した能力を有する人材の発掘・確保も引き続き行っていく。また、例えばサイバー攻撃に対する対処法（防御手法、攻撃手法も含む。）の研究を通じ、自ら考え、対策を検討できる能力の育成を推進する。

さらに、サイバーセキュリティがグローバルな課題となっていることに鑑みれば、こうした突出した能力を有する人材はグローバル水準の能力を備える必要がある。つまり、国境を意識することなく十分に活躍できる人材の育成が不可欠である。このため、例えば、国内にいてもグローバル水準における自らの位置を把握でき、モチベーションを高めることができるよう、海外からの参加者を集めた競技イベントの実施、人材間のネットワーク形成等の取組を充実させるなど、政府として積極的に措置を講

ずる。

(4)　人材が将来にわたって活躍し続けるための環境整備

多くの一般的な組織は、その事業目的を実現するために情報通信技術を利活用しているが、このことは組織の経営課題として、サイバーセキュリティに取り組む必要性があることを意味する。これらの組織は実務の現場から経営までの各層において、それぞれのニーズに応じたサイバーセキュリティの知見を有する又は理解し判断できる人材が必要となる。また、サイバーセキュリティ関連産業においては、サイバーセキュリティに特化して突出した能力のある人材に加え、こうした人材をリードしていく人材も必要となる。さらに、それぞれの組織のニーズに応じた人材のキャリアパスを明確にすることが、組織の経営層、育成されたセキュリティ人材、人材育成者のそれぞれにとって有益である。

このため、サイバーセキュリティに従事する者の実践的な能力を適時適切に評価できる資格制度の創設や組織において業務に必要となる標準的なスキルの基準の整備により能力の可視化を図る。また、事業の性質や受入先のニーズも考慮しつつ、インターンシップ制度の充実を始めとしたマッチングに資する取組や、産学官横断的な人材のキャリアパス構築を推進する。加えて、企業財務その他の観点からも取組の促進を図る。こうした取組等を通じ、人材の需要と供給の好循環を創出していく。

(5)　組織力を高めるための人材育成

政府機関や重要インフラ事業者など組織全体をターゲットとしたサイバー攻撃が急増・深刻化する中、サイバー攻撃に的確・迅速に対応していくためには、個々人のサイバー攻撃対処能力の向上のみならず、これら個々人の能力を有機的に連携させ、組織全体としての能力の向上に結び付けていくことが極めて重要である。また、組織全体としての能力を効果的・効率的に向上させていくためには、異なる組織同士で切磋琢磨（せっさたくま）する環境を整備するとともに、個々の組織についてその実践的な能力や課題について具体的に把握できるようにしていくことが重要となる。

このため、組織のサイバー攻撃対処に必要な能力を体系化するとともに、それらの能力を向上させるための実践的演習の取組を充実させる。

加えて、深刻なサイバー攻撃等が発生した際、その被害拡大と再発抑止・低減等に向け、官民が一体的に連携して活動する体制の強化に取り組む。

6. 推進体制

サイバーセキュリティ戦略本部は、本戦略の推進に当たり司令塔機能を果たすとともに、NISC はその事務局として本戦略に基づく諸施策を推進するための主導的役割を担う。このため、ネットワークを通じた行政各部の情報システムに対する不正な活動の監視、監査、原因究明調査等の事務を行い、国内外のサイバーセキュリティに係る情報集約、分析、国際連携、各省庁のセキュリティ人材育成等の政府のサイバーセキュリティに係る能力を高める機能を担う。NISC は、この責務を確実に果たすため、高度セキュリティ人材の民間登用等により自らの対処能力の一層の強化を図り、インシデント発生時に適切に NISC へ情報が集約され、政府として適切な対応が行われるよう関係省庁（幹部クラスを含む。）との迅速な情報共有体制を構築するなど、必要な取組を推進する。

政府機関は、所掌事務を全うするため、NISC と十分に連携しつつ、必要なサイバーセキュリティの取組を行うとともに、所管する組織や事業者との情報共有や必要な助言を適切に行う責務を有する。特に、国全体としてサイバーセキュリティに係る能力を一層強化するため、産学官及び関係省庁間での情報共有など関係機関の連携強化を図る。また、インシデント発生時に冷静な対応を可能とするためには平素からサイバー攻撃等の事象の検知、分析及び対処のための体制を強化する必要がある。このため、平素からの情報収集を強化し、サイバー空間における脅威をあらかじめ予測し、また、迅速に察知し得るよう、国全体として、民間機関との連携や、カウンターサイバーインテリジェンスを含む、情報収集・分析機能の強化を行う。そして、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高度な情報分析・集約・共有機能を有する体制を整備する。

危機管理対応については、サイバーセキュリティ戦略本部長による勧告措置を始めサイバー攻撃等の事象に関する政府としての初動対処や対策状況の確認の在り方を改めて見直し、その一層の強化を図る。また、大規模なサイバー攻撃等の事象への対処に際し、政府機関､独立行政法人､セキュリティ事業者等が協力して対処する体制を確立するとともに、大規模なサイバー攻撃への対処や人材育成のための実践的な演習･訓練などの面において、産学官が緊密に協力し、一定の知見等を有する者と積極的な連携を図る。これには、独立行政法人情報処理推進機構等が有する知見を政府が行う不正な活動の監視、監査、原因究明調査等の事務に活用することや、国立研究開発法人情報通信研究機構等が有するサイバーセキュリティに係る対処能力向上のための演習基盤や攻撃観測・分析に対する技術的知見を活用するための方策が含まれる。これらを実現するため、法制の整備を含め所要の措置を講じる。

国家の関与が疑われるような、高度な技術と計画性を伴うサイバー攻撃は、近年増加している。こうした攻撃への対応は、我が国の危機管理、安全保障上においても重要な課題

である。このため、サイバーセキュリティ戦略本部は、必要に応じて重大テロ対策本部など危機管理の体制と情報共有、連携し、安全保障に関わる問題については国家安全保障会議と緊密な連携をして対応する。

さらに、2020 年のオリンピック・パラリンピック東京大会を始めとする国際的なビッグイベントにおけるサイバーセキュリティの十全な確保が必要である。とりわけオリンピック・パラリンピック東京大会については、同大会に係るサイバーセキュリティ上のリスクを明確にした上で、大会運営及びこれに関係する諸機関や、関連する重要インフラが提供するサービスへのサイバー攻撃に対して、予防、検知を的確に行い、関係主体に対して対処のための的確な情報共有を担う中核的組織としてのオリンピック・パラリンピック CSIRT の整備を加速化する。また、そのために必要となる組織・施設・協力関係の構築及び維持、専門家の確保、事前の十分な訓練について、2016 年の伊勢志摩サミット及び 2019 年に我が国で開催されるラグビーワールドカップにおける取組を踏まえ、段階的かつ着実に推進する。こうした取組によって培った対処能力については、持続的なサイバーセキュリティの強化のため、大会後においても活用していく。

こうしたサイバーセキュリティ政策は、危機管理・安全保障の観点からも極めて重要であり、これらを一層強力に推進するため、追加的に必要な経費等について、業務・システム改革その他施策の見直しを通じた行政の効率化等によって節減した費用等を振り向ける等による政府全体としての最適な予算の確保・執行を図るとともに、政府において専門性にふさわしい処遇等により高度なセキュリティ人材を登用するなど、実行可能なものは直ちに実施するとともに、新たな制度の整備が必要と認められる場合については、遅滞なく所要の措置を講じる。

7. 今後の取組

本戦略は、現状認識を踏まえ、2020 年代初頭の日本社会を見据えつつ課題を抽出し、その課題を解決するため、今後３年間に実施すべき施策の基本的な指針を示したものである。今後、本戦略を的確に実施するため、サイバーセキュリティ戦略本部はサイバーセキュリティ基本法に基づき、期間内各年度の年次計画を作成するとともに、その施策の進展を振り返り、年次報告として取りまとめることとする。あわせて、戦略で示された方向性に基づき各省庁の施策が効果的に実施されるよう、経費見積り方針を定める。また、サイバー空間においては、情勢や技術前提が非連続に変化することが極めて多いことを踏まえ、必要が生じた場合には、３年という計画期間に縛られることなく、機動的な見直しを行うこととする。

「サイバーセキュリティ戦略(案)」に対する意見募集の結果の概要

資料2－4

■ 実 施 方 法: NISCのWebページ及び電子政府の総合窓口(e-Gov)に掲載して公募を実施

■ 実 施 期 間: 2015年5月25日(月)～6月8日(月)

■ 意 見 総 数: 27者から83件

意見提出者の内訳 27者(個人:11、企業・団体:16)

83件(個人:30件、企業・団体:53件)

意見内容の内訳

- 全体に係る意見:21件
- 経済社会の活力の向上及び持続的発展に係る意見:25件
- 国民が安全で安心して暮らせる社会の実現に係る意見:23件
- 国際社会の平和・安定及び我が国の安全保障に係る意見:4件
- 研究開発、人材育成・確保等に係る意見:10件

※日本年金機構の個人情報流出事案に係る意見は3件

＜参考＞

提出者名:(株)アズジェント、アーバーネットワークス(株)、NPO法人市民オンブズマン・ネットワーク行政、(一社)新経済連盟、ソフトバンクモバイル(株)、トレンドマイクロ(株)、日本オラクル(株)、NPO法人日本セキュリティ監査協会、(一社)日本電気制御機器工業会、NPO法人日本ネットワークセキュリティ協会、日本ユニシス(株)、Virtual Engineering Community、BSA | ザ・ソフトウェア・アライアンス、ファイア・アイ(株)、(株)MESSA、メリルリンチ日本証券(株)、個人(11)

