コロナ禍でのサイバーセキュリティ対策「IoT・5G セキュリティ総合対策 2020」について

総務省
サイバーセキュリティ統括官室
参事官補佐
横澤田（よこさわた）　悠（ゆう）

総務省
サイバーセキュリティ統括官室
事務官
中村（なかむら）　公洋（きみひろ）

1. はじめに

総務省サイバーセキュリティタスクフォース（座長：後藤厚宏 情報セキュリティ大学院大学学長）[*1]は、2020年7月、「IoT・5Gセキュリティ総合対策2020」を策定した。

従来から、サイバーセキュリティタスクフォースにおいては、近年のサイバーセキュリティリスクの更なる高まりや、5Gサービスの2020年の本格的な導入を見据え、IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方を検討してきた。

2020年以降、我が国においては、新型コロナウイルス感染症（以下、COVID-19）への対応に官民で連携して取り組んでいる状況である。まさに未曾有の国難ともいえるこの状況において、テレワークシステムやWeb会議システムがビジネスやプライベートなど様々な分野で活用され、SNSアプリによるアンケートを通じたデータ収集がCOVID-19への対策の立案に活用されるなど、経済活動や国民生活においてICTの有用性が再認識されてきている。

「IoT・5Gセキュリティ総合対策2020」は、2019年8月に策定・公表した「IoT・5Gセキュリティ総合対策」について、上記のような社会の趨勢も踏まえつつ、必要な改定を行ったものである。本稿では「IoT・5Gセキュリティ総合対策2020」の内容について、主要なものを中心にご紹介したい。

2.「IoT・5Gセキュリティ総合対策2020」策定の経緯

IoTシステムは、これまで個別分野ごとに進められてきたICT化を越えて、異分野間のデータ連携を実現し、実空間とサイバー空間を連携させたデータの生成・収集・活用等を通じて、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ている。

一方で、IoT機器は、ウイルス駆除ソフトのインストールなどの対策が困難、利用者等においてインターネットにつながっているという意識が低いなどの理由から、サイバー攻撃の脅威にさらされている。

IoT分野のセキュリティ対策の重要性の高まりを受け、総務省では、2017年より、セキュリティ分野の有識者で構成されるサイバーセキュリティタスクフォースを開催し、同年10月に、IoTに関する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を整理した「IoTセキュリティ総合対策」が公表された。それ以降、進捗状況と今後の取組について定期的に整理が行われ、その結果は「IoTセキュリティ総合対策 プログレスレポート2018」（2019年7月）、「IoTセキュリティ総合対策 プログレスレポート2019」(2019年5月)、「IoT・5Gセキュリティ総合対策」（2019年8月）、「IoT・5Gセキュリティ総合対策 プログレスレポート2020」（2020年5月）に取りまとめられ、公表されている。

また、2020年1月には、2020年7月より開催される予定であった東京大会に向けた対処として、「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項［緊急提言］」が公表されている。

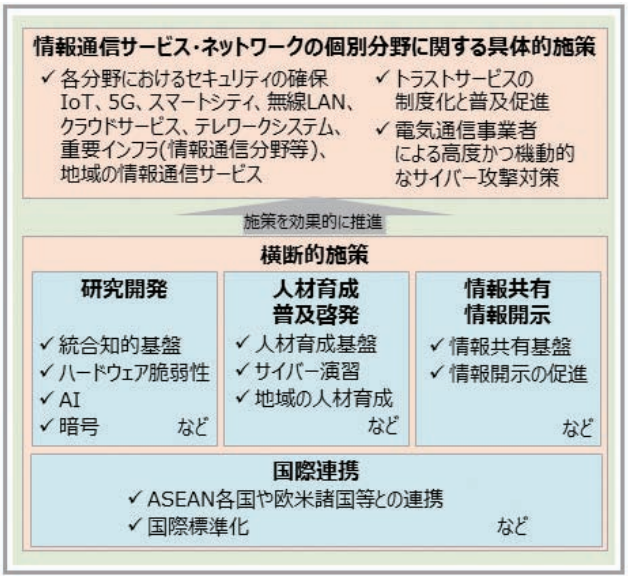
今般、「IoT・5Gセキュリティ総合対策」の策定・公表後の議論や状況変化を踏まえつつ、サイバーセキュリティタスクフォースでの検討の結果、「IoT・5Gセキュリティ総合対策」を改定し、新たな施策を盛り込む形で「IoT・5Gセキュリティ総合対策2020」が策定された。

