「ICTサイバーセキュリティ総合対策2021」に基づく総務省の取組み

総務省　サイバーセキュリティ統括官室 参事官補佐　廣瀬（ひろせ）　一朗（いちろう）

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）では、今後、総務省が取り組むべきサイバーセキュリティ政策に関する提言として、2021年7月29日に、「ICTサイバーセキュリティ総合対策2021」（以下、総合対策2021）を取りまとめ、公表した。本稿では、総合対策2021に基づく総務省の取組みについて、ご紹介する。

1. 総務省サイバーセキュリティタスクフォースについて

総務省では、2017年1月、東京オリンピック・パラリンピック競技大会を控えて、サイバーセキュリティに係る課題を整理し、情報通信分野において講ずべき対策などを幅広い観点から検討し、必要な方策を推進することを目的として、有識者会議である「サイバーセキュリティタスクフォース」を設置した（事務局は、サイバーセキュリティ統括官室）。

これまで、サイバーセキュリティタスクフォースは、2017年9月に「IoTセキュリティ総合対策」を、2019年8月に「IoT・5Gセキュリティ総合対策」を、2020年7月に「IoT・5Gセキュリティ総合対策2020」を策定してきた。今回の総合対策2021は、これらに次いで、第4次の提言となる。

2. 背景及び状況変化

2020年初以来のコロナ禍においては、テレワークの普及などの社会のデジタル化が急速に進展する一方で、行政サービスにおける様々な課題が明らかになった。これらを背景に、社会全体のデジタル・トランスフォーメーション（DX）の推進が重要な政策課題と改めて認識され、「デジタル社会の実現に向けた改革の基本方針」（2020年12月25日閣議決定）においては、デジタル社会のビジョンとして「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」を掲げ、このような社会の実現に向けて、「誰一人取り残さない、人に優しいデジタル化」を目指すこととした。2021年9月1日には、行政を含む社会全体のデジタル改革やDXを強力に進めるための司令塔としてデジタル庁が設置されている。

一方で、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、我が国のサイバーセキュリティ施策の推進に当たっての基本的方針等を定める「サイバーセキュリティ戦略」についても、3年ぶりの改定の検討が進められた。その結果、2021年9月28日に閣議決定されたサイバーセキュリティ戦略においては、サイバー空間があらゆる主体が参画する公共空間へと進化する中で、「誰一人取り残さない」

タスクフォース構成員（敬称略）

	鵜飼　裕司	株式会社FFRIセキュリティ　代表取締役社長
	宇佐美　理	日本テレビ放送網株式会社ICT戦略本部　専任部長
	岡村　久道	英知法律事務所 弁護士、京都大学大学院医学研究科　講師
（座長）	後藤　厚宏	情報セキュリティ大学院大学　学長
	小山　覚	NTTコミュニケーションズ情報セキュリティ部　部長、ICT-ISAC　ステアリング・コミッティ運営委員長
	篠田　佳奈	株式会社BLUE　代表取締役
	園田　道夫	国立研究開発法人情報通信研究機構（NICT）、ナショナルサイバートレーニングセンター　センター長
	辻　伸弘	SBテクノロジー株式会社　プリンシパルセキュリティリサーチャー
	戸川　望	早稲田大学理工学術院　教授
（座長代理）	徳田　英幸	国立研究開発法人情報通信研究機構（NICT）理事長、慶應義塾大学 名誉教授
	中尾　康二	ICT-ISAC　顧問、国立研究開発法人情報通信研究機構（NICT）　主管研究員
	名和　利男	サイバーディフェンス研究所　専務理事/上級分析官
	林　紘一郎	情報セキュリティ大学院大学前学長・名誉教授
	藤本　正代	情報セキュリティ大学院大学　教授、GLOCOM客員研究員
	吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院　准教授
	若江　雅子	株式会社読売新聞東京本社　編集委員

■図1.　サイバーセキュリティタスクフォースの構成員

サイバーセキュリティの確保（“Cybersecurity for All”）に向けた取組みを進める必要があるとの考え方の下、「DXとサイバーセキュリティの同時推進」「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」「安全保障の観点からの取組強化」を通じて「自由、公正かつ安全なサイバー空間」を確保するとの方向性が示された。