「サイバーセキュリティ戦略（案）」に係る意見募集の結果

資料２－５

27者　　83件

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
1	－	（株）アズジェント	5.2.3（１）ii. 被害の発生・拡大の防止	22	【意見内容】 ・訓練・演習に対する具体的な目標を如何に定めるか等の検討について記載してはどうか。 ・事態の早期把握のために、監視と監査を分離するのではなく、高い技術的調査も従来のセキュリティ監査に盛込むことを記載してはどうか 【理由】 政府や企業においては、ゲートウェイ・セキュリティ・ディバイス（FireWall、IDS/IPS、SandBOX 他）などを利用しSOCで監視を行っているが、これらのディフェンス・ラインで100%の防御は不可能であることは、世界的に周知の事実となっている。 侵入されてから被害が発見されるまで米国でも平均7か月というリサーチ結果にあるように、現状の焦点は発見・対策完了までの期間を短縮（潜伏期間中の早期発見）し、被害を最小限に抑えるフェール・セーフを如何に高い精度で、効率良く施せるかにある。 よって、ディフェンス・ラインの防御率を上げることは勿論であるが、侵入されてしまった後のフェール・セーフの仕組み作りを早急に進めることをガイドラインに組み込むべきである。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、御指摘の内容については、今後の施策の実施に当たっての参考とします。 なお、5.2.3(1)に記載のとおり、本戦略においては「全ての政府機関等において、攻撃に直面することを前提とした多層的な対策を講ずる」旨を掲げており、御意見のように侵入されてしまった後のことも想定した対策についても推進して参ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
2	－	アーバーネットワークス（株）	5.2.2 重要インフラを守るための取組 5.2.3 政府機関を守る	18-23	重要な国家インフラは、例えば、金融、航空、鉄道、電力、ガス、水道などだけでなく、政府機関はすべて、攻撃者のターゲットになる可能性が高い。経験と統計では、DDoS攻撃やAPT攻撃は共に最も一般的な攻撃であることが示されている。 従って、日本政府は、さまざまな産業がサイバーの世界でさまざまな種類の攻撃から自分自身を守るための勧告を提唱する必要がある。 組織は、ビジネスの継続性、運用手順、災害復旧に対して、独自の要件を考慮し、そこに主要な構成要素としてのDDoS防御を含める必要がある。異なるDDoS防御の組み合わせは、Webプレゼンスにとって重要であり、組織のために必要である。同時に、それは、組織内に必要なベストプラクティス（最善の措置）を開発することでもある。 攻撃者らは非常に狡猾であるため、ここ数年では、攻撃の特定カテゴリとして、多くのAPT（Advanced Persistent Threat）攻撃と呼ばれる新しいタイプの攻撃が一般的になっている。 残念ながら、今日の企業は、予防セキュリティメカニズムに過度に依存している。予防措置が違反を検出する唯一の方法であってはならない。いわゆるサンドボックス機能を備えた違反検出システムは、多くの場合、完全なネットワークや組織が識別できるようなコンテキストデータ、完全な範囲を提供したり、問題となる攻撃も優先しない。また、それらは、ネットワーク全体からIOC	御指摘の内容については、政府機関、重要インフラ、企業等における今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
			ための取組		（侵害指標）を相関分析したり、より高度な隠密攻撃に迅速に対応するために必要なネットワーク機能を提供していない。 重要インフラ組織は、内部へのAPT攻撃に対処するためのセキュリティ分析のアプローチを採用する必要がある。 セキュリティ分析の目標は、組織内のネットワークセグメントからすべての重要なトラフィックをキャプチャし、分析を完了することである。それは、フルパケットデータ解析を行うために設計されたビッグデータソリューションである。 我々は、さまざまな当事者がマルウェアやその他の高度な脅威の識別および無力化のために共同作業を行うことができ、日本国内のさまざまな組織から信頼できるセキュリティ専門家のプライベートソーシャルネットワークを構築することをお勧めする。これは、セキュリティ担当が効果的に、多くの場合、伝統的なセキュリティ防御では検出されない複雑な隠密攻撃に対抗するための実用的な情報を共有する場合に非常に有効である。	
3	－	NPO法人市民オンブズマン・ネットワーク行政	全般	－	【意見内容】 機密保護は国家として火急に絶対安全を完成させなければならない。 【理由】 同封のセキュリティを考え特許を取得した者は、イタリア人であるが、ガリレイガリレオの再来と云われる天才である。このソフトを破るには25億年かかると言われるものである。是非検討されることを進言します。 そして採用される事を希望します。国民のためです。これでセキュリティは万全です。	御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
4	－	（一社）新経済連盟	全般	－	情報セキュリティの意識向上が必要不可欠であり、そのために必要な官民の取り組みを提言として政府に提出している。今回の戦略案に記述として反映いただくとともに、施策の実行の参考にぜひしていただきたい。 http://jane.or.jp/topic/detail?topic_id=394 （提言概要） ・関係有識者のヒアリングの結果まとめ ・セキュリティに関するグローバル調査の解析結果を踏まえ、日本企業とグローバルでの意識の格差等を提示 ・以下具体的な政策提案項目 ①企業ボードメンバーによるセキュリティ対策に対する意識を向上し、当該対策に必要な経営資源を振り向けるようにする。 ②IT分野全般及びセキュリティに関する幅広い知見・技術と倫理観を持ったセキュリティ人材の養成と地位向上 ③企業や業種を超えたセキュリティ担当者間の情報共有の充実強化 ④社員へのセキュリティ教育を徹底するほか、一般社会のセキュリティ意識の向上と企業全体のセキュリティレベルの向上を図る。	今回のサイバーセキュリティ戦略においては、 5.1.2「セキュリティマインドを持った企業経営の推進」として ・企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築 ・経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成 ・民民間・官民間における脅威・インシデント情報の共有・演習等実施の推進 等について記載しております。 5.4.1「人材の育成・確保」として ・他分野の知識も併せ持つハイブリッド型人材の育成促進 ・高等教育等における産学連携の推進・実践的演習の充実 ・国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保　　等について記載しております。 御提言の趣旨は、これらの方向性と合致するものであると考えます。また、これらの施策の推進にあたっては、経済界と政府との連携が重要であると考えております。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
5	－	ソフトバンクモバイル（株）	5.2.1（3）サイバー犯罪への対策	17-18	2105年4月17日、総務省にて意見募集が開始された「電気通信事業における個人情報に関するガイドライン及び解説の改正案」において、接続認証ログにおける保存の在り方が明確化されるところですが、本来、接続認証ログを含め通信履歴は、課金目的や苦情対応などの各通信事業者が業務を遂行する場合に限り、記録・保存することが可能な通信の秘密として保護されるべきものです。 よって、通信履歴の保存の見直しについては、必要性及び有効性を都度慎重に議論する必要があると考えます。仮に上述の目的や理由以外の必要性において通信履歴を保存する場合は、事前に十分な法的議論を経た上で、法令等の改正やガイドラインの整備といったステップを踏むべきです。 また、トラヒックが急増する昨今において、新たな目的のために通信履歴を保存することになれば、通信事業者に対し新たに多大なコスト負担・運用負荷がかかることは明白です。よって、本件に関しては、その必要性及び有効性が認められることを明確にし、国民の理解を得たうえで、議論をすべきと考えます。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
6	1	トレンドマイクロ（株）	5.1.1(3)	10	【記載内容】 官民で連携しつつ、IoTシステムの構成要素であるM2M（Machine to Machine）機器やウェアラブル端末等の機器を含め、エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドラインや基準の整備を行う。 【意見内容】 記載内容にそれが意識されているか不明であるが、将来的には管理者のわからない自律的に稼働し続けるIoT機器やハイジャックされ管理者からは制御不能IoT機器がネットワーク上に存在し、他社への攻撃や帯域を占有するなどの被害が想定される。そのような事案が発生した際に所定の手続きを経てそれら機器を排除できる手法についても検討するべきである。 【理由】 おもにISPなどがその実務にあたるとは思うが、発生から排除までに時間を要さずに行動する必要があるため、事前の取り決めが存在することが望ましい。	御指摘の内容については、5.1.1(3)の「関係者が連携しIoTシステムや、その構成要素である機器等の脆弱性を調査し、供給者への修正を促すとともに、利用者に着実に対策が行き届くような仕組み」を検討していく中で、参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	2	トレンドマイクロ（株）	5.1.2(1)	11	【記載内容】 CISO（Chief Information Security Officer）の機能が各企業の経営層に確実に位置付けられるよう、官民で連携して促す。 【意見内容】 CISOを育成する講座や教育コースなどの整備が求められる。 【理由】 CISOの定義やミッションは各社によって異なる。現状の日本にはCISOのあるべき姿やベストプラクティスが少なく、CISOがどのようにあるべきかを学ぶ場所も少ない。CISOという役職が形骸化しないために事例研究を含めた研究と成果のトランスファーが求められる。	御指摘のとおり、CISOを含む企業経営層に対する普及・啓発活動については重要と考えており、具体的な施策については年次計画の中で記載しています。
