第5節 サイバーセキュリティ対策の推進

1 サイバーセキュリティ対策に関する取組方針の検討

1 政府の取組

世界的規模で深刻化するサイバーセキュリティ上の脅威の増大を背景として、我が国におけるサイバーセキュリティ政策の基本理念等を定めた「サイバーセキュリティ基本法」が2014年（平成26年）11月に成立した。2015年（平成27年）1月、同法に基づき、サイバーセキュリティ政策に係る政府の司令塔として、内閣の下にサイバーセキュリティ戦略本部が新たに設置された。

同本部における検討を経て、同年9月に「サイバーセキュリティ戦略*1」が閣議決定されており、同戦略では、監視対象の拡大等、「政府機関全体としてのサイバーセキュリティを強化するため、独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等における対策の総合的な強化」や、「実践的な訓練・演習の実施等の取組」等を推進することが掲げられている。

その後政府は、サイバー空間とフィジカル（実）空間を高度に融合させることにより、経済的発展と社会的課題の解決を両立する人間中心の社会を目指す方針を決定し、経済社会が、人々に豊かさをもたらし、持続的に発展するためには、その基盤であるサイバー空間のサイバーセキュリティが確保されつつ、自律的・持続的に進化・発展していく必要があるとされた。こうした認識の下、東京2020大会等の国際的なイベントを控えていることを見据え、2020年（令和2年）以降の目指す姿を念頭に置きつつ、サイバーセキュリティに係る我が国としての基本的な立場や在り方を明らかにするとともに、今後3年間の諸施策の目標及び実施方針を国内外に明確にするため、新たな「サイバーセキュリティ戦略*2」が2018年（平成30年）7月に閣議決定された。同戦略では、目指すサイバーセキュリティの在り方を「サイバーセキュリティエコシステム」と名づけ、3つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進することとしている。また、同戦略の下、実施した具体的な施策の実施状況等の年次報告と、次年度に実施する具体的な施策等の年次計画をそれぞれ毎年取りまとめており、2020年度については「サイバーセキュリティ2020」が2020年（令和2年）5月に本部決定された。

また、サイバーセキュリティに対する脅威が一層深刻化する中、我が国におけるサイバーセキュリティの確保を促進し、東京2020大会の開催に万全を期すため、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策を推進する必要があることから、「サイバーセキュリティ基本法の一部を改正する法律」が2018年（平成30年）12月に成立し、同法に基づいて、官民の多様な主体が相互に連携して情報共有を図り、必要な対策等について協議を行うための協議会として、新たに「サイバーセキュリティ協議会」が2019年（平成31年）4月に創設された。同協議会は、国の行政機関、地方公共団体、重要インフラ事業者、サイバー関連事業者、教育研究機関、有識者等で構成され、構成員には秘密保持義務及び協議会への情報提供の協力義務が課されることとされており、専門機関等から得られた脅威情報を戦略的かつ迅速に共有し、サイバーセキュリティの確保に取り組んでいく。

2 総務省の取組（サイバーセキュリティタスクフォース）

総務省においては、2017年（平成29年）1月から、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」（現座長：後藤厚宏　情報セキュリティ大学院大学　学長）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」を取りまとめ、公表した。同総合対策では、「(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推進」、「(4) 人材育成の強化」、「(5) 国際連携の推進」の5つの観点から、今後取り組むべき具体的な施策をまとめている。2019年（令和元年）5月には、同対策の進捗状況及び今後の取

＊1　サイバーセキュリティ戦略：https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf
＊2　新たな「サイバーセキュリティ戦略」：https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf

組について整理した「IoTセキュリティ総合対策 プログレスレポート2019[*3]」を公表した。さらに、「IoTセキュリティ総合対策」策定・公表後の様々な状況変化などを踏まえつつ、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について検討を行い、2019年（令和元年）8月に「IoT・5Gセキュリティ総合対策[*4]」を公表した。

