参考資料１

IoT セキュリティ総合対策

平成 29 年 10 月

サイバーセキュリティタスクフォース

目次

はじめに

本タスクフォースでは、IoT 機器を踏み台としたサイバー攻撃等が深刻化している状況[1]を踏まえ、本年４月、「IoT セキュリティ対策に関する提言」を取りまとめたところであり、この提言に基づき具体的な施策展開のあり方について検討を進めてきた。

IoT 化の進展は、これまで個別領域ごとに進められてきた ICT 化を越え、異なるシステムの連携による仮想的な統合システム（System of Systems）となって異なる領域のデータ連携を実現する。その結果、IoT システムはリアルな現実空間とサイバー空間を緊密に連携させたデータの生成・収集・連携・解析を通じ、社会課題の解決をもたらす社会基盤として機能していくことが期待される。

他方、社会基盤としての IoT 化が進展すると、IoT システムのセキュリティ対策が十分でない場合、その影響として広範囲に及ぶ連鎖のリスク（システミックリスク）が顕在化する可能性がある。このため、IoT システムのセキュリティ対策に際しては、部分最適ではなく、システム全体を俯瞰した全体最適を実現する観点から総合的な対策を講じていく必要がある。

本総合対策は、上記の問題意識を踏まえ、IoT システムのセキュリティ対策の総合的な推進に向けて取り組むべき課題について整理したものである。

Ⅰ　基本的考え方

IoT システムのセキュリティについては、平成 28 年８月に内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）が公表した「安全な IoT システムのためのセキュリティに関する一般的枠組」を踏まえつつ、総合的な視点に立って対策を講じていく必要がある。その際、分析の枠組みとしては、上記枠組において示されているように、「機器、ネットワーク、認証等のプラットフォーム、サービス等のレイヤーに分けて分析・検討を行う」ことが適当であり、各

---

[1] 国立研究開発法人情報通信研究機構（以下「NICT」という。）では、ダークネット（未使用の IP アドレス 30 万個）を活用したグローバルなサイバー攻撃観測網である NICTER を構築・運用しているが、当該 NICTER で観測されたダークネットに到達したパケット数（これらは主にマルウェアが次の攻撃先を探すための通信と考えられる）は 545.1 億パケット（平成 27 年）から 1,281 億パケット（平成 28 年）と１年間で 2.4 倍となっている。このうち、IoT 機器を狙ったパケットは前年の 5.8 倍に増加しており、全パケットに占める割合は 26%から 64%に増加している。

こうした中、平成 28 年 10 月、米国においてマルウェア「Mirai」に感染した監視カメラ等の IoT 機器が特定の DNS サーバに対して DDoS 攻撃を行い、当該 DNS サーバを利用していた大手の SNS 事業者、動画配信事業者、報道機関等のサイトが閲覧不能となるなど深刻な影響が出た。

