平成２７年４月１６日
自由民主党政務調査会
ＩＴ戦略特命委員会

# 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

サイバー空間における脅威の深刻化、拡散、グローバル化が急速に進展する中、本年１月、世界に先駆けてサイバーセキュリティ基本法が全面施行され、サイバーセキュリティ戦略本部及びその事務局である内閣サイバーセキュリティセンター（ＮＩＳＣ）が新たに発足し、政府のセキュリティ政策の司令塔機能が強化された。

サイバーセキュリティの確保は、社会経済システムを健全に機能させ、国民に安全かつ豊かな日常生活をもたらすだけなく、経済の好循環に寄与し、持続的な経済成長の実現に不可欠である。

このような理念の下、政府は本年夏頃を目途に新たなサイバーセキュリティ戦略を決定すべく検討を重ねている。そこで、ＩＴ戦略特命委員会として今後のサイバーセキュリティ政策の在り方について以下のとおり提言する。

## １　セキュリティ確保を起点とする産業創出の実現

インターネット前提社会が到来し、モノのインターネット（ＩｏＴ：Internet of Things）が今後急速に普及し、リアル空間とサイバー空間の一体化と情報資源の活用が急速に進展するものと見込まれる。

ＩｏＴの進展は社会経済システムの深層に至るまでＩＴが浸透することとなるため、セキュリティ確保が一層重要な課題となる。

ＩｏＴセキュリティの確保は日本発のＩｏＴシステムはもとより、広く我が国の産業競争力の強化につながるものであることから、政府としてＩｏＴセキュリティの確保を起点とした産業創出の実現に向け、具体的な政策効果を関係者間で共有しつつ、ＩｏＴセキュリティの強化に向けた投資促進支援、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のほか、制御システムの国際標準等に基づく認証等を推進すべきである。

## ２　サイバー脅威への対処能力の強化

事故前提社会における企業のサイバー脅威への対応は、企業の保有する知的財産や顧客情報の保護など企業経営の中核に関わる重要事項であるが、企業経営層におけるサイバー脅威への認識は十分ではない。

このため、セキュリティ対策は「費用」でなく「投資」であるとの認識の下、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、資金や人手不足に悩む中小企業を対象としたセキュリティ投資等の支援、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、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等を推進すべきである。

また、一般のネット利用者のうち若年層、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が必要である。

## ３　グローバルパートナーシップの強化

サイバー脅威への対応はもはや一国でできるものではなく、日本にとって最も重要な同盟国である米国の他、有志国との緊密な連携を更に強化していく必要がある。これはサイバー空間における国家安全保障、テロ対策等の観点からも極めて重要である。

このため、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、各国におけるサイバー分野の能力構築支援、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・分析能力の向上等に努める必要がある。

## ４　セキュリティ人材の育成強化

我が国におけるセキュリティ人材は量的・質的に圧倒的に不足しており、セキュリティ人材の育成強化は喫緊の課題である。そこで、産学官の連携の下、セキュリティ人材の育成強化に努めることが強く求められる。

このため、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、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）、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等を検討する必要がある。

また、初等中等教育の段階から人材育成を図るため、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）、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、サイバーセキュリティ人材に対する奨学金制度の活用、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、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、サイバーセキュリティ人材のネットワークの形成等を推進すべきである。

さらに、人材のキャリアパスを描きやすくし、セキュリティ人材の有効活用を促進するため、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を検討すべきである。

## ５　セキュリティ研究開発力の強化

サイバーセキュリティ確保のためには優れた技術が基盤となる。また、政府の国家安全保障戦略にも記載されているように、安全保障の視点から、サイバーセキュリティ等の技術開発関連情報等、科学技術に関する動向を平素から把握し、産学官の力を結集させて、安全保障分野においても有効に活用するように努めていくことが求められる。

しかし、我が国の研究開発予算は米国に比べて１２分の１にとどまる（対ＧＤＰ比）など、十分な予算が措置されているとは言えない状況にある。

このため、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他、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を図るとともに、有志国との国際共同研究の推進、ベンチャー企業等の研究開発・国際展開支援等を推進すべきである。とりわけ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など、メリハリの効いた研究開発力の強化を図るべきである。また、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が必要である。

さらに、セキュリティ関連技術の研究開発において、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する。

## 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ィリティ対策の強化

２０２０年夏に開催されるオリンピック・パラリンピック東京大会の成功に向け、サイバーセキュリティ対策は最重要課題の一つである。2012 年のロンドン大会では、英

国政府において６年前からセキュリティ対策を行っていたところであり、我が国においても早急に取組む必要がある。

このため、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、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、実際の大会を想定した演習の実施等を推進すべきである。また、上記１～５の取り組みの成果を東京大会に最大限投入することで、我が国のセキュリティ対策強化のレガシーとして活用することが求められる。

## ７　政府における体制強化

今般のＮＩＳＣの機能強化を実効あるものとするには、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、ＧＳＯＣ（Government Security Operation Coordination team）システムの抜本的強化、一層の人材確保等が急務である。このため、政府におけるセキュリティ予算の十分な確保を大胆かつ柔軟に図る必要がある。とりわけ、サイバーセキュリティにかかる人材の登用や活用を促すため、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に取組むなど、引き続き政府における体制強化に向けた不断の見直しを図るべきである。

また、２０１６年から稼働する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等を図るほか、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を推進する必要がある。

さらに、高度化が進むサイバー攻撃に対処するためには、既存の枠組みでは限界があり、また実効性のある国際的な協調を確保することも困難な状況にある。政府は、サイバー攻撃への対処能力を強化する観点から、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、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等について、関係府省の連携の下、早急かつ具体的に検討を開始すべきである。

以　　上

（別紙）

IT 戦略特命委員会で実施したヒアリングにご協力いただいた民間企業等

（ヒアリング順）
アカマイ・テクノロジーズ合同会社
日本マイクロソフト株式会社
トレンドマイクロ株式会社
日本電気株式会社
NRI セキュアテクノロジーズ株式会社
徳田英幸慶応義塾大学環境情報学部教授
株式会社アズジェント
株式会社ＦＦＲＩ
株式会社スプラウト
株式会社ラック

以上 10 社