3.「IoT・5Gセキュリティ総合対策2020」

3.1 全体構成

「IoT・5Gセキュリティ総合対策2020」では、改定に当たって4点の主要な政策課題を掲げた上で、総務省として取り組

*1 サイバーセキュリティタスクフォース第1回会合（2017年1月）から第15回会合（2019年8月）は安田 浩 氏（当時 東京電機大学学長）が座長を務めた。後藤 厚宏 氏（情報セキュリティ大学院大学学長）は第16回会合（2019年11月）より座長を務める。



出展：総務省作成

■図1. IoT・5Gセキュリティ総合対策2020の枠組み

むべき施策を「情報通信サービス・ネットワークの個別分野に関する具体的施策」及び「横断的施策」に分類して整理している（**図1**）。

「具体的施策」としては、「IoTのセキュリティ対策」、「5Gのセキュリティ対策」、「クラウドサービスのセキュリティ対策」、「スマートシティのセキュリティ対策」、「公衆無線LANのセキュリティ対策」、「テレワークシステムのセキュリティ対策」など、計10個の領域が挙げられている。「横断的施策」としては、「研究開発の推進」、「人材育成・普及啓発の推進」、「国際連携の推進」及び「情報共有・情報開示の促進」を挙げている。

以下では、主要な政策課題とそれに対応する個別施策を概観する。

3.2 「IoT・5Gセキュリティ総合対策」改定に当たっての主要な政策課題

(1) COVID-19への対応を受けたセキュリティ対策の推進

①テレワークの利用の増加への対応

COVID-19の感染拡大防止に当たっては、早期からテレワークの活用を呼びかけており、特に2020年4月の緊急事態宣言の発出後は、人と人との接触機会を8割程度低減することと併せ、テレワークが強力に推進されてきた。テレワークの実施に当たっては適切なセキュリティ対策を取る必要があるが、実際にテレワークを導入するに当たっては、約7割の企業が「情報セキュリティの確保」が課題と感じている。

そのため、総務省では、企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として、2018年4月に「テレワークセキュリティガイドライン（第4版）」[*2]を作成しているが、これをより具体的で分かりやすくした、実践的な内容のチェックリスト等が有用であり、総務省において早期に策定を行う必要がある[*3]。また、COVID-19への緊急対応のため多くの企業では準備期間が十分とれずにテレワークを導入・導入検討していると想定されるが、特に中小企業等においては十分なセキュリティ知識を有した担当者がいない場合が多いと想定されるため、テレワーク導入時及び導入後においてセキュリティ対策の専門家が相談を受け付ける体制を提供する必要がある[*4]。

また、テレワークが実施又は推奨されている企業においても、急遽テレワーク実施中に出社する必要が発生するケースが存在し、具体的な理由として請求書や押印手続、印刷など紙の書類の処理の必要性が挙げられている。この点で、テレワークの普及の促進の観点からも、紙の書類のデジタル化や業務そのもののデジタル化の更なる促進が必要である。

他方、デジタル化の促進のためには、業務上作成又は保管等を行っている書類の真正性を電子的に確保できる手段が必要不可欠であり、例えば、電子署名やeシールなどのト

＊2　2021年2月現在、総務省では、テレワークを取り巻く環境やセキュリティ動向の変化を踏まえ、2021年2月15日から3月5日にかけて、「テレワークセキュリティガイドライン（第5版）」（案）に対する意見募集を実施している。

＊3　2020年9月に総務省は中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（初版）を公表。併せて、手引き（チェックリスト）の内容を具体的な環境で実施する際の参考となるよう、テレワークで多く利用される製品（Cisco Webex Meetings, Microsoft Teams, Zoom）を対象とした補足的な設定解説資料も公表。https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