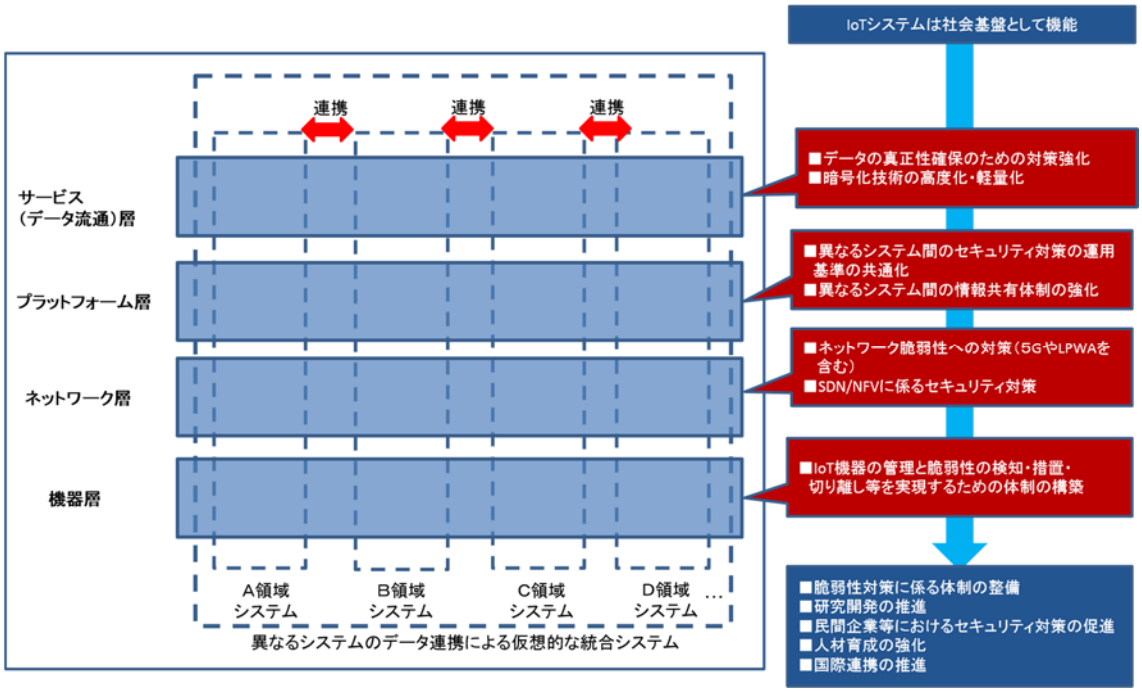
レイヤー（層）に分けて想定される課題を抽出する。

まず、サービス層においては、IoT システムの作動が正しいデータに基づくことが必須要件であり、データの改ざんを防止したデータの真正性の確保のための対策の強化や暗号化技術の高度化・軽量化の取組が必要である。

プラットフォーム層においては、異なるシステム間の認証等を通じて相互に接続されることから、システム間のセキュリティ対策の運用基準の共通化や異なるシステム間の情報共有体制の強化が求められる。

ネットワーク層においては、機器層とプラットフォーム層をつなぐデータ伝送の役割を担い、特に IoT システムを構成する無線ネットワークの脆弱性を最小化する取組が求められる。例えば、平成 32 年を目途に商用化を目指している５G(第５世代移動通信システム)や実導入が開始されている LPWA[2]といった無線ネットワークのセキュリティ対策を強化するほか、ネットワークの制御がソフトウェアで行われる SDN/NFV[3]技術が実装されていくと見込まれることから、当該技術のセキュリティ対策の強化が必要である。

さらに、機器層においては、IoT 機器の管理と脆弱性の検知・措置・切り離しなどを関係者の連携と明確な責任関係の上で実現するための体制構築が不可欠である。



[2] LPWA (Low Power Wide Area)

[3] SDN (Software Defined Network) / NFV (Network Function Virtualization)

Ⅱ　具体的施策

上記１においては、IoT システムのセキュリティ対策についてレイヤーごとに課題の抽出を行ったが、実際の対策を推進する上では、複数レイヤーに関わる施策を一体的に推進することが効率的であると考えられる。このため、以下においては、具体的な施策群を（１）脆弱性対策に係る体制の整備、（２）研究開発の推進、（３）民間企業等におけるセキュリティ対策の促進、（４）人材育成の強化、（５）国際連携の推進の５つの項目に分けて整理する。

（１）脆弱性対策に係る体制の整備

IoT 機器の脆弱性については、設計・製造、販売(輸入を含む。)、設置、運用・保守、利用のライフサイクル全体を見通した対策が必要であり、以下のとおり、各段階において適切な対策が必要である。その際、他国における同様の取組[4]について動向を注視し、必要に応じて国際連携を図っていくことに留意する必要がある。

（設計・製造段階）

① セキュリティ・バイ・デザイン等の意識啓発・支援の実施

設計・製造段階においては、所有者・運用者・利用者による安全な設定が行われるよう、ID/パスワード設定、ファームウェアのアップデート及び Wi-Fi 設定の仕様を設計時に盛り込むなど、製造業者におけるセキュリティ・バイ・デザインの考え方をいかに浸透させるかが重要となる。このような考え方を踏まえて設計された機器に認証マークを付与し、当該認証マークの付された機器の使用を推奨すること等について検討を行い、セキュリティ・バイ・デザイン等の意識啓発・支援を実施する必要がある。その際、認証を行った後に脆弱性等が発見される場合が想定されることから、認証は定期的に行い、最新の認証を受けているかどうかを利用者等が確認できる仕組みとすることが望ましい。

---

[4] 平成 29 年５月、米国ホワイトハウスは「連邦政府ネットワーク及び重要インフラのサイバーセキュリティの強化」と題する大統領令（Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure）を発出し、米国連邦政府における今後のサイバーセキュリティに関連する政策等の検討項目やスケジュールについて明確化した。この中で、「ボットネットその他の自動化・分散化された脅威へのレジリエンス」について、商務長官及び国土安全保障長官を中心に検討を行い、大統領令の発効から 240 日以内に中間報告を策定・公表するとともに、１年以内に最終報告を策定・公表することとされている。

（販売段階）

② 認証マークの付与及び比較サイト等を通じた推奨

販売段階においては、脆弱性を有する機器の流通を防止することが重要となる。そのため、一定のセキュリティ要件を満たしている IoT 機器に上記の認証マークを付与することや、比較サイト等を通じて認証マークが付与された機器が推奨される（利用者が容易に認証取得の有無等を確認できる）仕組みの構築について、具体的な検討を進める必要がある。

なお、IoT 機器の中でも国民生活や社会経済活動への影響が大きい機器については、市場への流通後も管理が可能となるよう管理番号を付与できる仕組みが考えられる。これに関して、例えば、民間団体では、IC チップ内に電子証明書を格納することにより、製造元等を識別する取組が開始されている。