総務省が所管するIoTや5Gを含むICT（情報通信技術）に係るインフラやサービスは、デジタル社会や「自由、公正かつ安全なサイバー空間」の基盤となるものであり、国民一人ひとりがICTを安心して活用できるよう、ICTサイバーセキュリティを確保することが、いわば不可欠の前提としてますます重要になっている。

これらの状況変化や2020年の提言の公表後のサイバーセキュリティタスクフォースにおける議論を踏まえて、「IoT・5Gセキュリティ総合対策2020」を改定し、新たな施策を盛り込む形で総合対策2021を策定した。

以下では、重点的に推進すべき施策として、

①電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進

②COVID-19への対応を受けたセキュリティ対策の推進

③デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策の推進

④サイバーセキュリティ情報に関する産学官での連携・共有等の促進

⑤横断的施策

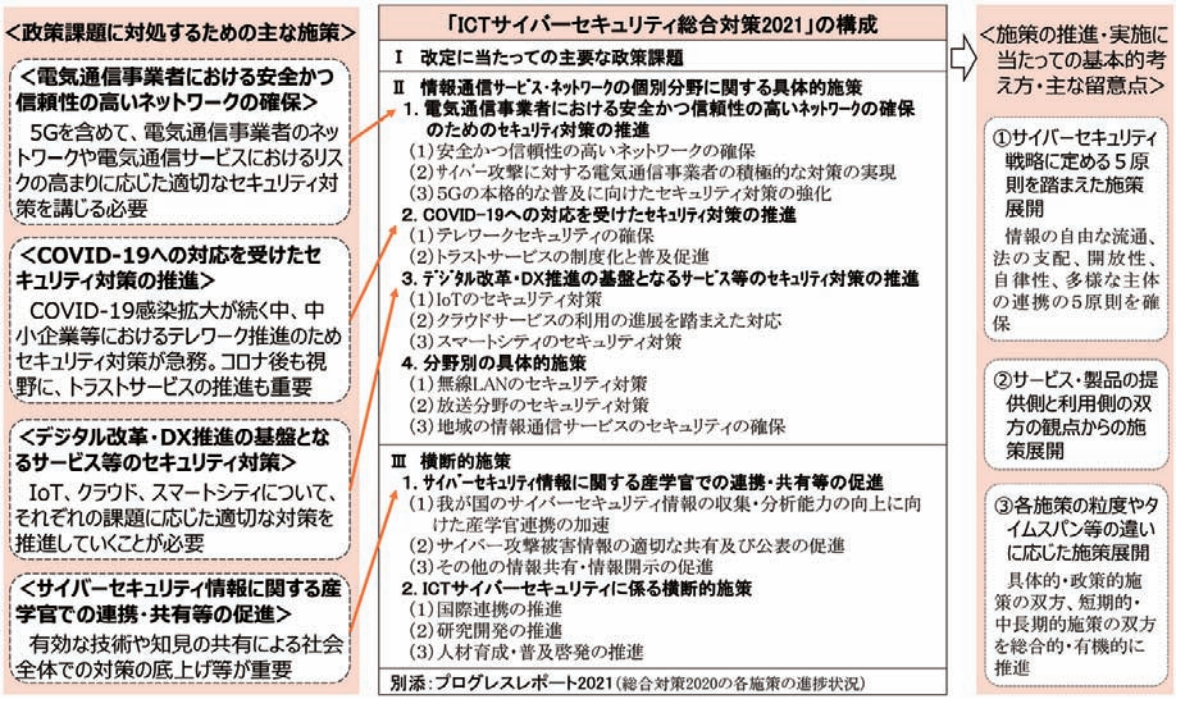
の5つに分類して、総合対策2021に基づく総務省の施策を解説する。

3. 電気通信事業者における安全かつ信頼性の高いネットワークの確保のためのセキュリティ対策の推進

社会全体のデジタル改革やDXの進展とともに、国民の生活や経済活動に必要な多くのやり取りが、電気通信事業者のネットワークやサービスを通じて行われることとなる。そのため、デジタル社会の実現に向けて、国民一人ひとりがICTを安心して活用していくためには、今後本格的な展開が見込まれる5Gのセキュリティ対策の強化も含め、電気通信事業者のネットワークにおけるリスクの高まりに応じた適切なセキュリティ対策を講じ、電気通信事業者における安全かつ信頼性の高いネットワークを確保していくことが重要である。