＊4　2020年7月に総務省はテレワークにおけるセキュリティに関する相談を受け付ける無料相談窓口「テレワークのセキュリティあんしん無料相談窓口」（2020年7月～2021年3月）を開設。https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

ラストサービスの活用を促進することが考えられる[*5]。併せて、一定の基準を満たすトラストサービスを認定するような公的な枠組みを構築することで、一層その普及を加速していくことが重要であり、例えば、タイムスタンプについて、2020年度中に国による認定制度の整備を行うこととしている[*6]。

②クラウドサービスの利用の進展を踏まえた対応

クラウドサービスが重要な社会基盤となりつつある現在においても、大手クラウドサービスでサービス障害が発生したり、自治体専用IaaSサービスにおいてストレージ障害やデータアクセス障害が発生したりするなど、セキュリティに対する不安やセキュリティ上の課題は依然として存在する。

政府機関等が調達するクラウドサービスのセキュリティに関しては、「政府情報システムのためのセキュリティ評価制度」(通称 ISMAP：Information system Security Management and Assessment Program) が2020年6月に立ち上げられ、サービスの登録に向けた準備が進められている。また、従前より民間団体等においては、クラウドサービスのセキュリティに関する認証等の取組もなされているところであり、このようなクラウドサービスのセキュリティの可視化の取組が着実に進んでいくことが望ましい。

(2) 5Gの本格開始に伴うセキュリティ対策の強化

5Gは4Gなどの従来の移動通信システムと比較して、「超高速」、「超低遅延」、「多数同時接続」であるという特長を有しており、IoT時代の基盤技術として、様々な産業分野での利活用が期待されている。サイバーセキュリティの観点からは、5Gのネットワークでは、モバイルエッジコンピューティング (MEC) の活用に加え、ネットワーク機能の仮想化・ソフトウェア化などが一層進んでいくことが想定されるため、ソフトウェアをはじめとするサプライチェーンリスクへの対応が不可欠である。

2020年より、携帯電話事業者が一般向け5Gサービスを提供開始しているほか、ローカル5Gについても免許交付が始まっているところであり、将来の社会基盤としての5Gの安全性や信頼性の確保のため、5G黎明期の現段階から、セキュリティ・バイ・デザインの観点で、官民で連携して対策を取る必要がある。具体的には、脆弱性の検証手法等の確立と体制整備、脆弱性情報や脅威情報等の共有の枠組みの構築及び産業振興と制度面の両面からの5Gのセキュリティ対策の促進を進めることが必要である。

(3) サイバー攻撃に対する電気通信事業者のアクティブな対策の実現

これまでのIoTのセキュリティ対策は、IoT機器の機能要件の設定や、パスワードの設定等に不備のあるIoT機器等の調査及び注意喚起の実施など、IoT機器に対する対策が中心であった。一方で、IoTのセキュリティ対策をより実効的なものにするためには、サイバー攻撃が通過するネットワーク側でより機動的な対処を行う環境整備が必要と考えられる。

このため、IoTをはじめ、情報通信システム全般において、海外における動向 (制度、実施状況等) も参考としながら、ユーザ側で運用している情報通信機器や情報システムのセキュリティ対策と連動する形で、インターネット上でインターネットサービスプロバイダが管理する情報通信ネットワークにおいても高度かつ機動的な対処を実現するための方策の検討が必要である。

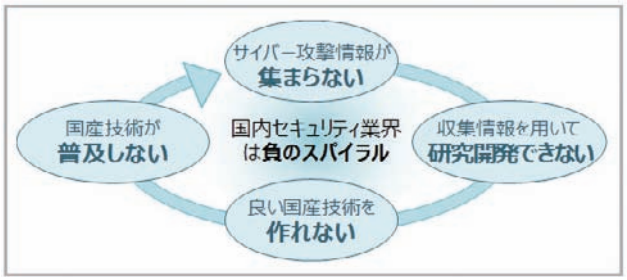
(4) 我が国のサイバーセキュリティ情報の収集・分析能力の向上に向けた産学官連携の加速