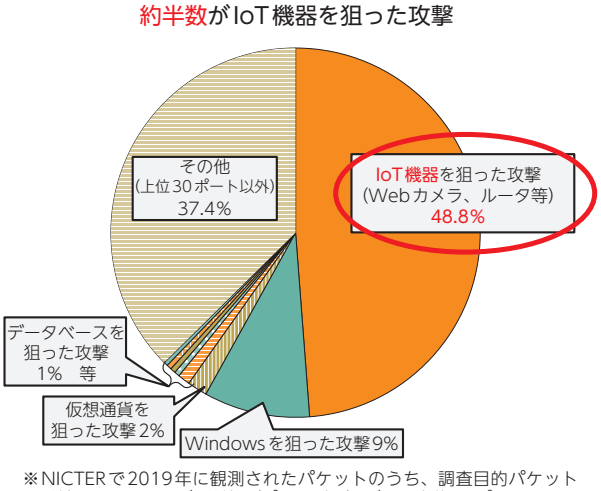
その後も同タスクフォースでは、東京2020大会を控える中、取り組むべき施策の総点検を行うとともに、新たな課題への対応や施策展開の加速化を図るため、サイバーセキュリティに関する課題や必要な方策について短期的及び中長期的な観点から議論を継続してきたところである。2020年（令和2年）1月には、東京2020大会に向けた対処として短期的な観点から早急に取り組むべき事項を整理した、「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項［緊急提言］[*5]（以下「緊急提言」という。）を公表した。その上で、2020年（令和2年）7月には、これまでの短期的・中長期的な観点の議論や緊急提言の内容、さらには新型コロナウイルス感染症への対応等を踏まえつつ、「IoT・5Gセキュリティ総合対策」について、必要な改定を行い、①COVID-19への対応を受けたセキュリティ対策の推進、②5Gの本格開始に伴うセキュリティ対策の強化、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、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の4点を主要な政策課題として盛り込んだ、「IoT・5Gセキュリティ総合対策2020」[*6]を公表した。

2 サイバーセキュリティ対策の強化

1 IoT等に関する取組

社会基盤としてのIoT化が進展する一方で、IoT機器については、管理が行き届きにくい、機器の性能が限られ適切なセキュリティ対策を適用できないなどの理由から、サイバー攻撃の脅威にさらされることが多く、その対策強化の必要性が指摘されている。情報通信研究機構（NICT）が運用するサイバー攻撃観測網（NICTER）が2019年（令和元年）に観測したサイバー攻撃関連通信のうち、約半数がIoT機器を狙ったものであるという結果が示されている（図表6-5-2-1）。実際に、米国では、2016年（平成28年）10月、マルウェアに感染したIoT機器が踏み台となり、大規模なDDoS攻撃が発生し、一部サイトにアクセスできなくなる等の障害が発生した（図表6-5-2-2）。

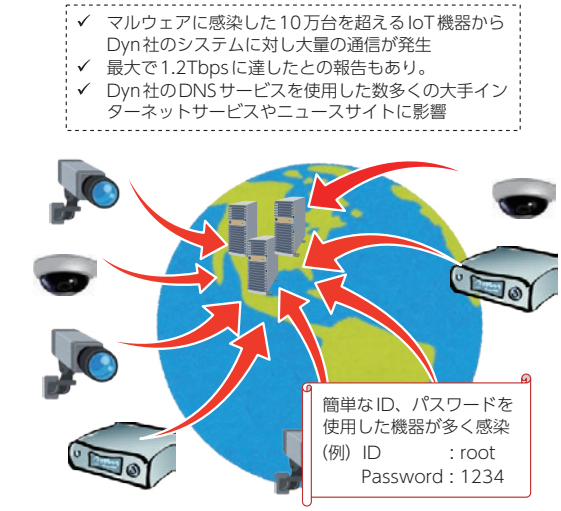
図表6-5-2-1　NICTERによる観測結果



※NICTERで2019年に観測されたパケットのうち、調査目的パケット以外についてサービス種類（ポート番号）ごとに上位30ポートまでを分析したもの。

※IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

図表6-5-2-2　「Mirai」による大規模サイバー攻撃



＊3　IoTセキュリティ総合対策 プログレスレポート2019：https://www.soumu.go.jp/main_content/000623344.pdf
＊4　IoT・5Gセキュリティ総合対策：https://www.soumu.go.jp/main_content/000641510.pdf
＊5　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］：https://www.soumu.go.jp/main_content/000666221.pdf
＊6　IoT・5Gセキュリティ総合対策2020：https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html