(1) 電気通信事業者のガバナンス確保の在り方についての検討

電気通信事業者のネットワークへのサイバー攻撃、委託



■図2.「ICTサイバーセキュリティ総合対策2021」の概要（2021年7月公表）～Ⅰ改定に当たっての主要な政策課題～

先や内部からの情報漏えいといったリスクに対して適切かつ積極的な対策を講じることにより、ネットワークやサービスの安全・信頼性を確保し、ユーザが安心してICTを利用できる環境を確保することが必要であることから、2021年5月、総務省において、「電気通信事業ガバナンス検討会」を設けた。検討会においては、電気通信事業におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の在り方、具体的には、電気通信事業に係る情報の漏えい・不適正な取扱い等、通信サービス停止といったリスクへの対策としての事業者における利用者情報の適正管理の在り方等について検討を行っている[*1]。

(2) 電気通信事業者による積極的なサイバーセキュリティ対策

IoTのセキュリティ対策としては、これまで端末側の対策として、電気通信事業法（昭和59年法律第86号）における端末設備等規則（昭和60年郵政省令第31号）へのセキュリティ要件の導入や、パスワード設定に不備のあるIoT機器やマルウェアに感染している機器の利用者への注意喚起（NOTICE）といった取組みを実施してきた。こうした対策をより実効的なものにするためには、トラフィックが通過するネットワーク側において、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、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（ISP）が管理するネットワークにおいて、高度かつ機動的な対処を実現するための方策として、ISPが自らトラフィックの流れ（フロー情報）を把握・分析して攻撃元のC&Cサーバ（マルウェアに感染した端末に対して指令を与えるサーバ）を検知し、検知したC&Cサーバに関する情報を電気通信事業者間で共有し、サイバー攻撃の予兆を捉えて早期に対処することについて、通信の秘密との関係について整理を行っている[*2]。また、C&Cサーバ検知・共有に当たっての技術面・運用面の課題を把握・整理するための実証事業を行うことを検討している。

このほか、5Gセキュリティに関して、制度面におけるサプライチェーンリスク対策、不正な機能や脆弱性の技術検証などの既存の施策を着実に遂行し、我が国の基幹的重要インフラである5G通信ネットワークの安全性と信頼性を確実なものとすることとしている。

4. COVID-19への対応を受けたセキュリティ対策の推進

総務省においては、2020年7月の「IoT・5Gセキュリティ総合対策2020」策定・公表以降、COVID-19への対応を受けたテレワークシステム等のICT利用の促進のためのセキュリティ対策を進めてきた。一方で、COVID-19の感染拡大が続く中、特に中小企業等におけるテレワークの普及・定着にはいまだ課題もあるところであり、その対策の強化は急務である。また、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は、COVID-19後のいわゆるニューノーマルの社会においても同様であり、中期的な視点も視野も入れつつ、引き続きCOVID-19への対応を受けたセキュリティ対策に取り組むことが重要である。

(1) テレワークのセキュリティ確保

テレワークにおいては、インターネット経由でオフィスのネットワークへアクセスしたり、私用端末を利用したりすることも想定されることから、これらに対応したセキュリティ対策を実施する必要がある。実際に、テレワーク導入企業に対するアンケートでもセキュリティの確保が最大の課題とされている。

こうした状況を踏まえ、総務省では、「テレワークセキュリティガイドライン」や、セキュリティの専任担当がいない場合や、担当が専門的な仕組みを理解していない場合でも、最低限のセキュリティが確実に確保されることに焦点を絞った「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）」等を策定し、2021年5月に最新のセキュリティ動向等を踏まえた改定を実施した。これらガイドライン類について、関係省庁や関連団体・企業等とも連携するとともに、オンラインコンテンツ（動画等）の活用も検討しつつ、

*1　2021年11月20日現在、11回にわたって検討会を開催している。資料などは総務省ホームページ参照。https://www.soumu.go.jp/main_sosiki/kenkyu/sd_governance/index.html