（設置段階）

③ IoT セキュアゲートウェイ

機器の性格上セキュリティ対策を取ることが困難なものや海外製品など、流通している機器の中から、脆弱性を有する機器を完全に排除することは困難であることから、機器の設置(ネットワークへの接続)段階において、脆弱性を有する機器が存在することを前提として、セキュアなシステム構築を実現する仕組みが重要となる。また、IoT 機器単体では必要なセキュリティ対策の実現が困難な場合や IoT 機器に精通していない利用者についてはセキュリティ対策が十分講じられない場合が想定される。このため、IoT システム・サービス全体としてセキュリティを確保する観点から、IoT 機器とインターネットの境界上にセキュアゲートウェイを設置する取組について、総務省において実証を進めるとともに、セキュリティ評価や実際の導入を進める仕組みについて検討する必要がある。

（運用・保守段階）

④ セキュリティ検査の仕組み作り

IoT 機器が実際に利用されている状況においても、運用・保守段階において、継続的に安全安心な状態を維持することが求められる。そのため、継続的な安全性を確保するためのセキュリティ検査の仕組み作り（機器の脆弱性に係る接続試験を行うテストベッドの構築を含む。）と対策が不十分な IoT 機器への対応について検討する必要がある。ただし、この検査の仕組みについては、家庭用の IoT 機器から重要インフラで利用される IoT 機器まで様々な IoT 機器がある中で、どの機器を対象とするか慎重に検討する必要がある。

⑤　簡易な脆弱性チェックソフトの開発等

利用している IoT 機器に脆弱性が有するか確認したい利用者に対して、簡易に脆弱性をチェックできるソフトを開発して配布する取組や、脆弱性を調査する民間サービスの実施を促進する取組を検討する必要がある。

（利用段階）

⑥　利用者に対する意識啓発の実施や相談窓口等の設置

IoT システムの運用に際しては従来の端末機器以上に利用者による十分な対応が重要となることを踏まえ、利用者に対する意識啓発を推進していくことが求められる。このため、セキュリティに適合している IoT 機器の使用を推奨する取組を進めるとともに、ID/パスワード設定、ファームウェアのアップデート、Wi-Fi 設定の３点を中心とした利用者への意識啓発を行う必要がある。また、利用者からの相談窓口や、脆弱性が見つかった場合の関係機関との調整窓口を設置することが適当であり、関係府省等と連携して具体化を図る必要がある。

（脆弱性調査の実施）

上記のとおりライフサイクル全体を見通した対策に加え、既に設置されている IoT 機器はもとより、製造・販売された新規の IoT 機器についても新たな脆弱性が発見され、こうした脆弱性を突いたサイバー攻撃が行われる可能性がある。このため、関係者の連携による体制を整備し、計画的かつ包括的な脆弱性調査を継続的に実施する必要がある。

その際、重要インフラで利用される IoT 機器のように、国民生活や社会経済活動に直接影響を与える可能性がある重要 IoT 機器と、家電製品などの IoT 機器を含むサイバー攻撃の踏み台となってネットワークに悪影響を及ぼすおそれのある機器の双方について、所要の脆弱性調査と当該調査結果に基づく対策を講じる必要がある。併せて、脆弱性調査の効果を高める観点から所要の法制度の整備についても併せて検討する必要がある。

⑦　重要 IoT 機器に係る脆弱性調査

重要 IoT 機器は、サイバー攻撃の対象となった場合に国民生活や社会経済活動に深刻な被害が生じることが想定されるため、特に迅速な対策が求められる。総務省においては、平成 29 年９月から以下の事業を実施しているところであるが、この事業により得られたデータ、ノウハウ等を活用し、調査範囲の拡大、データベースの蓄積等を図る必要がある。

１）　重要 IoT 機器の脆弱性調査の実施（現地の設置環境や施工面の状況調査を含む。）。
２）　調査結果から脆弱性のある重要 IoT 機器のデータベースの作成。
３）　特定された重要 IoT 機器の所有者・運用者・利用者に対して注意喚起を行い、各者による対策を促進。
４）　特定された重要 IoT 機器の製造業者に対して情報提供を行い、今後製造する機器への対策を促進。

⑧　サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査

家庭用 IoT 機器など、サイバー攻撃の踏み台となってネットワークに悪影響を与えるおそれがある機器については、幅広く調査を行い、脆弱性を有する機器を特定する必要がある。しかし、SHODAN や Censys といった海外の公開データベースに頼った調査では、詳細な仕様が公開されていないため、そのデータベースの信頼性が疑わしく、また把握できる機器にも限りがあることから、脆弱性を有する機器を特定するため、以下の取組を実施する必要がある。

