「今後のサイバーセキュリティ政策の在り方に関する提言」への対応状況

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
1.セキュリティ確保を起点とする産業創出の実現			
1-1	IoTセキュリティの強化に向けた投資促進支援	5.1.1(1)	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。
1-2	IoTセキュリティの確保に必要な国際標準化等に係る産学官連携による積極的貢献	5.1.3(3)	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
1-3	制御システムの国際標準等に基づく認証の推進	5.1.3(3) 5.2.2(3)	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 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。
2.サイバー脅威への対処能力の強化			
2-1	企業におけるサイバーセキュリティ人材育成に係る税制等による財務上の支援	5.4.1(4)	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。

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
2-2	中小企業を対象としたセキュリティ投資等の支援	5.1.2(1)	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。
		5.1.3(1)	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。
		5.1.3(1)	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。
2-3	セキュリティ対策が市場において評価されるための情報開示の在り方やセキュリティに係る監査制度の普及に向けた検討	5.1.2(1)	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。
		5.1.3(1)	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。

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
2-4	サイバー脅威への対処能力の強化に向けた情報共有や実践的な演習に係る環境整備の加速化	5.1.2(3)	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(2)	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。
		5.2.2(2)	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。
		5.2.2(2)	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。
		5.4.2(1)	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。
		5.4.2(5)	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。
2-5	若年層、高齢者等を対象とした普及啓発活動を産学官民で連携して行う仕組みの強化	5.2.1(2)	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。

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
3.グローバルパートナーシップの強化			
3-1	二国間及び多国間のサイバー協議を通じた信頼醸成やサイバー空間における国際秩序の形成への積極的貢献	5.3.2(1) 5.3.2(2)	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。 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。
3-2	各国におけるサイバー分野の能力構築支援	5.3.2(4)	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。
3-3	サイバー空間における国際テロ組織の活動に関する情報の収集・分析能力の向上	5.3.2(3)	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.セキュリティ人材の育成強化			
4-1	セキュリティ人材育成に向けた企業や大学等との間における緊密連携による取り組みに対する政策支援	5.4.2(1) 5.4.2(4)	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。 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、事業の性質や受け入れ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。
4-2	大学等教育機関における実践的演習に係る教材の共同開発やクラウドサービスによる提供への支援(サイバーナショナル訓練センターの設立を視野)	5.4.2(1)	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。 (中略) 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。

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
4-3	極めて深刻なサイバー事案が発生した場合に企業の専門家が集結するサイバーディフェンスリーグの創設	5.4.2(5) 6.	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。 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(中略)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。
4-4	初等教育におけるプログラミング教育の導入(論理的思考の涵養)	5.4.2(2)	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。 (中略) 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。
4-5	高等専門学校等における実践的なセキュリティ教育の強化	5.4.2(1)	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。
4-6	サイバーセキュリティ人材に対する奨学金制度の活用	5.4.2(1)	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。
4-7	サイバーセキュリティに係る専門知識に加え法律や経営学などの知見も兼ね備えたハイブリッド人材の育成	5.4.2(1)	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。
4-8	セキュリティコンテスト等を通じた突出人材の発掘・育成	5.4.2(3)	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。 (中略) 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。

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
4-9	サイバーセキュリティ人材のネットワークの形成	5.4.2(3)	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。
4-10	実践的な能力を客観的かつ継続的に保証できる資格制度の導入	5.4.2(4)	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。
5.セキュリティ研究開発力の強化			
5-1	国が推進するIT研究開発プロジェクトにおいてセキュリティ確保を必須要件とする	5.4.1(1)	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。
5-2	サイバーセキュリティ関連の研究開発予算の十分な確保	5.4.1	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。
5-3	有志国との国際共同研究の推進	5.4.1(4)	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。
5-4	ベンチャー企業等の研究開発・国際展開支援	5.1.3(1) 5.1.3(3)	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。 「我が国企業の国際展開のための環境整備」全般で記載。
5-5	IoTセキュリティ技術、IT利活用の推進により更なる成長や効率化が期待される医療健康、農業、行政、エネルギー等の分野に有用なセキュリティ技術、暗号技術等の研究開発に重点を置く	5.1.1(3) 5.1.1(4) 5.4.1(3)	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。 「IoTシステムのセキュリティに係る技術開発・実証」全般で記載 「サイバーセキュリティのコア技術の保持」 全般で記載

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
5-6	サイバー空間における攻撃予兆分析、対処法（防御手法、攻撃手法も含む。）の研究及び自動対処、可視化等の技術開発支援、サプライチェーンリスクを排除するための技術開発を国として自立的に行う体制の整備等を推進するとともに、その成果について政府において積極的な導入を図ること	5.1.3（3） 5.4.1（1）	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。 「サイバー攻撃の検知・防御能力の向上」全般で記載
5-7	経済学、心理学等を含む学際的な融合研究領域に対する支援を拡充	5.4.1（2）	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。
6.オリンピック・パラリンピック東京大会におけるサイバーセキュリティ対策の強化			
6-1	オリンピックCSIRT（Cyber Security Incident Response Team）の整備に向けた検討の加速化	6.	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。
6-2	オリンピックを支える重要インフラ防御のための情報共有体制の強化	5.2.2（2） 6.	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。 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。

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
6-3	実際の大会を想定した演習の実施	6.	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、 （中略） 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。
7.政府における体制強化			
7-1	オープンソースインテリジェンスを含む国内外の動向に関する情報収集・情勢分析のための機能強化	6.	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。
7-2	GSOC（Government Security Operation Coordination team）システムの抜本的強化	5.2.3（1）ii	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
		6.	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。
7-3	一層の人材確保	5.2.3（2）	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。
		6.	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 （中略） 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。

提言事項		戦略に記載した内容	
項番	内容	項番	該当箇所
7-4	政府におけるセキュリティ予算の十分な確保	6. 7.	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。 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。
7-5	処遇等の改善を図るなど従来の枠組みに囚われない制度整備	6.	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。
7-6	マイナンバー制度に係るセキュリティ確保は政府全体に関わる重要かつ喫緊の課題であることから、内閣官房を中心に関係府省の連携強化	5.2 5.2.2(3)	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。 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。

提言事項			戦略に記載した内容	
	項番	内容	項番	該当箇所
	7-7	マイナンバーを介した官民の認証連携の実現に向けた標準化等の環境整備	5.2.2(3)	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。
	7-8	サイバー犯罪対策を効果的に進めるための新たな手法の導入	5.2.1(3)	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。
	7-9	調査・分析を目的とするアクセス行為やリバースエンジニアリングを特例的に認めることとする等の制度の見直し	5.1.3(1)	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 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。