6	3	トレンドマイクロ（株）	5.1.2(2)	12	【意見内容】 以下の文言を追加する。 「政府は警察庁または防衛省において毎年数百名単位でサイバーセキュリティ専任者を採用し、育成に努めサイバー犯罪への対策、国家の安全の維持に努める。」 【理由】 今回の戦略案においてはセキュリティ技術者の出口・キャリアプランまで盛り込まれており、大いに期待できるところではある。しかしながらそのほとんどが民間の努力に期するものであり、現状を鑑みるに短期的に成功をもたらすとは考えにくい。よって、政府が率先してセキュリティ技術者育成のために機会を提供し、次代を担う世代がセキュリティで立身できる世界を実現するべきである。	御指摘のとおり、政府も含め官民をまたいだセキュリティ人材のキャリアパスの構築は重要な課題であると考えておりますので、「インターンシップ制度の充実を始めとしたマッチングに資する取組を推進する。」を「インターンシップ制度の充実を始めとしたマッチングに資する取組や、産学官横断的な人材のキャリアパス構築を推進する。」に修文します。 なお、「新・情報セキュリティ人材育成プログラム」（2014年５月 情報セキュリティ政策会議決定）において、「専門人材の育成・登用は、求められる人材像を社会に示し、情報セキュリティ人材に関する需要の呼び水にもなりうることから、政府として率先して進めることとする。」としているところです。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	4	トレンドマイクロ（株）	5.2.1(3)	17	【意見内容】 「このため、国は、サイバー空間の脅威に関する実態把握のための情報収集の強化やサイバー犯罪に係る捜査能力の向上、取締り体制及び取締りのための情報技術解析体制等の体制強化を進め、必要な人材育成や技術開発を着実に推進する。」の後に以下を追加する。 「そして、国は、国民に対してサイバー空間の脅威の啓発に努め、国民が被害通報・報告のしやすい環境の整備を推進する。」 【理由】 追跡の前段階としての、利用者からの被害通報が重要である。サイバー空間における少額被害など通報されることなく潜在しているマイクロ犯罪が多発している。これら犯罪を放置することが結果、犯罪者優位な状況を生み出す結果となっている事を広く国民に理解を求める必要があると考える。 被害情報が早期に共有されることで、類似犯罪発生時に利用者自らが危険を察知し、犯罪抑止につながる効果も期待できる。 サイバー犯罪に巻き込まれた疑いがあるときに、そのサービスを提供するプロバイダへ報告・相談することを呼びかけ、よいサイバー空間の習慣を実践する事が、世界中のデジタル社会に恩恵をもたらす結果となることを広く周知すべきである。	ご指摘いただきました、国民に対する啓発、国民が被害通報・報告のしやすい環境の整備につきましては、5.2.1(2)「国は、各種啓発主体と連携し、「サイバーセキュリティ月間」を始めとし、不正プログラムや不審なメールへの対処の方法等に係る普及啓発活動を推進する。」や「さらに、インターネット利用における悩みや不安に関する相談に応じられる人材を育成し、活動を促す取組についても、引き続き着実に推進する。」に含まれるものと考えており、原案のとおりとさせていただきます。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	5	トレンドマイクロ（株）	5.2.3(1) ii	22	【意見内容】 「また、政府機関で重大なインシデントが発生した場合における原因究明調査のための取組を強化し、分析結果を共有することによって被害の拡大防止を図るとともに、対策の改善に反映させる。」を以下のとおり修文する。 「また、各政府機関が有するCSIRTと普段から連携すると共に、政府機関で重大なインシデントが発生した場合における原因究明調査のための取組を強化し、分析結果を各政府機関のCSIRT共有することによって被害の拡大防止を図るとともに、対策の改善に反映させる。」 【理由】 既に中央省庁ではCSIRTが整備されていると思われ、CSIRT連携はインシデント発生時の連携だけでは円滑なコミュニケーションは図れない。そのため、定常時から連携体制を確認し合い、重大なインシデントに備えることが重要であるから。	御意見を踏まえ、「政府機関横断的な監視・即応機能及び各機関における事態の把握・対処機能の強化に取り組むとともに、インシデントの発生に備えた訓練・演習を実施し、対処要員の能力及び連携の強化を図る。」を「GSOCによる政府機関全体における検知・解析機能の強化、並びに各機関におけるインシデント対応を行うチーム（CSIRT）の体制及び事態の把握・対処機能の強化、インシデント発生時の情報提供の迅速化・高度化に取り組む。また、インシデントの発生に備えた訓練・演習を実施し、その教訓を施策に反映させるとともに、対処要員の能力・連携の強化及び各機関幹部による指揮の下での組織的対処の徹底を図る。」に修文します。
6	6	トレンドマイクロ（株）	5.4.1(1)	32	【意見内容】 「政府機関、研究者その他の関係者間で必要となる情報・データの共有」を以下のとおり修文する。 「政府機関、研究者その他の関係者間で連携の行いやすい形式で、必要となる情報・データの共有」 【理由】 データの共有においては、機械処理（コンピュータの取り扱い）がしやすく、連携可能な標準形式を策定しての配信が必要である。実例として、Excelのセル結合を使用し、再加工しなければ、機械に取り込みができないようなデータ形式での配信事例が見られる。このような機械処理しづらい形式でのビッグデータ共有は、生産性を低下させる恐れすらある。あらかじめデータ連係を想定した情報共有システムデータの設計が重要と言える。	御指摘を踏まえ、5.4.1(1)の「政府機関、研究者その他の関係者間で必要となる情報・データの共有」を「政府機関、研究者その他の関係者間で利用しやすい形式で必要となる情報・データの共有」に修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
6	7	トレンドマイクロ（株）	5.4.2(2)	35	【記載内容】 このような素養としては、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解が必要であり、それらを初等中等教育段階から、児童生徒の発達段階に応じて培うことは不可欠である。 【意見内容】 User-Generated Contentsの作成に掛かるコストの低下により、利用者による十分な思慮が行われなかった情報発信の結果、自らまたは他人を傷つけるような事象が頻発している。自らの行動がどのような影響を及ぼす可能性があるのか、立ち止まって、考えるための教育機会の提供が必要である。その為の素養として、知的財産リテラシー、プライバシーポリシーなどを読み解く能力が必要と考える。具体的事案として、児童が自らの意思で投稿を行った動画や写真による児童ポルノへの悪用、他人のコンテンツの無断使用、反社会的行動を自らの意思でさらけ出すような行為、サービス提供内容の理解不十分による過剰な範囲での情報共有などがあげられる。サイバー空間上の自身の行動によって、世界中の人々を含め、他の方々すべてに影響を及ぼす可能性があることを初等中等教育段階から継続的な取り組みが必要であると考える。 【理由】 情報セキュリティ教育に加え、早期段階から知財教育を実施することが望ましい。	御指摘の内容は、5.4.2(2)の「初等中等教育段階から、児童生徒の発達段階に応じて、情報活用の実践力、情報の科学的な理解、情報社会に参画する態度を培う教育を一層推進し、情報セキュリティを含む情報モラルの理解等を促し、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解を促すようなものとなるよう取り組む。」の「情報モラルの理解等」に含まれていると考えています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
7	1	日本オラクル（株）	5.1. 経済社会の活力の向上及び持続的発展	8	【意見内容】 「IoTシステムの提供するサービス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ことが、今後の社会全体としての課題（チャレンジ）となる。」の後に次の段落として以下を追記する。 「また、IoTの活用の背景には、ネットワークを通じたサービスの利用を普及させるというネットワーク中心思想から、情報システム及びサービスの 中核であるデータを個人や部門の所有ではなく、エンタープライズ単位で、或いは関連企業等のステークホルダー、消費者などの拡大コミュニテイ内で 共有し、活用していくというデータ中心思想への転換がある。データ中心の情報システム及びサービスを円滑に動かすためには、データオーナー（data owner）の責任とマスタデータ管理が不可欠であるとともに、ネットワークセキュリティからデータセキュリティへの軸足の移動が必要とされる。クラウド 化の推進により、データセンタに膨大なデータが集約され、一回のサイバー攻撃で数百万件の個人情報等が漏洩する現状を考慮すると、データベースセ キュリティを含む多層のデータセキュリティを確保するのは急務である。」 【理由】 日本年金機構における大量の個人情報漏洩が社会問題化している現状に見られるように、最早、水際対策では高度サイバー攻撃を阻止できず、効果的 な内部対策の実現が求められている。	御指摘を踏まえ、5.1において、以下のとおり修文します。 「例えば、サイバー攻撃によりモノが意図しない動作をするよう遠隔操作されたり、ウェアラブル端末を通じて個人に関する情報が窃取されたりといった実空間に密着したリスクや、1回のサイバー攻撃で多くのステークホルダーが関与するデータベースから数百万、数千万件の個人情報等が流出するといった経済社会に重大な影響を及ぼすリスクは、こうしたサービスの信頼性や品質を根本的に損なう。」