１）　サイバー攻撃観測網（NICTER、ハニーポット等）による感染機器の把握。
２）　広域の脆弱性スキャンの実施（必要に応じて、調査ツールの研究開発）。
３）　上述のサイバー攻撃観測網や脆弱性スキャンを活用し、特定のポートが開いている IoT 機器等についてデータベースを作成。

また、脆弱性を有する IoT 機器を特定した場合には、それらの機器がサイバー攻撃の踏み台となってネットワークに悪影響を与えることとならないよう、以下の取組を実施することを検討する必要がある。

４）　特定された脆弱性を有する IoT 機器が踏み台となることを防止するため、所有者・運用者・利用者に対して脆弱な機器の注意喚起を行い、各者による対策を促進。また、製造業者に対して情報提供を行い、今後製造する機器への対策を促進。

なお、脆弱性を有する IoT 機器が踏み台となったことが確認された場合の対応として、以下の取組の推進を検討する必要がある。

５）　被害拡大を防止するため、ISP による C&C サーバとの通信制御の実

施。

⑨　被害拡大を防止するための取組の推進

脆弱性を有する IoT 機器が踏み台となったことが確認された際、被害の拡大を防止するため、ISP による、当該 ISP の利用者の端末と C&C サーバの間の通信を遮断する等の取組を促進するための方策について、年度内を目途に方向性が得られるよう検討する必要がある。

⑩　IoT 機器に関する脆弱性対策に関する実施体制の整備

IoT セキュリティ対策は、例えば、IoT 機器を利用したサービス全体としてのセキュリティを考えれば、機器のライフサイクルの各段階にとどまらず、IoT 機器製造業者、流通業者、保守ベンダー、ISP 及び利用者といった各主体が補完し合いながら対応していくことが求められる。これらの各主体と相互に連携し、ネットワーク全体のセキュリティを確保するため、情報共有のあり方を含め、IoT 機器に対する脆弱性対策を実施する体制（IoT セキュリティ対策センター（仮称））のあり方について、年度内を目途に結論が得られるよう検討する必要がある。

（２）研究開発の推進

サイバー空間における攻撃の態様は常に変化しており、これに対応するには、政府が支援する産学官連携による研究開発の成果を即座に反映した最新のサイバーセキュリティ対策を実施していくことが有効である。

政府においてもサイバーセキュリティに関する研究開発は重要な課題とされており、「サイバーセキュリティ研究開発戦略」（平成 29 年７月 13 日　サイバーセキュリティ戦略本部決定）において、研究開発を通じて国際競争力を強化すること、研究開発で得られた知見により経済成長につながる新産業を創出することや我が国として必要な技術力を獲得・保持すること等を目的として、サイバーセキュリティに関連する研究開発を推進することが重要である旨が示されている。

他方、サイバーセキュリティの研究開発は、社会的なニーズ、特にセキュリティ運用の知見を踏まえた形で実施され、その成果が早期に社会へ還元されることが求められる。このため、セキュリティ運用の現場の状況を、いち早く研究開発の場へ情報共有し、ニーズにあった研究開発が促進されるような枠組みを検討する必要がある。ただし、セキュリティ運用の現場における知見、特にサイバー攻撃を防げなかった原因・教訓等については、研究開発に限らず、運用組織の

外部へ情報共有されることが少ないことに留意することが求められる。

したがって、セキュリティ技術の研究開発においては、こうしたセキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進する枠組みを構築するとともに、研究開発により産業競争力が高まることで、さらに新たな技術を獲得し、我が国のセキュリティ技術に関する知見が深まるといった好循環が生み出される研究開発環境を整備していく必要がある。

① 基礎的・基盤的な研究開発等の推進

これまでNICTでは、中長期計画に基づき、サイバーセキュリティ分野の基礎的・基盤的な研究開発等を実施しているところであり、引き続き、サイバーセキュリティ技術、セキュリティ検証プラットフォーム構築活用技術、暗号技術の研究開発等に取り組むとともに、研究開発成果の普及や社会実装を目指すことが求められる。

特に、サイバー攻撃は巧妙化・複雑化しており、特定の組織の情報をターゲットとする標的型攻撃は、近年、特に大きな脅威となっていることから、標的型攻撃への対策に向けた研究開発を重点的に行うことが求められる。

NICTは、平成29年５月、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、その攻撃活動を長期観測することで、従来では収集が困難であった攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能にするサイバー攻撃誘引基盤「STARDUST」（スターダスト）を開発したことを公表した。

こうした研究開発を基に、今後、早期の社会実装を目指し、新たに出現する未知の標的型攻撃の挙動を早い段階で明らかにするとともに、分析結果をセキュリティ対策機関等と連携して情報共有を図ることが可能な、高度で効率的なサイバー攻撃誘引基盤を構築する必要がある。