*2　具体的には、2021年10月1日の「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」において、第4次取りまとめ案を決定し、ISPにおけるフロー情報分析によるC&Cサーバの検知について正当業務行為と、検知結果の共有について通信の秘密の保護規定に抵触しないと整理した。取りまとめについては、意見募集を経て、2021年11月24日に公表した。資料などは総務省ホームページ参照。https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000130.html

テレワーク実施企業やテレワーク勤務者に広く周知していく。

(2) トラストサービスの推進

トラストサービスについては、タイムスタンプに関して、2021年4月に、時刻認証業務の認定に関する規程（令和3年総務省告示第146号）に基づき、国による認定制度を整備した。また、eシールに関しても、今後、我が国のeシールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準等について整理したeシールに係る指針を作成し、2021年6月に公表した。今後は、これまでに整備した国による認定制度を適切かつ確実に運用するとともに、政府におけるデータ戦略、とりわけトラストサービスの基盤となる枠組みの創設に向けた検討の動向を踏まえ、eデリバリー（電子的な配達証明付き内容証明郵便に相当）等、トラストサービスの更なる利用の拡大に向けた検討を行う。

5. デジタル改革・DX推進の基盤となるサービス等のセキュリティ対策の推進

社会全体のデジタル改革やDXは、IoTやクラウドサービス等のサービスの利用や、それらのサービスを組み合わせたユースケースであるスマートシティの構築・運営を通じて進展すると考えられる。今後、デジタル社会の実現に向けた改革を進め、ICTの活用を促進していくためには、このようなデジタル改革・DX推進の基盤となるサービス等における課題に応じた適切なセキュリティ対策を講じ、これらのサービス等を国民一人ひとりが安心して利用できる安全な環境を整備していくことが重要である。

(1) IoTのセキュリティ対策

IoTのセキュリティ対策については、NOTICEやNICTER注意喚起等の既存の取組みを引き続き継続するとともに、NOTICEについては、増減要因の詳細分析や調査対象ポートの拡大等の調査の詳細化・高度化を行うとともに、IoT機器製造事業者との連携や、IoT機器利用者への一般的な周知広報等を通じたIoT機器のセキュアな設定についての周知啓発を進める。

(2) クラウドサービスのセキュリティ対策

クラウドサービスにおいては、一般的に「責任共有モデル」が採用されており、クラウドサービス事業者と利用者・調達者の共通の認識の下、それぞれの管理権限に応じた責任分担を行うものであることを踏まえ、クラウドサービス利用時の設定ミスを防止・軽減し、安全に安心してクラウドサービスを利用できる環境を整えるため、発生している設定ミスやそれに起因する事故、クラウドサービス事業者における取組状況等を把握しつつ、クラウドサービス事業者における取組みを促す方策を検討していく。

(3) スマートシティのセキュリティ対策

スマートシティのセキュリティ確保のため、総務省において、2021年6月、「スマートシティセキュリティガイドライン（第2.0版）」を公表した。このガイドラインを政府が実施するスマートシティ関連事業における要件として活用するなど、その普及を図り、また、国際標準化も視野に、国際的に発信していく。

6. サイバーセキュリティ情報に関する産学官での連携・共有等の促進

デジタル改革・DX推進の前提としてサイバーセキュリティを確保するためには、サイバー攻撃等に関する情報の収集・分析等を行い、有効な技術や知見を生み出すとともに、それらを関係者間で共有し、社会全体でのセキュリティ対策の底上げを図ることが有用である。そのため、産学官連携してのサイバー攻撃等に関する情報の収集・分析等や適切な共有・公表等を進めることが重要である。

(1) 統合知的・人材育成基盤の構築

情報通信技術を専門とする我が国唯一の国立研究開発法人であるNICT（情報通信研究機構）では、NICTが有する技術・ノウハウや情報を中核として、我が国のサイバーセキュリティ情報の収集・分析とサイバーセキュリティ人材の育成における産学の結節点となる「サイバーセキュリティ統合知的・人材育成基盤」（CYNEX）を構築中である。得られた情報の効果的な共有と適切な管理、育成人材の質の担保やスキルアップの階層化等にも留意しつつ、早期の本格稼働に向けてシステム基盤構築・運営環境整備を引き続き進める。