我が国のセキュリティ事業者は、海外のセキュリティ製品を導入・運用する形態が主流である。そのため、我が国のサイバーセキュリティ対策は、海外製品や海外由来の情報に大きく依存しており、国内のサイバー攻撃情報等の収集・分析等が十分にできていない状況である。さらに、海外事業者の製品の使用により、国内のデータが海外事業者に流れ、我が国のセキュリティ関連の情報が海外で分析される一方、分析の結果得られる脅威情報を海外事業者から購入する状況が継続している。

これは、(a) 国内でのサイバー攻撃関連の実データが集まらず、(b) 実データが集まらないため実データを使った研究開発ができず、(c) 研究開発ができないため良い国産セキュリティ技術を作れず、(d) 良い技術を作れないため国産技術が普及せず、(a') 国産技術が普及しないからサイバー

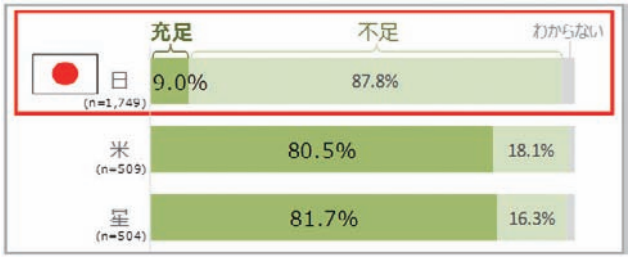
＊5　電子署名法に関連して、総務省、法務省、経済産業省は、利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&Aを2020年7月及び9月にそれぞれ公表。

＊6　2020年12月19日、「タイムスタンプ認定制度に関する検討会取りまとめ (案) 及び時刻認証業務の認定に関する規程 (案) に対する意見募集」を開始。



出展：総務省作成

■図2. データ負けのスパイラル



出展：企業における情報セキュリティ実態調査2019
（NRIセキュアテクノロジーズ）より総務省作成

■図3. セキュリティ対策に従事する人材の充足状況

攻撃関連の実データも集まらない、という「データ負けのスパイラル」に陥っている状況である（図2）。

このように国内のセキュリティ事業者においては、実データが集まらないためコア部分のノウハウや知見を蓄積することができず、我が国がグローバルレベルの情報共有において一層の貢献を果たし、国際的に通用するエンジニアの育成をより効果的に実施することが難しくなっている。一方で、利用者側企業においても、セキュリティ製品やセキュリティ情報を適切に取り扱える人材が不足している状況がある。我が国においてセキュリティ人材が充足しているとの回答は1割を切っており、人材不足は深刻な状況である（図3）。

我が国の企業を支えるセキュリティ技術が過度に海外に依存する状況を回避・脱却し、サイバーセキュリティ人材の育成を含めて我が国のサイバー攻撃への自律的な対処能力を高めるとともに、我が国としてグローバルレベルの情報共有において一層の貢献を実現していくためには、オープン型の研究開発や人材育成の基盤を構築・運用して産業界等に開放し、産学官の英知を結集して、取組を進めていく必要がある。