② 広域ネットワークスキャンの軽量化

近年、IoT機器を狙ったサイバー攻撃は著しく増加傾向にあり、脆弱なIoT機器への対策は喫緊の課題である。脆弱なIoT機器のセキュリティ対策のため、膨大なIoT機器に対して広域的なネットワークスキャンを実施する必要がある。このため、広域ネットワークスキャンの軽量化など、その効率的な実施のために必要な技術開発を推進する必要がある。

③ ハードウェア脆弱性への対応

集積回路の設計工程において、ハードウェア脆弱性が存在する可能性が指摘されており、平成29年度から、戦略的情報通信研究開発推進事業（SCOPE）に

おいて、ハードウェア脆弱性の検知技術の研究開発が行われている。具体的には、膨大な数の回路設計図をビッグデータとして収集・蓄積し、これを元に脆弱性が存在する可能性のあるチップを、AI を活用して類型化し、ハードウェア脆弱性を発見することを目指すものである。

今後、IoT 端末はさらなる増加が見込まれており、ソフトウェアやファームウェアに対する対策と合わせて、引き続き、ハードウェアに組み込まれるおそれのあるハードウェア脆弱性を検出する技術の研究開発について、ビッグデータや AI を活用しつつ推進していく必要がある。

④　スマートシティのセキュリティ対策の強化

総務省では、都市に設置されたセンサーから収集・生成・蓄積・解析されるデータを活用し、その解析結果を都市経営の課題解決などに活用するデータ利活用型スマートシティ事業を平成 29 年度から開始している[5]。同様の取組は EU の研究開発プロジェクト Horizon 2020 や米国国立標準技術研究所（NIST）が主導する GCTC（Global City Team Challenge）[6]プロジェクトでも展開されている。スマートシティにおいてデータの連携・解析などを行うプラットフォームのセキュリティ対策はデータの真正性を確保し、かつスマートシティの機能をサイバー攻撃から防御するためにも極めて重要である。

このため、スマートシティのプラットフォームに係るセキュリティ要件の具体化や所要の技術開発を推進するとともに、その成果を国際的な標準化プロセスに提案する等の取組を一体的に進めていく必要がある。

⑤　衛星通信におけるセキュリティ技術の研究開発

宇宙産業の急速な発展に伴い、今後、衛星へのサイバー攻撃（衛星回線の傍受やデータの窃取など）が増加することが懸念される。しかし、衛星の実装スペースの制約等により、マルウェア対策ソフトや暗号仕様を更新するのは容易ではない。

こうした問題意識の下、「宇宙×ＩＣＴに関する懇談会報告書」（平成 29 年８月　宇宙×ＩＣＴに関する懇談会）においても指摘しているように、どれ程の計算力をもってしても解読できない安全性を備えた通信を実現するために、

---

[5] 平成 29 年度においては、北海道札幌市、神奈川県横浜市、兵庫県加古川市、香川県高松市、福島県会津若松市、埼玉県さいたま市浦和美園地区が選定されている。

[6] GCTC は、スマートシティに関する全米、国際的な連携を目指した取組であり、複製可能・拡張可能・持続可能なモデル作りを目指し、平成 26 年９月から開始された。本プロジェクトの次期ラウンド（平成 29 年９月～平成 30 年秋）では、サイバーセキュリティ対策に焦点をあてた”Secure Cities and Communications Challenge (SC3)”という取組を進めていくこととしている。

量子暗号技術の研究開発や高秘匿衛星光通信技術の実証を行うとともに、衛星のバックアップや高高度での中継を行うための航空機等による移動体光通信技術の研究開発などに取り組む必要がある。

⑥　AI を活用したサイバー攻撃検知・解析技術の研究開発

日々、数多く発生するサイバー攻撃に対して、AI（人工知能）を活用することにより、サイバー攻撃の検知・解析を自動化することができ、また、機械学習により、サイバー攻撃のパターンを抽象化することで、多様なサイバー攻撃に対する迅速なセキュリティ対策を講ずることが可能となる。

したがって、今後、AI を活用したサイバー攻撃検知・解析技術の研究開発にも取り組む必要がある。その際、研究開発に有用な各種調査のデータの情報共有の仕組み、検知・解析の対象となるインシデント情報の収集・集約体制、検知・解析に必要となる十分な計算処理能力やシミュレーション能力を有するサイバー攻撃検知・解析環境の整備が求められる。

（３）民間企業等におけるセキュリティ対策の促進

民間企業等におけるサイバーセキュリティ対策の促進については、「2020 年及びその後を見据えたサイバーセキュリティの在り方について　―サイバーセキュリティ戦略中間レビュー―」（平成 29 年７月　サイバーセキュリティ戦略本部決定）において、民間企業等のサイバーセキュリティに係る投資を促進することで、セキュリティ産業における継続的な需要喚起を促すこととされている。また、一定品質を備えたセキュリティサービスを認定する仕組みを構築し、供給側の競争力を強化するとともに、これらのサービスの活用を促すこととされている。