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
7	2	日本オラクル（株）	5.2.3 、i.インシデントの未然防止	22	【意見内容】 「また、サプライチェーン・リスクへの対応を始めとした情報システムの企画・設計段階からセキュリティの確保を盛り込むための取組を推進する。」に以下のとおり追記、修文する。 「また、サプライチェーン・リスクへの対応を始めとし、データの保全を念頭にした情報システムの企画・設計段階からセキュリティの確保を盛り込むための取組を推進する。」 【理由】 サイバー空間で懸念される現実の脅威は、例えば、個人情報を含む機密情報の窃取、データの改ざんなどを起点として、サイバー空間を含む人間社会 全体に問題が波及する。つまり、起点となるデータの保全こそが最大の課題になる。そのため、情報システムの企画・設計段階から、データのライフサ イクルに焦点に当て、データの保全を念頭においたセキュリティの確保が最低限必須の要件となる。	御指摘のとおり、情報システムの企画・設計段階からデータ保全を念頭に置くことは重要であると考えています。他方、企画・設計段階から念頭に置くべき事項は必ずしもデータ保全に限られるものではないため、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
7	3	日本オラクル（株）	5.4.1(4) 国際連携による研究開発の強化	33	【意見内容】 「同時に、様々な国際標準化の取組が行われている中で、セキュリティ技術に関する国際標準の策定・普及や相互承認の枠組み作りを進めていく。」を以下のとおり修文する。 「同時に、さまざまな国際標準化の取り組みの中で、セキュリティ技術を中心とした要素技術、システムインテグレーション技術など幅広い視野に立った国際標準の策定・普及や相互承認の枠組み作りを進めていく。」 【理由】 IoTまでを視野に入れたサイバーセキュリティを考えるとき、単なるセキュリティ技術に関する国際標準の策定・普及や相互承認の枠組み作りでは 片落ちになる懸念がある。例えば、クラウドコンピューティング環境を前提とするIoTの場合では、インターネットにつながる機器がクラウドサービ ス使用者となり、現在想定されているクラウドコンピューティングのモデルを一歩進化させねば対応が難しいと考えられる。このような状況も踏まえた 上で、国際標準の策定を行わねばならない。そのためには、セキュリティに関する標準化技術者のみならず、幅広い標準化技術者の参画が必須となろ う。「4.5　多様な主体の連携」に「サイバーセキュリティに係るビジョンを共有し、それぞれの役割や責務を果たし、また努力する必要が ある。そして、政府はこれらのステークホルダーを適切な連携関係へと促す役割を担っている。」とあるが、この考え方は、堅牢で柔軟なサイバーセ キュリティを実現するための国際標準化にとって極めて重要なカギとなる。	御指摘の趣旨を踏まえ、セキュリティに資する幅広い技術等という観点から、5.4.1(4)の「セキュリティ技術に関する国際標準」を「セキュリティ技術を中心とした様々な国際標準」に修正します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
8	1	NPO法人日本セキュリティ監査協会	5.1.2 セキュリティマインドを持った企業経営の推進	11	【意見内容】 「セキュリティ人材の育成、組織能力の向上等を図ることが必要となってくる。」の後に以下を追記する。 「加えて、企業と政府、企業相互ならびに企業と利用者間の信頼を醸成するために、経営者が情報セキュリティ管理に関する説明責任を果たすことが求められる。」 【理由】 経営者の意識改革のためには、重要な情報を扱っている企業の経営者自身が説明責任を果たす責務を負うことが必要となる。意識改革の啓発活動において、説明責任を果たすことを明確にしておくとともに、そのためには自社の情報セキュリティ対策が適切に行われていることを確認する必要がある。特に、重要な情報を扱う民間企業においては、第三者として独立した専門家による監査に基づく保証を得ることが重要である。	御指摘のとおり、経営者による的確な認識と説明は重要であり、5.1.2(1)に「サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成」と記載しており、この中に御指摘の考え方も含まれていると考えており、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
8	2	NPO法人日本セキュリティ監査協会	5.1.2 (1) 経営層の意識改革	11,12	【意見内容】 「ステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成のための官民が一体となった啓発活動を実施する。」の後に次の段落として以下を追記する。 「また、情報セキュリティ管理が適切に行われていることを情報セキュリティ監査で確認し、その結果の公開等を通じて、情報を取り扱う主体としての説明責任を果たすことを促す。特に、大量の個人情報を取り扱う事業主体、重要インフラ事業者およびオリンピック・パラリンピックにおいて中核的な役割を担う主体においては、開催の前年度までに保証型情報セキュリティ監査を行い、第三者の保証を得ることとする。」 【理由】 経営者の意識改革のためには、重要な情報を扱っている企業の経営者自身が説明責任を果たす責務を負うことが必要となる。意識改革の啓発活動において、説明責任を果たすことを明確にしておくとともに、そのためには自社の情報セキュリティ対策が適切に行われていることを確認する必要がある。特に、重要な情報を扱う民間企業においては、第三者として独立した専門家による監査に基づく保証を得ることが重要である。	御指摘のとおり、経営者による的確な認識と説明は重要であり、5.1.2(1)に「サイバーセキュリティを経営上の重要課題として取り組んでいることが市場や出資者といったステークホルダーから正当に評価される仕組みや資金調達等の財務面で有利となる仕組みの構築、認識醸成」と記載しており、この中に御指摘の考え方も含まれていると考えており、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
8	3	NPO法人日本セキュリティ監査協会	5.2.3　政府機関を守るための取組	21	【意見内容】 「新たに直面した脅威・課題についても基準に逐次反映することによって対応してきたところである。」の後に以下を追記する。 「環境変化が急激であることからこれを加速し、基準等に準拠した情報セキュリティ対策が実施できていることについて、確認を行い、国民の信頼をより高めるようにしていく。」 【理由】 政府の情報セキュリティ対策に関する国民の信頼をより得ると共に、情報セキュリティ監査の結果をより有効に活用することが望ましいため。	御指摘の内容については、5.2.3に「政府機関等においては、既に顕在化している脅威や課題はもとより、未知の脅威等に直面した場合であっても柔軟かつ迅速に対応できるよう、従来から推進している対策に万全を期すことを前提としつつ、先々を見据えて以下の事項について重点的に取り組むとともに、政府機関における統一的な基準を始めとした規程に適時反映し、監査や平素からの教育などの取組によりその徹底を図る。」と、5.2.3(2)に「定期的な自己点検や第三者的視点からのマネジメント監査を始めとした点検の実施を通じて、政府機関等における対策強化のための体制・制度の検証・改善に取り組む」とそれぞれ記述しており、これに含まれると考えることから、原案のとおりとします。 なお、御指摘の「新たに直面した脅威・課題についても基準に逐次反映することによって対応してきた」については、政府機関等におけるこれまでの取組の概要として記述しています。
8	4	NPO法人日本セキュリティ監査協会	5.2.3（1）攻撃を前提とした情報システムの防御力の強化	23	【意見内容】 新たにⅳ項として以下を追記する。 「ⅳ. 信頼の確立　政府機関は国民の安全を守る立場であり、また、国民生活に重大な影響を与える可能性のある情報を国民から預託されている立場である。このため、国民の十分な信頼と期待に応える必要があり、実施している情報セキュリティ管理について、国民への説明責任を果たす必要がある。これまでも、情報セキュリティ監査等を行い、情報セキュリティ管理について報告書を公開するなど国民への説明に努めてきた。更に、新たな体制に基づきより厳密な監査を行うこととしている。今後、情報セキュリティ管理の責任者のコミットメントが果たされているかを検証する助言型監査を行うと共に、2020年までに重要な情報を取り扱う組織を対象に保証型監査を実施し、信頼の確立を図る。」 【理由】 政府の情報セキュリティ対策に関する国民の信頼をより得ると共に、情報セキュリティ監査の結果をより有効に活用することが望ましいため。	5.2.3(1)の「攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進」は、サイバー攻撃への対処に関する施策を記載するパートとしており、原案のとおりとします。 なお、情報セキュリティ監査に関しては、5.2.3(2)において「定期的な自己点検や第三者的視点からのマネジメント監査を始めとした点検の実施を通じて、政府機関等における対策強化のための体制・制度の検証・改善に取り組む」としているところであり、御意見については当該施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
9	1	（一社）日本電気制御機器工業会	全般	－	文章の至るところに「官民」連携という文言がありますが、「産学」の文言が入っておりませんが、なぜでしょうか。	「官民」と記載している場合は、官庁と民間組織（産学を含む）を指して用いていますが、「産学官」と記載した方がより文意が通じやすい箇所について、「官民」の記載を「産学官」に修文します。
9	2	（一社）日本電気制御機器工業会	全般	－	各戦略におけるスケジュールをある程度、明確にされてはいかがでしょうか。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、各年度に実施する具体的な施策の内容については、別途、年次計画を作成し推進していく旨、7.に記載しています。
9	3	（一社）日本電気制御機器工業会	5.2. 国民が安全で安心して暮らせる社会の実現	23	政府及び重要インフラ企業に対し、監査を徹底していく旨の内容が提示されています。そこで、各団体の制御システムセキュリティに関する取り組みを記載してはどうでしょうか。	本戦略では、重要インフラ企業に対する監査を徹底していく旨の内容は記載しておりませんが、制御系システムのセキュリティについては、その重要性を認識し、国際標準に即した第三者認証制度の活用等について記載しています。
10	－	NPO法人日本ネットワークセキュリティ協会	全般	－	官民を問わず、様々なサイバーセキュリティインシデントが頻発している昨今、さらに様々なIT新技術の利用が急拡大している現在、政府としてのサイバーセキュリティ戦略改定は大きな意味を持つものと考えます。新戦略に賛同すると同時に、サイバーセキュリティ業界の団体として、また、民間のサイバーセキュリティ向上をになう一翼として、日本のサイバー空間の安全、安心に今後とも様々な形で協力いたしていく所存です。とりわけ、民間企業においては、IT現場のセキュリティ能力向上や、情報交流、インシデント対応能力向上などが大きな課題となっており、こうした面でも政府と情報交換しながら、積極的に取り組みを進めたいと考えます。	本案に賛同する御意見として承ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	1	日本ユニシス(株)	全般	－	過去に策定された戦略との関係が不明なので、例えば平成25年に策定された「サイバーセキュリティ戦略2013」との関連性や継続性について1章で補足を付記していただきたい(過去の戦略とは変化があった部分や、捨てる部分、継続する部分についてなど)。	今回のサイバーセキュリティ戦略は、サイバーセキュリティ基本法(平成26年法律第104号)に基づき、閣議決定文書として策定されることとなっており、これまでの情報セキュリティ政策会議で策定していた戦略とは位置付け・内容ともに異なるものです。なお、個別の施策については、年次計画に記載することとします。
11	2	日本ユニシス(株)	2.2.サイバー空間における脅威の深刻化	2	「場所・時間の制約を受けず誰もが容易に参加できるサイバー空間は、悪意ある攻撃者に対し、防御側と比べて非対称な優位性を与えている。」における「非対称な優位性」の意味が判らないので補足を付記していただきたい。	御指摘の「非対称な優位性」とは、例えば、攻撃者は世界中の任意の場所から任意のタイミングで任意の手段で攻撃できることに対して、防御側は世界中のどこからどのような方法で来るかわからない攻撃に対して常にセキュリティを確保し続けなければならないため、取組の負荷やコスト、影響度等において攻撃側に非対称な優位性があることを指しますが、ここでは基本的な考え方のみ列記しており、個々の具体的な内容は記載していないことから、原案のとおりとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	3	日本ユニシス(株)	5.目的達成のための施策	7	【意見内容】 「4章 基本原則」の「4.5. 多様な主体の連携」において、「国民の表現の自由とプライバシーの保護を共存させ」とのあるべき姿が記述されていることに鑑み、5章の「目的達成のための施策」のどこかに「プライバシー・バイ・デザインの考え方を推進する」旨を追記してはいかがでしょうか。 【理由】 5.1.1(1)において「セキュリティ・バイ・デザインの推進」が記述されています。 今後の連接融合情報社会においては、パーソナルデータやマイナンバー情報を扱うことが飛躍的に増大するので、セキュリティ・バイ・デザインと並び、プライバシー・バイ・デザインの概念が必須となります。	サイバーセキュリティに係る施策を推進する中で、プライバシー保護の観点は非常に重要であると認識しておりますが、本戦略の「5. 目的達成のための施策」では、サイバーセキュリティに係る施策を示すことを目的としているため、「プライバシー・バイ・デザイン」の推進を掲げることは馴染まないものと考えます。尚、施策の推進に当たっては「4.1情報の自由な流通の確保」で記載している通り、「所要の規律とプライバシーの確保の適正なバランスについて十分な吟味を行うべきである」という基本原則に従うことも明示しております。