具体的には、以下の取組を自律的に実施する仕組み・体制を構築し、国内でサイバーセキュリティ情報を収集・蓄積（生成）・提供する環境が必要である（図4）。

（A）実データを大規模に集約・蓄積する仕組み

具体的には産学官が連携して、各種公的機関等が観測した情報やインターネット上の公開情報（OSINT）を大規模に集約して蓄積する仕組みが考えられる。

（B）実データを定常的・組織的に分析する仕組み

具体的には攻撃ツールや手法を並列かつリアルタイムに観測・解析する環境を構築するとともに、本環境を活用した高度解析者の結集・育成を行う仕組みが考えられる。

出展：総務省作成

■図4. サイバーセキュリティ統合知的・人材育成基盤の構築

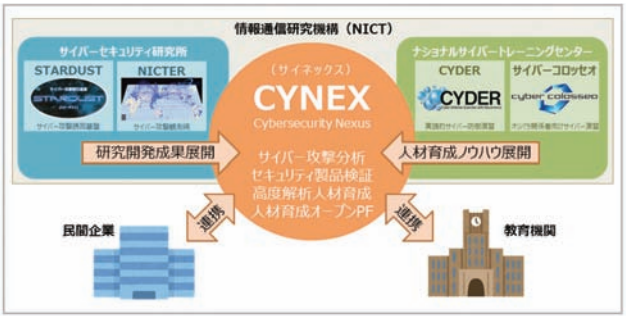
（C）実データで国産製品を運用・検証する仕組み

具体的には国産製品のプロトタイプ群を長期運用・機能検証できる環境を構築するとともに、本環境を活用したSOC人材の育成を行う仕組みが考えられる。

（D）実データから脅威情報を生成・共有する仕組み

以上（A）～（C）で収集した実データを用い、AIを駆使した大規模横断分析を行い、日本独自の脅威情報を生成し、信頼性の高い、説明可能かつ即時的なセキュリティ情報を関連機関で共有することが考えられる。

加えて、我が国全体としては、特に戦略を立ててシステムベンダと共働しつつ組織のセキュリティ対策を先導できる人材が不足しているほか、環境構築技術者・開発者層のセキュリティ知識の不足により、本来防げるはずのセキュリティインシデントが発生している。このような人材育成を全て国で実施することは困難であるため、特に民間事業者において大学等の教育機関を巻き込みながら自立的に育成を行うことが求められるが、演習用の環境構築やシナリオ開発には高度な知識や技術力、そして基盤となる計算機環境が必要であり民間企業・教育機関のみでは十分に対応できていない。また、このような不十分な国内基盤を背景として、既存の民間演習事業においても、海外の演習教材に依存し、日本特有の事例が反映できない状況である。こうした課題に対応するため、サイバーセキュリティの人材育成に関し、演習の実施に関する様々な要素（データセット、教材、演習用ミドルウェア、計算機リソースなど）を総合的にカバーする、オープン型の新たな人材育成プラットフォームや、産学官の連携によって当該プラットフォームを積極的に活用するためのコミュニティの支援が必要である（**図4**）。



出展：サイバーセキュリティタスクフォース第28回会合資料「サイバーセキュリティ統合知的・人材育成基盤CYNEXの構築について」（NICT作成）

■図5. サイバーセキュリティに関する産学官の結節点『CYNEX』

我が国で唯一の情報通信技術に関する公的研究機関である国立研究開発法人情報通信研究機構（NICT）においては、従来より、サイバーセキュリティ研究所において、最先端のサイバーセキュリティ関連技術の研究開発を実施するとともに、ナショナルサイバートレーニングセンターにおいて、実践的サイバー防御演習等による人材育成を実施してきた。2021年2月に開催されたサイバーセキュリティタスクフォースの会合では、これらの取組に加えて、新たにサイバーセキュリティに関する産学官の結節点となる先端的基盤として「CYNEX（Cybersecurity Nexus：サイネックス）」を構築する予定であることがNICTから発表されている*7（**図5**）。

4. おわりに

我が国の社会経済活動においては、2020年以降、COVID-19の感染拡大という未曾有の事態に対してあらゆる手段を用いた対応を迫られる中、時間や距離の壁を越えることを可能にするICTの役割はこれまで以上に大きくなり、ICTを安全・安心に利用するためのサイバーセキュリティの重要性がますます高まることが想定される。

総務省ではこのような状況も踏まえつつ、安全・安心な社会を実現するために、「IoT・5Gセキュリティ総合対策2020」に基づき、内閣サイバーセキュリティセンター（NISC）や経済産業省をはじめ、関係する各府省庁との連携の下、サイバーセキュリティの更なる強化に取り組んでいく。

なお、本稿では紙面の都合上、「IoT・5Gセキュリティ総合対策2020」の主要な内容を一部に限定して紹介させていただいた。その他の部分も含めてご関心がある方は、以下のウェブサイトに掲載されている「IoT・5Gセキュリティ総合対策2020」をご覧いただければ幸甚である。

▼「IoT・5Gセキュリティ総合対策2020」の公表（2020年7月17日）
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html

*7 サイバーセキュリティタスクフォース第28回会合資料「サイバーセキュリティ統合知的・人材育成基盤 CYNEXの構築について」
https://www.soumu.go.jp/main_content/000733733.pdf