さらに同レビューにおいては、重要インフラ事業者等における攻撃・脅威情報の共有については、既に様々な取組がなされており、着実に進展しているが、情報の提供者における課題を解消しつつ、利用者がより対策を講じやすい情報を共有することにより、サイバー攻撃の被害及び被害の拡大防止に更に努める必要があるとされている。

このため、以下の取組により、民間企業等におけるサイバーセキュリティ対策を促進する必要がある。

①　民間企業のセキュリティ投資等の促進

民間企業においては、１社がサイバー攻撃の被害を受けた場合に、被害がサプライチェーン全体に広がる懸念が増すことになるため、企業間の取引におい

ても、取引条件としてサイバーセキュリティに関する要求がなされつつある状況にある。しかしながら、コスト等が原因でセキュリティサービスの導入が進んでおらず、また、サイバーセキュリティ製品の効果的な活用もできていない状況にある。

そこで、経済産業省と連携して、IoT 産業等の関連産業等の成長を見据え、企業におけるセキュリティ投資を促進するため、高レベルのサイバーセキュリティ対策に必要なシステムの構築やサービスの利用に対して、税制優遇措置を講ずる方向で検討していく必要がある。

② セキュリティ対策に係る情報開示の促進

民間企業においては、複雑・巧妙化するサイバー攻撃に対する対策強化を進める動きが見られるようになってきており、こうした取組をさらに促進するためには、セキュリティ対策を講じている企業が市場を含む第三者から評価される仕組みを構築していくことが求められる。

米国においては、日本の有価証券報告書にあたる 10－K 報告書において記載することが推奨されるセキュリティ対策について証券取引委員会（SEC）がガイドラインを策定・公表している[7]。こうした情報開示はあくまで任意のものであるが、企業の対策促進の観点からみて有益な取組であると考えられる。

このため、我が国においても、あくまで任意の情報開示であることを前提としつつ、企業のセキュリティ対策に係る情報開示に関するガイドラインの策定について、関係府省と連携しつつ、年度内を目途に一定の結論が得られるよう検討する必要がある[8]。その際、開示する情報の粒度については情報開示が新たな攻撃を誘発しないよう十分に配慮するとともに、こうした情報開示とサイバーセキュリティ保険の普及の在り方について併せて検討する必要がある。

③ 事業者間での情報共有を促進するための仕組みの構築

事業者間の情報共有を促進するためには、解析・対処能力が事業者間で一様ではないことを踏まえ、情報共有の目的・利点・手順、必要とされる情報を明確化するとともに、平時・非常時などの状況に応じた提供すべき情報の範囲及び提供先の範囲等を明確化することが重要である。また、単に各事業者の情報

---

7 SEC (Securities and Exchange Commission), ”CF Disclosure Guidance : Topic No.2 Cybersecurity”（平成 23 年 10 月）

8 「企業経営のためのサイバーセキュリティの考え方の策定について」（平成 28 年８月 NISC）における議論や、「サイバーセキュリティ経営ガイドライン Ver 1.1」（平成 28 年 12 月　経済産業省、独立行政法人 情報処理推進機構）に関する動向等を踏まえつつ、検討する必要がある。

を共有するだけではなく、効果的かつ効率的に実施することが重要であり、将来的には、共有された情報に基づき、サイバー攻撃に応じた自動防御を目指すことも考えられる。

そのため、事業者間での情報共有を促進するための仕組みを検討する必要がある。具体的には、新たに情報共有を開始する事業者との間でも安全・安心な情報共有ができるよう、情報提供元及び共有される情報自体の信頼性を担保する仕組みや、様々な事業者から提供された大量の情報の分析、情報の重複の排除、情報の重み付け、サイバー攻撃の全体像の把握を行った上で、入力フォーマットの標準化などの情報共有を実施する仕組みを検討する必要がある。また、国内の民間団体においては、米国国土安全保障省（DHS）が運営する自動情報共有システム（AIS[9]）との連携を開始しており、こういった取組を支援することも重要である。

④　情報共有時の匿名化処理に関する検討

情報を共有する際、当該情報に通信のネットワーク設備に係る情報などのセンシティブな情報や個人情報が含まれ得ることから、事業者によっては情報共有をすることに対して消極的になることが想定される。

そこで、情報共有に当たって、情報の秘匿性を担保する観点から、情報の匿名化処理の導入を検討する必要がある。その際、どのような方法で、どの程度まで情報を匿名化するべきかについての評価指標やガイドラインの整備を検討する必要がある。なお、これらの検討事項については、情報共有基盤等を活用した自動化処理の可能性に留意して検討する必要がある。