(2) 攻撃被害時の情報共有の推進

サイバー攻撃の被害を受けた場合に、被害組織においては、共有した情報を端緒に被害を受けたのが自組織であることが特定されて二次被害が発生する懸念があることや、いかなる情報をどのようなタイミングで外部専門機関等に共有すればよいのかが判然としないことなどで、外部専門機関等への情報共有が適切に進んでいない。このため、

今後、いかなる情報をどのようなタイミングで外部専門機関等に提供すれば、自組織に不都合が発生する状況を避けつつ社会的に求められる情報共有ができるのかをまとめた、ガイダンスを作成・発信していく。

7. 横断的な施策

(1) 国際連携

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。そのため、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情報共有や国際的なルール作りを多様なルートで進めつつ、情報通信サービス・ネットワーク分野の具体的な施策、研究開発、人材育成・普及啓発、情報共有・情報開示の取組みなどを進めていく必要がある。例えば、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）における実践的サイバー防御演習「CYDER」等の実施を通じたASEANのセキュリティ人材の育成支援、国内の産業分野ごとに設立されるサイバーセキュリティに関する脅威情報等を共有・分析する組織であるISAC（Information Sharing and Analysis Center）における国際的なISAC間等の連携促進、ISO/IEC及びITU-TにおけるIoTセキュリティに係る国際標準化の議論への積極的な貢献などを行う。

(2) 研究開発

サイバー攻撃の対象の拡大、攻撃手法・能力の巧妙化・大規模化に対応するには、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。このため、NICTや民間企業等と連携しつつ、研究開発の成果が民間企業等への技術移転によって広く普及し、社会実装が進むことを視野に入れながら、サイバーセキュリティ対策に係る研究開発を効果的に推進する必要があることから、NICTにおけるサイバーセキュリティ分野の基礎的・基盤的な研究開発、IoT機器のセキュリティ対策技術の研究開発等を引き続き推進する。

(3) 人材育成

NICTの「ナショナルサイバートレーニングセンター」を通じた、実務者層・技術者層及び若年層を対象とした人材育成施策について、まず、国の機関等、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習（CYDER）を引き続き実施するとともに、未受講の地方公共団体の受講の促進や、オンライン演習の実施についても積極的に進めていく。また、25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出し得る最先端のセキュリティ人材（セキュリティイノベーター）を育成する「SecHack365」についても、我が国における高度セキュリティ人材の育成のため、引き続き、取組みを進める。

(4) 地域におけるコミュニティ形成

地域においては、首都圏と比較してサイバーセキュリティに関する情報格差が存在するほか、経営リソースの不足等の理由により、単独で十分なセキュリティ対策を取ることが難しかったり、セキュリティ対策の必要性を認識するに至らなかったりするケースが存在する。このため、各種民間企業、行政機関、教育機関、関係団体等が、顔の見える関係の中で、イベント等の継続開催による地域のセキュリティ意識向上・人材育成や、国や専門家を招へいした情報提供が持続的・自発的に実施されるコミュニティ（地域SECUNITY）の形成を推進する。

8. 今後の課題

サイバーセキュリティタスクフォースは、前述のとおり、2017年に、東京オリンピック・パラリンピック競技大会に向けたサイバー攻撃の増加を見据えて初めて開催された。おりしも、2021年の総合対策2021は大会期間中に策定され、9月に大会が終了したが、幸いにも、大会の運営に支障を生じるようなサイバー攻撃は確認されていない[*3]。とはいえ、国内企業へのサイバー攻撃による情報漏えい事案は相次いでおり、総務省が所管する通信・放送を含む重要インフラへのサイバー攻撃により国民生活に大きな影響が及ぶ事態も懸念される。今後も、サイバー攻撃の複雑化・巧妙化は続くことが想定されることから、引き続き、気を緩めることなく対策を継続することが求められる。

総務省としては、本稿において紹介したように、総合対策2021に基づく取組みを、関係省庁、事業者等とも連携しつつ、引き続き積極的に推進していきたいと考えている。

＊3　第31回サイバーセキュリティ戦略本部（2021年9月27日）資料7参照。https://www.nisc.go.jp/conference/cs/index.html