11	4	日本ユニシス(株)	5.1.1.(3) IoTシステムのセキュリティに係る制度整備	10	「官民で連携しつつ、IoTシステムの構成要素であるM2M(Machine to Machine)機器やウェアラブル端末等の機器を含め、エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドラインや基準の整備を行う。」とありますが、「官民で連携しつつ」の対応策として、ウエアラブルデバイスセキュリティの対策ガイドを検討・策定している(社)日本スマートフォンセキュリティ協会等を活用してはいかがでしょうか。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
11	5	日本ユニシス(株)	5.1.3.(2) 公正なビジネス環境の整備	14	「セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置に対しては、国際的な連携の下、厳格に対処する。」における「セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置」の意味が判り難いので具体例を追記していただきたい。	ここでは一般論として記載しており、特定の例を挙げることは適切でないと考えるため、原案のとおりとします。
11	6	日本ユニシス(株)	5.2. 国民が安全で安心して暮らせる社会の実現	15	「残存リスクの情報も添えて経営者層に対し総合的な判断を受ける機能保証(任務保証)の取組が必要である。」における「機能保障(任務保障)の取組」の意味が判り難いので、具体的に記述していただきたい。	御指摘を踏まえ、より文意が通じやすいよう、御指摘の箇所について、「残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証(任務保証)」の考え方に基づく取組が必要である。」と修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	7	日本ユニシス(株)	5.2.3政府機関を守るための取組	21	実際にインシデントが発生してしまった場合にどう対応するかについての指針が必要に思われます。例えば、インシデント発生時の被害状況公開の指針、被害者からの問い合わせへどんな情報を提供するかなどの指針など。	インシデント発生時の対応については重要であると考えており、5.2.3(1)において対応方針を記載しているところです。御指摘の内容については、今後の施策の検討に当たっての参考とします。
11	8	日本ユニシス(株)	5.4.1　研究開発の推進	32	【意見内容】 長期的な視野に立って、老若男女のあらゆる利用者が、そのリテラシーの高低にかかわらず、いつでもどこでも、ストレスなく使いこなせるセキュリティ対策技術の研究開発推進を追記してはいかがでしょうか。 【理由】 現在のインターネット利用環境においては、一般利用者が使用する端末機器のセキュリティ確保において相当なリテラシーが要求され、普通の利用者にはあまりに実現困難な対策が多くあります。そのため、一般利用者のリテラシーに係わらず適正なセキュリティ確保が実現できるような対策手法の研究開発の推進が望まれます。	御指摘の点については、5.4.1(1)「サイバーセキュリティの研究開発は社会的なニーズを踏まえ実用化されることが重要であり、研究成果の社会還元の推進が重要である。」に含まれるものと考えており、原案のとおりとします。 なお、「情報セキュリティ研究開発戦略(改定版)」(2014年7月 情報セキュリティ政策会議決定)において、利用者の視点を踏まえた研究開発について記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
11	9	日本ユニシス（株）	全般（連接融合情報社会の適切な維持のため、比較的実行が容易な物理テロ対策の追記について）	－	【意見内容】 例えば民間のクラウド・データセンター等に対する、郵便による炭疽菌の送り付けや火炎瓶等の発火物持参による突入など、比較的簡単に実行が可能な物理テロへの備えは、大規模（地震）災害対策と同様に必須と考えます。 しかしながら、ISO27000ベースの規程や日本国内の各省庁が制定しているセキュリティ基準やガイドラインには物理テロ攻撃を想定した対策要件が記述されておらず、また民間企業にはその対策に係る知見がありません。 連接融合情報社会の適切な維持のためには、サイバーセキュリティと並んで比較的実行が容易な物理テロによる情報システム破壊への適切な防御施策が望まれます。これにより、グローバルな性質を持つサイバー空間の平和と安定に寄与できます。	御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、サイバーセキュリティの観点からも重大な事象については、サイバーセキュリティ戦略本部は、必要に応じて重大テロ対策本部などの危機管理の体制との連携や、国家安全保障会議との緊密な連携等により対応していきます。
12	1	Virtual Engineering Community	全般	－	制御システムでは、現場の安全基準と対策があり、それに「制御システムセキュリティ対策」が加わったリスクアセスメントが求められると考えます。 日本の各産業別特異性も考慮した制御システムセキュリティアセッサ制度の実現と、認定試験及び普及啓発活動を実施していく民間機関創設の必要性を感じております。	制御システムのセキュリティに係る評価・認証制度等への取組については、5.1.3(3)において、「制御装置等を含むIoTシステムのセキュリティに係る国際的な標準規格や評価・認証制度の国際的な相互承認への枠組み作りについて、産学官が一体となり、国際的議論を主導していくほか、我が国のベストプラクティスの国際的な共有・展開を図る。」と記載しています。 御指摘の内容については、今後の施策の検討に当たっての参考とします。
12	2	Virtual Engineering Community	全般	－	制御システムを対象にしたペネトレーションテストする場合は、現場の安全対策を施した上で実施されなければならない為、かなりのコストと時間が必要となります。 できるだけコストと時間をかけないで安全に実施効果を出す技術的検討も事前検討に含めておくことになると思います。	制御システムを含むIoTシステム全体としてのセキュリティ確保のための対策として、5.1.1(4)において、「テスト環境の構築や、システム全体の脅威分析・リスク評価手法の開発、ICチップを含むハードウェアの真正性の検証等、社会科学的な研究も含め、IoTシステムにおける対策検討等に必要な技術開発・実証事業を行う。」と記載しています。具体的な施策については年次計画の中で記載します。 御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
12	3	Virtual Engineering Community	5.2.2 重要インフラを守るための取組	18-21	重要インフラ事業者の内部監査、外部監査の実施について 内部監査や外部監査を実施するに、監査範囲・監査項目・監査基準・監査方法の定義と内容設定が必要となります。アセットオーナー対象とサプライヤ対象の監査チェックシートを活用してはいかがでしょうか。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
12	4	Virtual Engineering Community	5.4.2 人材の育成・確保	34-36	e-learning教育ビデオ講座やゲーム形式でインシデント疑似体験ができるトレーニングの活用、制御システムセキュリティ対策のセキュアなアセットオーナー管理者やセキュアな制御システムエンジニアリング設計技術者やセキュアな制御製品開発技術者を目指す方々が自分の実力がどこにあるかを見る目安となる模擬試験の実施などによる制御システムセキュリティ対策の人材教育が重要と考えます。	実践的演習や能力の可視化の重要性や取組について、5.4.2(1)、5.4.2(4)、5.4.2(5)で記載しており、御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、具体的な施策については年次計画の中で記載します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	1	BSA｜ザ・ソフトウェア・アライアンス	5.1.1 (1) 安全な IoT システムを活用した新規事業の振興	9	【意見内容】 当該箇所については、「IoT システムに係る新たな事業を成功させるためには、競争力の源泉となる高いレベルでのセキュリティ品質の実現が不可欠である。このため、システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。そして、IoT事業者は、この考え方を、既存システムのアップグレードやレガシーインフラへのつなぎこみの際にも考慮すべきである。具体的には、「IoT システムに係る事業について、セキュリティ・バイ・デザインの考え方に基づき所要のセキュリティ対策を業態横断的に推進し、メリハリをもって、積極的に新規事業の振興を図る。」との方針を記載すべきと考えます。 【理由】 セキュリティ・バイ・デザインを推進していくべきことについては賛同しますが、現実には、既存のシステムがセキュリティ・バイ・デザインの考え方に基づいた新システムに完全に入れ替わるまでには、長い時間を要します。このため、完全に新システムに移行するまでの間、既存のシステムのアップグレードやレガシーインフラへのつなぎこみの際にも、セキュリティを確保していく方策について考える必要があります。	御指摘を踏まえ、「このため、システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。」を「このため、連接される既存システムを含めて、IoTシステム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。」に修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	2	BSA｜ザ・ソフトウェア・アライアンス	5.1.1 (2) IoTシステムのセキュリティに係る体系及び体制の整備 (3)IoTシステムのセキュリティに係る制度整備	9,10	日本政府が、セキュリティー般、特にIoTに依存する部分について、そのルールを、事業者にとってより明確になるよう取り組まれることを歓迎します。また、民間部門と十分な協議のもとルールを策定するとの本戦略のアプローチに賛同します。日本政府においては、適切なサイバーセキュリティ政策及び当該政策を実施するための正しい制度的枠組を策定すべく、引き続き取り組んでいただけるようお願い致します。この際、サイバーセキュリティに関する体系・体制・制度整備は、以下の重要な原則（以下「推奨基本原則」という。）に基づき策定されるべきと考えます。 （ア）リスク・ベースかつ優先順位をつける （イ）技術中立性 （ウ）実行可能であること （エ）柔軟性 （オ）プライバシー及び市民の自由の尊重 以上に加えて、（ア）不必要で不合理な要求事項の策定を避け、事業者が自らが最も直面し得るリスクを低減できるように、幅広く、最も効果的な最先端のサイバーセキュリティソリューションを開発し、採用できるようにし、（イ） 業界が参加して国を超えて承認された、国際的認知のある標準を採用し、（ウ）最先端の製品及びサービスは、複数の異なる国に存在する研究開発拠点の国際的な協力のもと開発されるものであるから、現地で生まれた技術を優先する政策を回避することも非常に重要であり、これらを政策として採用するよう政府に対し要望致します。	IoTシステムのセキュリティに係る体系・体制の整備、制度整備について、産学官が連携して取り組んでいくことは重要であり、御指摘の内容については、各種ガイドラインの策定等、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	3	BSA｜ザ・ソフトウェア・アライアンス	5.1.2 （1）経営層の意識改革	11	事業者及び団体におけるサイバーセキュリティ対策の採用を促進する政府の取組みに賛同します。堅牢なサイバーセキュリティの確保は、我が国の経済社会の活力の向上及び持続的発展のために必要であることにとどまらず、海外における競争力の向上にも役立つものであるため、その点追記すべきと考えます。即ち、堅牢なサイバーセキュリティの確保は、消費者及び投資家双方の信頼を獲得し維持するものだからです。	本案に賛同する御意見として承ります。
13	4	BSA｜ザ・ソフトウェア・アライアンス	5.1.2（3）組織能力の向上	12	ガイドラインの策定や第三者認証の活用にあたっては、前記の推奨基本原則を考慮するよう要望致します。 また、本戦略は、サイバーセキュリティに関する懸念に対応する上で情報共有が重要であること及びこれを達成するためには官民協働が促進されるべきことを指摘しており、これに賛同します。	御指摘の内容については、今後の施策（ガイドラインの策定や第三者認証の活用等）の検討に当たって参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	5	BSA｜ザ・ソフトウェア・アライアンス	5.1.3(1) サイバーセキュリティ関連産業の振興(13頁)	13	サイバーセキュリティ分野におけるベンチャー企業等の活性化のため、政府系ファンドの活用によるベンチャー企業同士の国際的な交流を含む共同研究開発等の促進、公的研究機関とベンチャー企業との共同研究開発の促進等の取組が挙げられていますが、国家プロジェクトの予算が終了した後も持続可能なビジネスにするためにはどのようにすればよいのかというビジョンも提示すべきと考えます。従って、国内外の民間企業及び公的研究機関においてどのような実証実験及び事業が展開されているかの調査を行い、その結果を有効活用するような取組を本戦略に加えるべきであると考えます。	IoT産業等の関連産業の成長に伴い、今後、コンサルティングや人材育成ビジネスを含むサイバーセキュリティ関連産業に対する需要が一層増加することが見込まれることから、サイバーセキュリティ産業がこうした需要を捉え、成長産業となるよう、国内外で大規模に活躍できる企業の育成やベンチャー企業の育成等によりこれを振興していくことが重要であると考えており、御指摘の内容については、今後の施策の実施に当たっての参考とします。