⑤　公衆無線 LAN のサイバーセキュリティ確保に関する検討

公衆無線 LAN については、2020 年東京オリンピック・パラリンピック競技大会（以下「2020 年東京大会」という。）に向けて、観光や防災の観点から、その普及が進んでいるところである。しかし、多くの公衆無線 LAN のサービスにおいて、セキュリティに対する配慮に欠けるものも多く、これらのサービスを踏み台にした攻撃や情報漏洩などのインシデントが発生することが考えられる。このため、公衆無線 LAN におけるサイバーセキュリティ上の課題を整理し、今後必要な対策について、年度内を目途に一定の結論が得られるよう検討する必要がある。

（４）人材育成の強化

[9] AIS (Automated Indicator Sharing)

これまで、総務省においては、実践的サイバー防御演習（平成 25 年度より総務省が実施、平成 28 年度より NICT が実施主体となっている。）を実施してきたところである。平成 29 年４月からは、NICT に組織された「ナショナルサイバートレーニングセンター」において、

１） 国の行政機関・地方自治体及び重要インフラ事業者などを対象とした実践的サイバー防御演習（CYDER）
２） 2020 年東京大会の適切な運営に向けたセキュリティ人材の育成（サイバーコロッセオ）
３） 若手セキュリティエンジニアの育成（SecHack365）

の取組を行っているところである[10]。

政府においてもサイバーセキュリティ人材の育成は重要な課題とされており、「サイバーセキュリティ人材育成プログラム」（平成 29 年４月 18 日　サイバーセキュリティ戦略本部決定）において、企業をはじめとする社会で活躍できるサイバーセキュリティに関する人材育成の方向性が示されたところである。

同プログラムでは、ビジネスにおけるイノベーションを実現するために必要なサイバーセキュリティ人材の育成や、若年層に必要な教育の在り方など、企業をはじめとする社会で活躍できるサイバーセキュリティに関連する人材育成の方向性が示されている。

なお、現在、サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会の下に設置されているサイバーセキュリティ人材の育成に関する施策間連携ワーキンググループにおいて、政府全体での人材育成の取組について検討が行われているところであり、今後、文部科学省をはじめとする関係省庁・機関とも連携した人材育成の取組が必要である。

① 実践的サイバー防御演習（CYDER）の充実

NICT は、大規模仮想 LAN 環境上に CYDER を構築し、平成 28 年度は全国 11 地域において約 1,500 名を対象に演習を実施し、平成 29 年度においては全国 47 都道府県において約 3,000 名を対象に演習を実施することとしている。引き続き、国の行政機関・地方自治体及び重要インフラ事業者などを対象としてこうした取組を進めるとともに、新たな手法のサイバー攻撃にも対応できる

10 上記のほか、平成 29 年７月の情報通信審議会答申「『IoT／ビッグデータ時代に向けた新たな情報通信政策の在り方』第四次中間答申」（IoT 総合戦略（改訂版））を踏まえ、SDN/NFV 人材の育成を推進する一般社団法人「高度 IT アーキテクト育成協議会」が設立されたところであり、SDN/NFV に係る技能の習得に際してもセキュリティ教育が十分に行われることが期待される。

演習プログラム・教育コンテンツの開発を継続的に行うよう努める必要がある。

② 2020 年東京大会に向けたサイバー演習の実施

大規模クラウド環境を用いて、公式サイト、大会運営システムや、社会インフラの情報システム等を模擬したシステムを構築し、当該システムを活用して、大会開催時を想定したサイバー攻撃を模擬し、大会組織委員会のセキュリティ担当者を中心に、攻撃側と防御側の手法の検証及び訓練を行う環境を整備している。平成 28 年度に開始した本事業について、更なる内容の拡充を図り、より実践的な環境の下でのサイバー演習の強化を図る必要がある。また、大会終了後に、同システムによる演習の実施により得られた知見、ノウハウを活用する方策について併せて検討する必要がある。

③ 若手セキュリティ人材の育成の促進

我が国のサイバーセキュリティ技術は、世界のセキュリティソフトウェアの市場における存在感が決して大きくないなど、製品開発等における分野では遅れをとっている。サイバー攻撃は、日々刻々と変化しており、高度な技術力を支えるセキュリティ人材の育成に中長期的に取り組む必要がある。

具体的には、引き続き、若年層の ICT 人材に対し、集中的な研修を行うとともに、海外派遣による経験等を通じて、サイバーセキュリティのコア技術を開発できるような人材、あるいは、そのような技術力を生かしてリスクを許容し、積極的に起業ができるような人材の育成方策を検討し、そうした人材に対する支援の枠組みの構築を促進する必要がある。

④ IoT セキュリティ人材の育成

IoT が社会に実装されていく中、従来の通信分野のみならず、製造、流通、サービスなど多岐にわたる分野で IoT システムが構築・運用されるものと見込まれる。このため、広く IoT セキュリティを担うことができる人材の育成が不可欠である。