13	6	BSA｜ザ・ソフトウェア・アライアンス	5.1.3(2) 公正なビジネス環境の整備	14	セキュリティを理由に国際的な貿易のルールに不適切な影響を及ぼす措置に対して、国際的な連携の下、厳格に対処することは非常に重要であり、これを強く支持します。 企業は、技術革新や消費者のニーズへの合致等、その目的に応じて、最適かつ最善のテクノロジーを使用することができなければなりません。また、インターネット関連サービスを提供する企業は、物理的なインフラを自国や自身の地域に保有する必要がないにもかかわらず、多くの国がそのような要件を課そうとしており、これにより企業に不必要なコストと負担を強いている問題があります。企業は、サービスをその国向けに変更したり、サービスを展開する国ごとに高コストのデータセンターを設置することを求められるべきではないと考えます。同様の関心を有する国と連携し、日本政府がこの問題に積極的に対応されることを要望致します。	本案に賛同する御意見として承ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	7	BSA｜ザ・ソフトウェア・アライアンス	5.1.3(3) 我が国企業の国際展開のための環境整備	14	【意見内容】 国際標準や評価認証制度の策定・関与が大変重要であることについて賛同致しますが、その取組においては、推奨基本原則に基づき牽引していただけるよう要望します。 また、サプライチェーン・リスクへのセキュリティ対策の協力を推進していくことは非常に重要な取組みであり、その際、ASEAN諸国のみに注力するのではなく、米国やEUなど同じ目標を持つ他の地域の政府ともパートナーシップを結んでいくことを要望します。 【理由】 「国際的なルールや規範の形成」「国際的な信頼醸成措置」「世界各国との協力・連携」等の箇所でも挙げられている事項ですが、このことは、サプライチェーン・リスクへのセキュリティ対策についても同様に行っていくことが有益であると考えます。これにより、本分野においても、より広範な国際協力体制の構築が可能となり、日本企業が世界のサプライチェーン要件を満たすことを確実なものとするからです。	御指摘のとおり、ASEAN加盟国のみならず、北米や欧州等との協力・連携を推進することが重要と認識しており、5.3.3において、その旨を記載しています。
13	8	BSA｜ザ・ソフトウェア・アライアンス	5.2.1(1)安全・安心なサイバー空間の利用環境の構築	15,16	調査を行った結果、ソフトウェアの不正利用とサイバーセキュリティの脅威との間に相関関係があることが分かりました。 管理を行うということは一見簡単なことのようですが、現実には、多くの事業者において、適正なソフトウェアライセンスのみの使用を命じる方針を採用するという、最初の第一歩が行われていません。 政府に対し、セキュリティリスクを減じるために、官民において、ソフトウェア資産管理のベストプラクティスを示し、これを共有することを要望します。	御指摘のとおり、安全・安心なサイバー空間の利用環境の構築を図る上でプラクティスの共有は重要と認識しており、一般利用者等への普及啓発に取り組む旨、5.2.1(1)においても記載しているところです。御指摘の内容は、今後の普及啓発施策検討に当たっての参考とさせて頂きます。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	9	BSA｜ザ・ソフトウェア・アライアンス	5.2.1(1)安全・安心なサイバー空間の利用環境の構築	15,16	マルウェアに感染したネットワークが構成するボットへの先手的な対応の検討は具体的なものである必要があると考えます。これには、法的・制度的に未整備の部分についての検討を含み、また、対応策について、民間の知見を充分に活用されることを期待します。日本においても、米国事例も参考に、より柔軟な制度を検討していくことが有益であると考えます。 さらに、警察、検察、裁判所等がサイバー犯罪に対して知見を蓄えることが有益であると考えます。この点、米国のNational Computer Forensic Instituteの活動が参考となります。また、人材面でも、官民の人材交流をさらに活性化することで、グローバルなサイバー犯罪に対応できる人材を育てていくことが肝要です。	御指摘のとおり、サイバー犯罪対策に関する制度の整備や人材の育成は重要と認識しており、5.2.1(3)や5.4.2(3)において、その旨を記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	10	BSA｜ザ・ソフトウェア・アライアンス	5.2.2(2)効果的かつ迅速な情報共有の実現	19	サイバー攻撃は、民間か政府機関かを問わず、また、国を超えてなされるため、情報共有に関する政策は、官民で又は民間企業・政府機関のそれぞれの間での情報共有を促進するものとすべきです。この観点から、政策決定者に対し、有効なサイバー脅威情報共有のために以下の6つの基本原則を推奨しています。 （ア）適切な目標を定めた政策を通じて、情報の共有及び受領に対する法律又は規制上の潜在的影響を明示的に限定することにより、民間機関が、国内及び海外において、サイバー脅威の指標に関する情報を他の民間機関又は政府と自発的に情報共有できる権限を付与すること （イ）サイバー脅威の指標を適時に共有することを妨げずに、サイバー脅威情報の共有により影響を受ける者のプライバシーを保護する適切な政策を策定すること （ウ）関連するサイバー脅威の情報を民間部門と共有する権限を政府機関に付与し促進すること、及び当該情報共有の期間を早めること（自動メカニズムによる場合を含む） （エ）民間機関による政府及び民間双方との間の情報共有を促進すること、共有される情報について義務づけられる契約上の条件を最小限にすること、並びに、影響を受ける当事者が適切な取引上の合意を締結できるような柔軟性を提供すること （オ）官民の情報共有のための民間のポータルを構築すること、及びこれらの情報共有に対する賠償保険が提供されるようにすること。 （カ）共有されたサイバー脅威の情報は、受領者によりサイバーセキュリティ促進にのみ用いられ、その他の目的に用いられず、及び、政府と情報を共有した場合にはその情報はサイバーセキュリティ促進又は限定された法の執行にのみ用いられることを保証すること	御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
13	11	BSA｜ザ・ソフトウェア・アライアンス	5.3 国際社会の平和・安定及び我が国の安全保障	24	サイバー空間がグローバルな空間であること、サイバー攻撃が容易に国境を越えて行われ得ることから、同盟国及び同様の立場に立ついわゆる有志国・機関との間の脅威情報の共有や人材育成等における協力・連携の積極的な推進が不可欠であり、また、その他の国とも信頼醸成を進めていくことが重要であるとの指摘につき賛同し、政府及び民間の双方のレベルで緊密な連携が進められるよう、確実な推進を望みます。	本案に賛同する御意見として承ります。
14	－	ファイア・アイ（株）	全般	－	【意見内容】 サイバー脅威に対して効果的な防御のために、基本的な基盤となる戦略的方針を構築するべきであり、この方針には、攻撃者の攻撃ライフサイクルを念頭に、シグネチャーに依存しないプロアクティブな方法をもってして、攻撃を検知し、防御する手法も含まれるべきです。 これらの新しい技術の導入と政府のセキュリティ防御の必要性の周知をすすめるために、担当職員、調達担当職員の皆様への研修や教育も含まれるようにしなければなりません。 この研修や教育には、高度なサイバー攻撃を行う攻撃者によって使用されるツール、戦術や手法に重点を置いて進化しているサイバー脅威を含める必要があります。 これは、担当職員の方が業務にあたる上で、最新の脅威状況に照らし合わせて、必要な決定事項を標準化することを可能とし、高度な攻撃者に対抗するセキュリティ対策をすすめます。 また、従来の調達手順に乗っ取らない、脅威の変化に対応できる新しいサイバーセキュリティ機能の、迅速かつ柔軟な取得を可能にする調達プロセスの確立もまた重要な課題であり支援するべきです。 高度なサイバー脅威から防御するための対策を導入することは、重要です。	御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、プロアクティブな対処の重要性については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）にも記載しているところであり、本戦略においては5.4.1(1)の「実態を踏まえた検知・防御能力の向上」の中で認識しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
15	－	（株）MESSA	全般	－	メール添付のファイルを開封する必要がある業務では、業務を行うクライアントを十分に管理する必要があると思います。GoogleのGMailなどでは、1つのアカウントに紐付けて数個のPOP3もしくはIMAPサーバーからメールを受信することが可能です。開封する必要があるファイル（Wordファイル、PDFファイルなど）はブラウザで見ることが可能です。クライアントのパソコン上にファイルをダウンロードしてから開く事よりリスクを軽減できるはずです。適応型の防御は必要だと思います。コストをかけないで、現状のシステムをリスクが少ない方向へシフトするのは大事だと思います。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
16	1	メリルリンチ日本証券（株）	5.1.2(1) 経営層の意識改革	11	経営層の意識改革については重要と考えるが、経営責任については法整備進めて経営に求める責任を明確にすることが望まれる。	御指摘の内容については、今後の施策の検討に当たっての参考とします。
16	2	メリルリンチ日本証券（株）	5.2.2(3) 各分野の個別事情への支援	20	各分野の個別事情への支援については期待したい。また、各分野リスクレベルにあったコントロール要件が設定することが望まれる。電気・ガスなどライフラインに係る業種のコントロール要件と、金融機関に求めるコントロール要件は相違するはず。	本案に賛同する御意見として承ります。なお、重要インフラの各分野における安全基準等は各分野におけるサービスの特性や社会環境等に応じて当然に異なるものであると考えます。
16	3	メリルリンチ日本証券（株）	6. 推進体制	37	情報共有について関係各所の連携強化を図ることは必要だが、障害原因のシステム名、ベンダー名など特有な情報に対しての情報共有について一定のルールを策定して運用することが大切と考える。 また、年金保険機構の問題などを考慮して、早期の限定的な情報共有のルール策定も必要。	情報の共有に当たっては、効果的な情報を迅速に共有していく必要があると認識しており、御指摘の内容については、今後の施策の検討に当たっての参考とします。
16	4	メリルリンチ日本証券（株）	－	－	事務所を独立した場所に設けるなど物理的な情報隔壁への対応も必要である。	御指摘の内容については、今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
17	－	個人（1）	全般	－	方針に経済性を意識して含めることも検討する必要があるのではないかと考えました。 ・サイバーセキュリティを公的な安全保障とするのであれば、公的サービスの提供と税の徴収を行いサイバースペースの治安維持に関する一定程度の責任を政府がもつことを明確にする ・この税の徴収を大規模なバグバウンティープログラムや民間企業との人材流動性向上（中途採用）にあてるなど競争性のあるモデルを政府主導で立案 ・日本独自の技術開発ではなく、米国からライセンス生産モデルなどを日本企業でもできるようサイバーセキュリティ製品にもあてはめて、日本企業による独自カスタマイズを日本企業が推進できるようにする ・IoTの安全は製品だけでなくバックエンドとAPIによるAPI経済圏支配が標準化のドミナントを起こすと推測される。よって単にセキュリティを組み込むだけでなく、相互接続プログラムのアジャイル化とAPIファーストの経済圏を日本スタンダードにすることを世界No1企業を有する日本の自動車業界等と連携して狙う ・上述のAPI経済のリードから得られるデータ基盤が次世代の競争力になる など、後手ではなく先手をとるなら経済的なモデルを成り立たせる意気込みを追加されるのがよいのではと思いました。	御指摘のとおり、サイバーセキュリティを考える上で、我が国の「経済社会の活力の向上及び持続的発展」も重要であると認識しており、5.1にその旨を掲げています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
18	－	個人（2）	5.1.1安全なIoTシステムの創出(2)IoTシステムのセキュリティに係る体系及び体制の整備,(3)IoTシステムのセキュリティに係る制度整備	9,10	IoTとして定義した各種機器は「今後」接続されるモノだけではなく、「すでに接続されている」モノが多数ある。 旧来のセキュアではないモノを安全な状態にするための解決策を開発することができれば新しいビジネスとして世界中に展開することも可能であり、産業育成の観点からも意義があると思われるので、慎重に対応する必要がある一方で、今後登場する新しい製品やサービスにおけるセキュリティ強度は一定の基準が必要であり、機能の更新を行うことのできる仕組みが必須であり、標準化と基準の制定とを常に対で提供する必要がある。 もし2020年により安全な環境を実現したいのであれば、速やかに開発および評価の基準とそれらを実現するための標準の策定を行い、事業者および個人を含め、一定のセキュリティを実現することのできないモノの販売や購入、利用の規制も視野に入れる必要があると思われる。 自由であることと、無秩序であることとは同義ではないので、運用と技術開発による新しいサイバーセキュリティの実現の検討をお願いいたします。	御指摘のIoTシステムのセキュリティに係る総合的なガイドラインや基準の整備については、5.1.1(3)において掲げています。具体的な施策については年次計画の中で記載します。 また、5.2.2(3)において、「制御系システム等の調達、運用には高度な専門性が必要とされることから、セキュリティ要件への適合を客観的に判断することが可能である国際標準に即した第三者認証制度の活用を進めていく。」と記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
19	1	個人（3）	5.1.1安全なIoTシステムの創出 (2)IoTシステムのセキュリティに係る体系及び体制の整備,(3)IoTシステムのセキュリティに係る制度整備	15	サイバー空間の中にも、実社会にあるような以下の観点が必要ではないか ・防犯 ・犯罪者の確保と訴追 ・流れてくる情報の遮断、情報の分析、発信元・有害情報の広がりの特定 ・犯罪発生時の機動的な対応、被害者保護 ・サイバー犯罪者予備軍の監視 現在は、民間人技術者が、国内外の犯罪者の軍隊に近い組織と戦っている現状です。 相手の攻撃手法が、想像を超える量で増えていますし、特定しきれないです。 技術は、オープンな技術を用いるのではなく、クローズドな技術にし、警察国防の技術のように扱い、犯罪者が抜け穴を見つけない施策が必要かと思います。 民間が、技術開発するとどうしても、情報が洩れます。	御指摘のとおり、サイバー空間における防犯、サイバー犯罪対策の強化は極めて重要であると考えています。このため、5.2.1(3)で、サイバー空間の脅威に関する実態把握のための情報収集の強化やサイバー犯罪に係る捜査能力の向上、取締り体制及び取締りのための情報技術解析体制の強化、人材育成や技術開発の着実な推進について記載しています。また、サイバー犯罪に対する事後追跡可能性を確保するため、通信履歴の保存の在り方について、関係事業者における適切な取組を推進することとしています。 また、クローズドな技術に関しては、5.4.1.(3)において、「また、安全保障の観点等から国として維持することが不可欠な技術もある。このため、公的研究機関や大学等の適切な研究機関において、研究開発を促す環境の整備を着実に進めていく。」と記載しています。
19	2	個人（3）	5.1.1安全なIoTシステムの創出 (2)IoTシステムのセキュリティに係る体系及び体制の整備,(3)IoTシステムのセキュリティに係る制度整備	15	以下の観点での監視も必要かと思います。 ・犯罪者予備軍、犯罪者及びその団体、利用者の保護観点での閲覧サイトの監視 ・流れてくるパケットの監視、犯罪者予備軍のシステムの監視 ・送金やクレジットカード決済のお金の流れの重点的な監視 サイバー交番の設置により、有害サイトの通知、被害の相談連絡ができるようにし、利用者の安心を担保する必要もあります。 サイバー空間でも、国民の生命財産を保護し、世界で一番治安のよい国を目指していただけることを切に望みます。	御指摘のとおり、悪意あるサイバー犯罪の実態を把握し、法令に従って適切に取り締まるとともに、サイバー空間において今後起こり得る新たな手口にも対処できるようにするため、犯罪対処能力・捜査能力の向上が不可欠であると認識しており、5.2.1(3)でその旨を記載しています。 また、利用者の安全・安心を担保するため、情報セキュリティ安心相談窓口や違法・有害サイトの届出窓口等で対応できる人材の育成を進めるべく、5.2.1(2)で、インターネット利用における悩みや不安に関する相談に応じられる人材を育成し、活動を促す取組についても、引き続き着実に推進することとしています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
20	1	個人（4）	5.4.2 人材の育成・確保 （1）高等教育段階や職業能力開発における社会ニーズに合った人材の育成	34	【意見内容】 「このため、大学院、大学、高等専門学校等の高等教育機関においては、サイバーセキュリティに係る理論・基礎の習得と演習を通じた実践力の強化が求められる。」は文章の趣旨が曖昧です。文章をより明確にすべきです。 【理由】 「実践力の強化が求められる」の主体は誰でしょうか？学生なのか、教職員・研究者なのか。それともカリキュラムや設備、セキュリティポリシといった体制なのか。それらの全てのことなのか。文意がよく理解できません。	御指摘のとおり本文の趣旨が分かりにくいことから、「実践力の強化が求められる。」を「実践力の強化に向けた取組を推進する。」に修文します。
20	2	個人（4）	5.4.2 人材の育成・確保 （3）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	35	【意見内容】 「また、例えばサイバー攻撃に対する対処法（防御手段、攻撃方法も含む）の研究を通じ、自ら考え、対策を検討できる能力の育成を推進する。」の後に、例えば、「育成する人材には、能力を発揮するにあたってプロフェッショナルとしての中立性を維持し、公益に反する欺瞞的な行動を自制できるだけの高い倫理観を付与する」といった文章を追加する。 【理由】 「5.4.2 人材の育成・確保」の節のどこにも「高い倫理観の醸成」が触れられないのは看過できません。「グローバルに活躍できる人材」の育成を目指すなら、育成した人材が「Code of Ethics」を遵守することは必須です（日本はここが特に弱い）。さもなければ、以前に発生した研究不正と同じような状況が発生し、サイバーセキュリティの分野においても国際的な信用を失うことになります。また、人材が公正な視点を失えば、例えば、「世界に通用する技術・ポリシ」ではなく、「自分や自組織に都合の良い技術・ポリシ」が採用され、結果として国内の技術・セキュリティ水準、更には国際競争力が低下する原因となります。	御指摘を踏まえ、5.4.2柱書の最後に「なお、こうした人材においては、技術的な能力のみならず、高い倫理観も同時に身に着ける必要がある。」と追記します。 なお、初等中等教育段階から児童の発達段階に応じて情報セキュリティを含む情報モラルの理解を促すこととしており、5.4.2(2)で「初等中等教育段階から、児童生徒の発達段階に応じて、情報活用の実践力、情報の科学的な理解、情報社会に参画する態度を培う教育を一層推進し、情報セキュリティを含む情報モラルの理解等を促し、論理的思考力や情報通信技術、機器の基本的な仕組み等についての理解を促すようなものとなるよう取り組む。」と記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
21	－	個人（5）	5.4.1（3）サイバーセキュリティのコア技術の保持	33	【意見内容】 「研究開発を促す環境の整備を着実に進めていく。」に以下を追記、修文。 「研究開発を促す環境の整備を着実に進めていくとともに、その研究成果を国や公的研究機関が積極的に活用することによってセキュリティ産業育成のための初期マーケットを創造することが必要である。」 【理由】 国家プロジェクトの研究成果を産業化するためには、新しいものを積極的に活用して初期マーケットを創出することが重要である。セキュリティは国防と同じで、国は率先してその市場を作り出すべきである。	研究成果の産業化等の社会還元の推進は重要と考えます。そのため、5.4.1(1)で「サイバーセキュリティの研究開発は社会的なニーズを踏まえ実用化されることが重要であり、研究成果の社会還元の推進が重要である。」と記載するとともに、関係者間での必要となる情報・データの共有に向けた取組を推進することとしており、原案のとおりとします。 また、5.1.3(1)において「サイバーセキュリティ関連産業の振興」として「研究開発成果を活用したベンチャー企業の育成」等に取り組むこととしています。
22	－	個人（6）	5.2.3 政府機関を守るための取組	21-23	政府機関又は政府機関から委任・委託を受け業務を行う特殊法人は、監査法人による金融監査と同様に、セキュリティ監査を行うように義務づけるようにお願い致します。	御意見を踏まえ、5.2.3に「(4)」として、以下のとおり追加いたします。 (4) 監視対象の拡大等による総合的な対策強化 政府機関全体としてのサイバーセキュリティを強化するため、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等における対策の総合的な強化を図る。 具体的には、当該法人におけるインシデント対処能力の向上や所管省庁による当該法人への監査の強化等を図るほか、当該法人におけるサイバーセキュリティに関する取組について、法人の特性等を踏まえつつ、政府機関の取組（上記(1)から(3)まで）に準じて推進する。とりわけ、当該法人について、公平な受益者の負担に留意しつつ段階的にGSOCの監視対象に追加するほか、サイバーセキュリティ戦略本部がNISCに実施させる監査及び原因究明調査の対象とする等の施策を推進する。また、本対策強化に際しては、専門的知見を有する関係法人との連携体制の整備を図ることを含め、所要の法改正について速やかに検討を行い、必要に応じて措置する。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
23	1	個人（7）	5.1.1 安全なIoTシステムの創出 (1)安全なIoTシステムの創出	9	【意見内容】 「このため、システムの企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。」の後に以下を追記する。 「製品設計においては、ハードウェア機能とソフトウェア機能およびそれらの協調によるセキュリティ性能を重視する。」を追記する。 【理由】 セキュリティ・バイ・デザインの具現には、製品のセキュリティ性能を付加価値として市場が認める必要があるため。	御指摘の製品のセキュリティ性能を付加価値として市場が認めることについては、5.1.2(3)に、企業における製品・サービスの関係者がセキュリティ・バイ・デザインを共通の価値として認識することを促していく旨を記載しており、この中に御指摘の考え方も含まれているものと考えることから、原案のとおりとします。
23	2	個人（7）	5.1.1 安全なIoTシステムの創出 (4)IoTシステムのセキュリティに係る技術開発・実証	11	【意見内容】 「このため、テスト環境の構築や、システム全体の脅威分析・リスク評価手法の開発、ICチップを含むハードウェアの真正性の検証等、」に追記し、以下のとおり修文する。 「このため、テスト環境の構築や、システム全体の脅威分析・リスク評価手法の開発、ICチップを含むハードウェアの真正性の検証やセキュリティ性能の定量評価等、」 【理由】 ハードウェアセキュリティを担うICチップについて、真正性の検証のみならず、そのセキュリティ性能を定量的に評価する手法も技術開発が必要であるため。	御指摘のセキュリティ性能の定量評価につきましては、5.1.1(4)の「ICチップを含むハードウェアの真正性の検証等」に含まれる内容であると考えており、原案のとおりとします。
23	3	個人（7）	5.1.3 セキュリティに係るビジネス環境の整備	14	【意見内容】 脚注8「機器やシステムの設計・製造・調達・設置・運用段階におけるリスクであって、これらの段階においてウィルスを含む悪意のあるプログラムを埋め込まれるなどのリスクを含む。」に追記し、以下のとおり修文する。 「ICチップおよびその応用機器やシステムの設計・製造・調達・設置・運用段階におけるリスクであって、これらの段階においてウィルスを含む悪意のあるプログラムを埋め込まれるなどのリスクを含む。」 【理由】 米国・欧州ではセキュリティ機能を有するICチップの改竄が潜在的リスクとして既に社会課題となっているため。	御指摘を踏まえ、脚注8の「機器」を、「機器（ICチップを含む。）」に修文します。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
23	4	個人（7）	5.3.2 国際社会の平和・安定 (5)国際的な人材育成	29	【意見内容】 「このため、このような人材には、サイバーセキュリティに関する十分な知識とともに、各国の社会・経済・文化等の状況についての理解も求められる。」に追記し、以下のとおり修文する。 「このため、このような人材には、サイバーセキュリティおよびハードウェアセキュリティに関する十分な知識とともに、各国の社会・経済・文化等の状況についての理解も求められる。」 【理由】 国際的な人材育成においては、サイバーセキュリティはもちろん、セキュリティ機能を有するICチップとその応用制御機器等のハードウェアについても十分に理解している人材が必要であるため。	御指摘のハードウェアのセキュリティに関する知識は、サイバーセキュリティに関する知識に含まれると考えており、原案のとおりとします。
23	5	個人（7）	5.4.1 研究開発の推進 (3)サイバーセキュリティのコア技術の保持	33	【意見内容】 「特に、コア技術を育む基礎研究については、暗号研究のように、直ちにビジネスにつながらないものの、経営力、事業開発力のある者との連携により、新たな産業創出の種となるものであり、また、安全保障の観点等から国として維持することが不可欠な技術もある。」の後に以下を追記する。 「国際的な市場競争力の高いセキュリティ機能・性能を具体化するハードウェアセキュリティ技術の研究も極めて重要である。」 【理由】 サイバーセキュリティ技術の研究開発において、わが国が国際的に先導的な立場にあるために、通信ネットワークなどの基本機能を担う日本製ハードウェアにおけるセキュリティ性能を十分に高め、国際市場に広く流通する必要があるため。	御指摘を踏まえ、5.4.1において以下のとおり修文します。 「さらに、サイバー攻撃は日々進化し高度化・複雑化しており、その変化に対処していくため、ネットワーク、ハードウェア、ソフトウェア等の幅広い分野において、創意と工夫に満ちたサイバーセキュリティ技術を生み出すための充実した研究開発の推進が不可欠である。」