そこで、IoT セキュリティに関するスキルを獲得するための教材作成や研修体制の整備、各種調査のデータの共有、機器の脆弱性に係る接続試験を行うテストベッドの構築等を行うための総合的な対策を産学官の連携により推進するための環境整備に向けた検討を行う必要がある。

（５）国際連携の推進

サイバー空間は国境を越えて利用される領域であり、サイバーセキュリティの確保のためには国際連携の推進が必要不可欠である。このため、米国をはじめとするG7各国を中心に、二国間及び多国間の枠組みの中で本分野における情報共有や国際的なルール作り（サイバー空間における国際法の適用関係の明確化や国際規範の具体化）のほか、先に述べたようなIoT機器の脆弱性対策、研究開発、人材育成などを進めていく必要がある。特に平成31年にはG20が我が国で開催されることを見据え、サイバーセキュリティ分野における国際協調に向けて主導的な役割を果たしていくことが求められる。その際、サイバーセキュリティの確保を理由とする情報の自由な流通を阻害する動きに対しては、データの越境流通の円滑化がサイバー空間の健全な発展に不可欠であることを踏まえて対応していく必要がある。

① ASEAN各国との連携

アジア地域においては引き続きASEAN各国との協力関係の強化が必要である。具体的には、日・ASEANサイバーセキュリティ協力ハブの構築による実践的サイバー防御演習「CYDER」等の海外展開を通じ、３年間（平成29年～平成31年）で500人を目標としてセキュリティ人材の育成支援を進める必要がある。

また、日・ASEAN情報セキュリティ政策会議、日ASEAN情報通信大臣会合及び高級実務者会合、ISPを対象とする日ASEAN情報セキュリティワークショップ等の定期的な開催により、我が国及びASEANにおけるサイバーセキュリティの脅威をめぐる状況やIoTセキュリティ対策に関する情報交換を行うほか、ASEAN側のニーズを踏まえつつ、ASEANにおけるIoTセキュリティ強化に向けた施策の導入・促進のための協力を推進する必要がある。

② 国際的なISAC間連携

国際的なISAC（Information Sharing and Analysis Center）間連携を引き続き推進していく必要がある。具体的には、国際連携ワークショップの開催等を通じて、日本のICT-ISACと米国のICT分野のISACとの連携を強化し、通信事業者、IoT機器ベンダー、セキュリティベンダー等が、AIS等を介して脅威情報を自動的に共有し、サイバーセキュリティ対策に活用することを促す必要がある。

③ 国際標準化の推進

IoTシステムのセキュリティに係る国際標準化がISO/IEC及びITU-Tで開始されているところであり、関係する府省庁と連携しつつ、こうした活動に積

極的に貢献していくことが求められる。その際、IoT 推進コンソーシアムの IoT セキュリティワーキンググループにおける議論等を通じ、産学官連携による検討結果を国際標準に反映すべく努める必要がある。

④　サイバー空間における国際ルールを巡る議論への積極的参画

サイバー空間における国際ルール等のあり方については、国連をはじめ、G7 や G20、二国間協議等の政府が主体となる場だけでなく、ISOC（Internet Society)や ICANN(Internet Corporation for Assigned Names and Numbers)、IGF（Internet Governance Forum）等のマルチステークホルダーによる場を含め、様々なチャネルを通じて議論が進められてきている。狭義のインターネットガバナンスのあり方について、物理的な伝送網の上に構築されたパケット伝送網については、「自律・分散・協調」を基本原則として民間主体のマルチステークホルダーによる運営が行われている。しかし、更にその上位に位置するデータ・情報流通層においては、情報の自由な流通（オープンエコノミーの確保)、個人データの越境流通、国際連携によるサイバーセキュリティの確保、サイバー空間における安全保障の確保などの様々な議論が行われているところであり、こうした議論に我が国として積極的に参画していく必要がある。その際、サイバー空間におけるルール整備は基本的にリアル空間と同等の規制が適用されるものであり、かつ領域ごとの議論は既存の国際ルールに準拠することを基礎として議論が進められることが期待される。

Ⅲ　今後の進め方

IoT セキュリティ総合対策の推進に際しては、半年に１度を目途としつつ、必要に応じて検証を行い、進捗状況を把握するとともに、本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、必要に応じて随時見直しを行っていくことが望ましい。また、対策の推進に際しては、NISC や経済産業省をはじめ、関係する府省庁との連携の下に進めていく必要がある。

IoT セキュリティ総合対策の推進は、2020 年東京大会の成功に向けても必須である。今後３年間で IoT システムの普及が急速に進むと見込まれることから、重要インフラの防御対策強化の観点を含め、IoT セキュリティ対策の強化に向け、関係するステークホルダーの連携によるビジョンの共有と取組の強化が不可欠である。