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
24	－	個人（8）	－	－	マイナンバー制度ネットワーク構築について。もっとも重要なことは、セキュリティ対策です。導入時初期にあっては「送受信分離・人介在システム」としてください。 私の意見は、新規なものではなく、たとえば学校では「成績」「給与」「汎用」のように、はっきり独立のLANが構築されていました。また成績LANは昔はフロッピーディスクで教員から提出される形式でした。最近はすべてネットで、処理するところに、運用上の不備が生じています。なぜ不備が発生するかといいますと、この20年間を振り返っても、コンピュータの性能が、ハード・ソフト両面で1000倍以上向上したからです。 私は、今後も、この技術革新は続くと思います（専用化・並列化・物性的・材料・製造技術など）。したがって、私が述べた、一見、陳腐な意見でも、担当者、責任者、利用者に、簡単、明確、明瞭に、その運用の要点を説明・納得できるようにしておくべきだと思います。その延長上に、さらなる自動化があると思います。	御指摘のとおり、マイナンバー制度におけるセキュリティの確保が重要であると認識しており、5.2.2(3)において以下のとおり修文します。 「マイナンバー法における個人番号利用事務において使用するシステムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を含めて検討の上、必要な措置を講ずるとともに、関係機関が連携し専門的・技術的知見を有する監視・監督体制を整備する。」
25	1	個人（9）	２．２　サイバー空間における脅威の深刻化	2	【意見内容】 サイバー脅威の認識として、論理攻撃が中心でネットワーク阻止攻撃としての電磁パルス(ElectroMagnetic Pulse: EMP)脅威が挙げられていないため、次の記述を追加されたい。「さらに、サイバー空間に巨大な脅威を及ぼす蓋然性の高いEMP脅威としては、①人工的EMP攻撃、特に小型の超EMP核兵器を用いた高々度電磁パルスによる電力網および電子機器の破壊、並びに②太陽活動がもたらす巨大な磁気嵐による電力網の破壊がある。」 【理由】 EMP脅威について、国家指導者が十分に認識し、政府機関および電力網を中心とした重要インフラのシステム防護のための態勢を優先的に整備する必要がある。	御指摘のEMP（電磁パルス）による脅威については認識しておりますが、当該箇所については、脅威を網羅的に挙げることとしていないため、原案のとおりとします。 なお、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.27 6.(1)①にEMP（電磁パルス）による脅威について記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	2	個人（9）	3. 目的（3）戦略において目指す日本の姿	4	【意見内容】 「実空間と融合したサイバー空間を活用していくためには、利便性の裏に潜む脅威に的確に対処できることが必要不可欠であり、高付加価値を創出するための「投資」が必要となる。」を以下のとおり修文する。 「実空間と融合したサイバー空間を活用していくためには、利便性の裏に潜む脅威に的確に対処できることが必要不可欠であり、高付加価値を創出するための「セキュリティ投資」が必要となる。」 【理由】 「投資」の意味がわかりにくい。	御指摘の箇所については、一般概念としての「投資」を記載していることから、原案のとおりとします。なお、セキュリティに関する投資の考え方については5.1に記載しています。
25	3	個人（9）	５．１．１（１）安全なIoTシステムを活用した新規事業の振興 ５．１．１（４）IoT システムのセキュリティに係る技術開発・実証	9,10	【意見内容】 情報システムよりも高い品質をIoTシステムに要求する場合、数学的に脆弱でないことを保証できる革新的なソフトウェア構築技術によりOS、通信プロトコル、アプリケーション等のソフトウェアをゼロから開発すべきである。米国のDARPAは、脆弱性のない高い保証された組み込みシステム構築技術開発のためのHigh Assurance Cyber Military System(HACMS)プログラムを産官学で推進している。 【理由】 情報システムでは、セキュリティ・バイ・デザインによる脆弱性の低減は普通の考え方であるが、この考え方を導入しても統計的品質管理の基づくソフトウェア開発方法である限り脆弱性をゼロにすることはできない。ソフトウェアの脆弱性をゼロにするためには、従来のソフトウェア構築技術と異なる革新的なソフトウェア構築技術を開発する必要がある。	5.1.1(4)において、「IoTシステムの構成要素の特徴を加味した情報通信技術の開発・実証事業を行う。」と記載しており、御指摘の内容については、今後の施策の検討に当たっての参考とします。 なお、脆弱性を作りこまないためのソフトウェア開発技術の必要性については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.32 6.(2)の「⑦ソフトウェアの安全性確保」に記載しています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	4	個人（9）	5．2　国民が安全で安心して暮らせる社会の実現	15	【意見内容】 「リスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し総合的な判断を受ける機能保証（任務保証）の取組が必要である。」の後に、以下のとおりサイバー空間に巨大な影響を及ぼす蓋然性の高い人工的EMP脅威に関する記述を追加する。 「さらに、サイバー空間に巨大な影響を及ぼす人工的EMP脅威に対応するために、政府機関および電力網を中心とした重要インフラの具体的な防護の取組が必要である。」 【理由】 EMP脅威について、国家指導者が十分に認識し、政府機関および電力網を中心とした重要インフラのシステム防護のための態勢を優先的に整備する必要がある。	御指摘のEMP（電磁パルス）による脅威については認識しておりますが、当該箇所については、脅威を網羅的に挙げることとしていないため、原案のとおりとします。 なお、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.27 6.(1)①にEMP（電磁パルス）による脅威について記載しています。
25	5	個人（9）	5．2．3（1）ii. 被害の発生・拡大の防止	22	【意見内容】 「政府機関横断的な監視・即応機能及び各機関における事態の把握・対処機能の強化に取り組むとともに、」を以下のとおり修文する。 「迅速なセキュリティリスク管理を行うために各機関における情報システムのセキュリティ状態（脅威、情報資産の脆弱性およびセキュリティ設定の脆弱性）の常時監視および任務保証のリスク評価／可視化並びに政府機関横断的なリスク評価／可視化に取り組むとともに、」 【理由】 APT攻撃は、作文的な対策では対応できないため実効性のある対策を導入すべきである。今回の社会保険機構のようなAPT攻撃事案発生時に政府機関トップの適時および適切な状況認識と判断支援をするためにリアルタイムなセキュリティリスク管理の仕組みを政府機関および関連機関が導入すべきである。そうしなければ、情報セキュリティ予算は国家予算の無駄遣いになる。	ご指摘の内容については、5.2.3(1) ii .の「GSOCによる政府機関全体における検知・解析機能の強化、並びに各機関におけるインシデント対応を行うチーム（CSIRT）の体制及び事態の把握・対処機能の強化、インシデント発生時の情報提供の迅速化・高度化に取り組む」、5.2.3(2)の「リスク評価に基づく組織的な情報システムの対策・管理の推進」、6.の「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高度な情報分析・集約・共有機能を有する体制を整備する」に含まれていると考えています。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	6	個人（9）	5.3.1 我が国の安全の確保	25	【意見内容】 「こうした認識を多様な関係主体間で共有した上で、これまでの連携を一層強固にし、切れ目のない重層的・多層的な防護を実現する。」を以下のとおり修文する。 「こうした認識を多様な関係主体間で共有した上で、これまでの連携を一層強固にし、各主体がリアルタイムのセキュリティリスク管理ができる態勢を実現する。」 【理由】 国家を主体としたゼロデイ脆弱性を用いたAPT攻撃に対して、現状の防御技術による政府や重要インフラ等が有している社会システムに重層的・多層的な防護を行っても完全な防護は不可能である。したがって、現状の防御技術を前提とした場合、サイバー攻撃に対してリアルタイムのセキュリティリスク管理のできるセキュリティ常時監視および任務保証のリスク評価／可視化が必要である。	御指摘の内容については、5.3.1において、「様々な主体によるサイバー攻撃の兆候を含む状況を早期に認識・把握し、問題点を検知して対応する能力の一層の向上を図っていく」と記載しておりますが、ご指摘を踏まえ、以下の通り修文します。 「様々な主体によるサイバー攻撃の兆候を含む状況を早期に認識・把握し、問題点を検知して迅速に対応する能力の一層の向上を図っていく」
25	7	個人（9）	5．3．1（3）政府機関・社会システムの防護	26	【意見内容】 「防衛当局である防衛省・自衛隊においては、自らが保有するネットワーク・インフラの防護を引き続き強化するとともに、上記の社会システムに対するサイバー攻撃も、任務遂行上の大きな阻害要因となる可能性を踏まえ、自衛隊の任務保証に関連する主体と連携を深化させていく。」を以下のとおり修文する。 「防衛当局である防衛省・自衛隊においては、自らが保有するネットワーク・インフラのリアルタイムなセキュリティリスク管理態勢を整備するとともに、上記の社会システムに対するサイバー攻撃も、任務遂行上の大きな阻害要因となる可能性を踏まえ、自衛隊の任務保証に関連する主体にもセキュリティリスク管理態勢を義務づける調達制度に深化させる。」 【理由】 APT攻撃は、作文的な対策では対応できないため実効性のある対策を導入すべきである。今回の社会保険機構のようなAPT攻撃事案発生時に政府機関トップの適時および適切な状況認識と判断支援をするためにリアルタイムなセキュリティリスク管理の仕組みを政府機関および関連機関が導入すべきである。そうしなければ、情報セキュリティ予算は国家予算の無駄遣いになる。	防衛省・自衛隊のネットワークは現在24時間体制で実施しており、リアルタイムでのセキュリティ監視体制を敷いています。 また、自衛隊の任務保証に関連する主体とは、御意見も踏まえ、連携を深化させていきます。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
25	8	個人（9）	5．4．1（1）サイバー攻撃の検知・防御能力の向上	32	【意見内容】 「また、政府が推進する研究開発プロジェクトにおいて、研究開発の企画段階からサイバーセキュリティを組み込むなど、防御能力の向上を進める。」を以下のとおり修文する。 「また、政府が推進する研究開発プロジェクトとして、脆弱性のないソフトウェア構築技術開発に取り組むなど、防御能力の革新的向上を進める。」 【理由】 国家を主体としたゼロデイ脆弱性を用いたAPT攻撃に対する防御能力の向上には、サイバー攻撃に対する強靭性向上と脆弱性のないソフトウェア構築技術の開発の2つのアプローチがある。前者については、本戦略案においても挙げられているが、後者については挙げられていない。攻撃者優位のサイバー空間の状況を変えるためには、政府の推進する研究プロジェクとして、APT攻撃を不可能にする革新技術としての「脆弱性のないソフトウェア構築技術開発」に取り組むべきである。特に、無人機、自動走行自動車、ロボット等の人命に係わるIoTシステムのソフトウェア開発には必須である。米国のDARPAは、脆弱性のない高い保証された組み込みシステム構築技術開発のためのHigh Assurance Cyber Military System(HACMS)プログラムを産官学で推進している。	御指摘の内容は、研究開発プロジェクトにシステムの企画・設計段階からセキュリティの確保を盛り込むことの重要性を述べているものであり、趣旨が異なること、またソフトウェアの脆弱性に関する課題に限らないことから、原案のとおりとします。 なお、脆弱性を作りこまないためのソフトウェア開発技術の必要性については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）P.32 6.(2)の⑦ソフトウェアの安全性確保に記載しています。
26	1	個人（10）	全般	－	【意見内容】 一昨年策定された現戦略においては、特定省及びその所管法人色の濃さを感じさせ、各省の関連白書の一部抜粋と見まがう部分も散見されたが、今回の戦略では、各省間でのバランスが取れ、かつ相互に整合し総合された内容になっており、全省庁的な取組を示す戦略になっている。法的根拠（サイバーセキュリティ基本法）に基づくNISC殿のリーダーシップに拠るものと理解する。 【理由】 本文全般をサーベイしての率直な感想である。	本案に賛同する御意見として承ります。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
26	2	個人（10）	5.2.1(3)サイバー犯罪への対策	17,18	【意見内容】 サイバー犯罪に係る現状及び見通しを踏まえた、現行法制の必要十分性の検証による現法令の見直し・強化、要すれば新たな法制度の整備を行うことを明確に謳うべきと考える。 【理由】 原案では、「法令に従って適切に取り締まる」こと、「犯罪対処能力・捜査能力の向上」が不可欠としているが、新たな法整備どころか、現法令の見直し・強化にすら踏み込んでいないように見える。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、その施策の実現に当たり必要がある場合には、法制度の整備等についても検討します。
26	3	個人（10）	5.2.2(2)効果的かつ迅速な情報共有の実現	19,20	【意見内容】 「情報源の秘匿」や「共有範囲の設定など適切な加工を行う」だけでは真に有意な情報の収集は困難であることから、現実的な対応としては、カルテル等におけるリニエンシー制度並みとは行かないまでも、有意な（提供主体にとっては不利な）情報を提供した場合の提供者への具体的なインセンティブを提示し、法的に担保すべき（その旨を記載すべき）である。 【理由】 真に有意な情報（提供側にとっては不利な情報）を民間企業等の側から本気で得ようとする場合、民間企業等にとって具体的かつ法的に担保されたメリットが必要である。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、その施策の実現に当たり必要がある場合には、法的な担保等についても検討します。
27	1	個人（11）	「5.1.2(3) 組織能力の向上」 「5.2.2重要インフラを守るための取組」	12,18	セキュリティ要件への適合を国際標準に即した第三者認証制度の活用を進める場合、CC（Common Criteria）、JCMVPといった既存の第三者評価制度も、積極的に活用することを明記していただきたい。例えば、IoTのPP（Protection Profile）を作成することで、既存のCC評価フレームワークを活用することができると考えます。	本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、第三者認証制度の活用の際には、当然のことながら、国際標準や既存の制度の活用も踏まえたものとします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
27	2	個人（１１）	「5.2.3(1)i インシデントの未然防止」	22	送信ドメイン認証（DKIM等）や暗号技術を利用したS/MIME等の対策を積極的に推進していただきたい。	御指摘の内容については、従来から取り組んでいるところであり、今後も引き続き推進していきます。
27	3	個人（１１）	「5.1.1(4) IoTシステムのセキュリティに係る技術開発・実証」 「5.4.1(3)サイバーセキュリティのコア技術の保持」	10	安全なIoTシステム」を計測する「安全性評価技術」の研究開発や評価体制の強化を継続的に推進していただきたい。例えば、暗号技術であれば、直ちにビジネスにつながらない「安全性評価技術=解読技術」の研究開発に対する支援や客観的に安全性を評価する体制（CRYPTREC）を維持していただきたい。	御指摘の内容に関し、5.4.1(3)において、「コア技術を育む基礎研究については、暗号研究のように、直ちにビジネスにつながらないものの、経営力、事業開発力のある者との連携により、新たな産業創出の種となるものであり、また、安全保障の観点等から国として維持することが不可欠な技術もある。このため、公的研究機関や大学等の適切な研究機関において、研究開発を促す環境の整備を着実に進めていく」としています。 また、暗号化技術の安全性評価体制（CRYPTREC）の維持については、「情報セキュリティ研究開発戦略（改定版）」（2014年7月 情報セキュリティ政策会議決定）の6⑫暗号技術　などで記載しており、引き続き推進することとしています。
27	4	個人（１１）	「5.2.1(2)サイバー空間利用者の取組の促進」	16	本サイバーセキュリティ戦略を推進する上で、サイバー空間における民間事業者・団体や、地方公共団体、公的機関の自らを特定するための基本情報（WebサイトのURL、英字名称など）に対して、国民がいつでもアクセス可能な情報基盤の整備を進めていただきたい。 そのため、5.2.1(2)に、「また、民間事業者・団体や、地方公共団体、公的機関が、自らWebサイトアドレス、法人番号等の基本的な情報を国民に提供可能とする基盤の整備を推進する。」と追加していただくことを提案します。	御指摘の内容については、普及啓発などの今後の施策の検討に当たっての参考とします。

番号	枝番号	提出者	該当箇所	ページ数	概要	御意見に対する考え方及び修正
27	5	個人（１１）	「6. 推進体制」について	37	サイバーセキュリティ戦略本部の位置付け・役割を明確に位置付けていただきたい。 分野ISACやC-CERT、JPCERT/CC、警察・防衛省を含めたインシデント情報の共有体制も明示していただきたい。	御指摘のサイバーセキュリティ戦略本部の位置付けや役割については、サイバーセキュリティ基本法（平成26年法律第104号）に定められています。 また、本戦略は、今後3年程度の基本的な施策の方向性を示すものであり、個別の組織や団体の役割や関係性を記載するものではないため、原案のとおりとします。