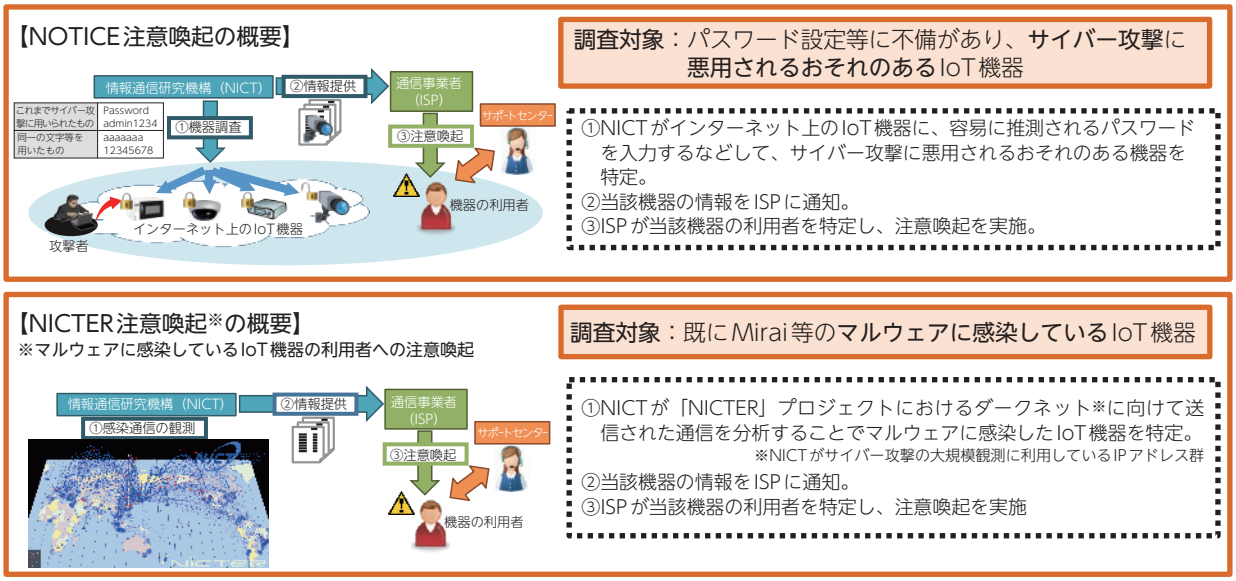
こうした状況を踏まえ、パスワード設定等に不備のあるIoT機器について対策を行うため、総務省は、「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案」を2018年（平成30年）3月に国会へ提出、同改正法は同年5月に公布、同年11月に施行された。

同改正法に基づき、総務省及びNICTは、インターネット・サービス・プロバイダ（ISP）と連携し、2019年（平成31年）2月から「NOTICE（National Operation Towards IoT Clean Environment）」と呼ばれる取組を実施している。これは、①NICTがインターネット上のIoT機器に対して、例えば「password」や「123456」等のこれまでにサイバー攻撃に用いられたパスワードや同一の文字列等を用いたような容易に推測されるパスワードを入力するなどにより、サイバー攻撃に悪用されるおそれのある機器を特定する。②その特定した機器の情報をNICTからISPに通知する。③通知を受けたISPがその機器の利用者を特定し注意喚起を行う、といった一連の取組である（図表6-5-2-3）。

また、NOTICEと並行して2019年（令和元年）6月から、総務省、NICT、一般社団法人ICT-ISAC及びISP各社が連携して、既にマルウェアに感染しているIoT機器の利用者に対し、ISPが注意喚起を行う取組を実施している。本取組は、NICTが前述のNICTERで得られた情報を基にマルウェア感染を原因とする通信を行っている機器を検知し、ISPにおいて当該機器の利用者を特定することにより行っている（図表 6-5-2-3）。

2020年（令和2年）3月時点でこれらの取組に参加しているISPは50社であり、当該ISPが保有する約1.1億の国内IPv4アドレスに対して調査を実施した。NOTICEについては、おおむね月に1回の調査を実施しており、調査対象となったIPアドレスのうち、パスワード等が入力可能であったものが直近での調査において約100,000件であり、このうち、特定のパスワード等の入力によりログインでき、注意喚起の対象となったものは延べ2,249件となっている。また、マルウェアに感染しているIoT機器の利用者への注意喚起については、NICTERにより検知した情報を日ごとにISPに通知しており、その1日当たりの平均件数は162件となっている。

図表6-5-2-3　NOTICE及びNICTERに関する注意喚起の概要



また、IoT機器を含む端末設備のセキュリティ対策に当たっては、製造業者にセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、対策がとられた機器の市場への展開を促進させることが重要であることから、今後製品化されるIoT機器がパスワード設定の不備等によりサイバー攻撃に悪用されないようにする対策として、2019年（平成31年）3月にIoT機器の技術基準にセキュリティ対策を追加するため、端末設備等規則を改正し、2020年（令和2年）4月に施行した。さらに、同規則の各規定等に係る端末機器の基準認証に関する運用について明確化を図る観点から、2019年（平成31年）4月に「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第1版）」を策定・公表している。

そのほかサイバー攻撃対策に資する取組として、上述の改正法により改正された電気通信事業法に基づき、2019年（平成31年）1月に、電気通信事業者がDDoS攻撃等のサイバー攻撃への対応を共同して行うため、サイバー攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関である「認定送信型対電気通信

設備サイバー攻撃対処協会」として、一般社団法人ICT-ISACを認定し、情報共有を促進するための体制整備を図っている。

2　人材育成に関する取組

我が国のサイバーセキュリティ人材は質的にも量的にも不足しており、その育成は喫緊の課題である。サイバーセキュリティ戦略（2018年（平成30年）7月27日閣議決定）においても「産学官が連携して人材の需要や人材育成施策に関する情報共有等の連携を図りつつ、人材育成・確保を強化していく。」と言及されているとおり、政府一丸となってサイバーセキュリティ人材の育成に取り組んでいる。

巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、2017年（平成29年）4月より、NICTの「ナショナルサイバートレーニングセンター」において、サイバーセキュリティ人材育成の取組（CYDER、サイバーコロッセオ、SecHack365）を積極的に推進している。

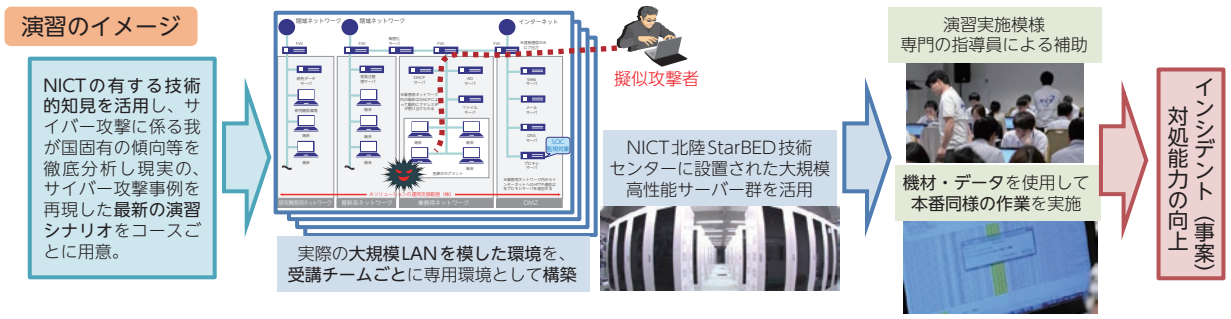
CYDERは、国の機関、地方公共団体、独立行政法人及び重要インフラ事業者等の情報システム担当者を対象とした実践的サイバー防御演習である。受講者は、チーム単位で演習に参加し、組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴ってサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験する。2019年度（令和元年度）は、全国47都道府県で全105回の演習を実施し、3,090名が受講した。2020年度（令和2年度）も同規模で実施予定である（図表6-5-2-4）。

サイバーコロッセオは、東京2020大会に向けた大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習である。大会に関わるシステムを忠実に再現した仮想のネットワーク環境上で、攻防型演習等による攻撃・防御手法の検証及び訓練を実施し、2019年度（令和元年度）は延べ193名が受講した。さらに、2018年度（平成30年度）からは、講義形式によりセキュリティ関係の知識や技能を学ぶコロッセオカレッジを開設しており、2019年度（令和元年度）は延べ992名が受講した。2020年度（令和2年度）については、大会延期の状況等に鑑みた上で、組織委員会とも緊密な連携を図りながら事業を実施する予定である。

SecHack365は、未来のセキュリティイノベーターの創出に向けて、25歳以下のICT人材を対象に、NICTの持つ実際のサイバー攻撃関連データを活用し、第一線で活躍する研究者・技術者が、セキュリティ技術の研究・開発等を1年かけて継続的かつ本格的に指導するプログラムである。2019年度（令和元年度）は15歳から24歳の45名が1年間のプログラムを修了した。2020年度（令和2年度）以降も、育成プログラムの質の向上を図りつつ、同規模で実施予定である。

また、特に人口減少が急速に進む地方において、サイバー攻撃に対処可能な人材の育成・確保は大きな課題となっていることから、2018年（平成30年）12月からサイバーセキュリティタスクフォースの下に「サイバーセキュリティ人材育成分科会」を開催した。同分科会の取りまとめも踏まえ、2019年度（令和元年度）は、「地域のセキュリティリーダーの育成」、「地域でのセキュリティ人材のシェアリング」及び「地域における人材エコシステムの形成」について、それぞれ対象地域を特定した上でその有効性を確認するための実証的調査を実施した。この調査結果を踏まえ、2020年度（令和2年度）は、地域で自立したサイバーセキュリティ人材の育成が行われる仕組みとなるよう実証的調査を継続するとともに、その成果を調査対象地域以外でも活用できるよう横展開を進めていく。

図表6-5-2-4　実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）



3　民間企業等のセキュリティ対策の促進に関する取組

IoT産業等の関連産業等の成長を見据え、民間企業におけるセキュリティ投資を促進するため、経済産業省と共同で税制改正要望を行い、2018年度（平成30年度）税制改正において、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入に対して、支援措置を講じる「情報連携投資等の促進に係る税制」（コネクテッド・インダストリーズ税制）を創設し、説明会等を通じて同税制の周知を行い、活用を促進した。（図表6-5-2-5）。なお、令和2年度税制改正において、コネクテッド・インダストリーズ税制は、2020年（令和2年）3月31日をもって廃止された。

図表6-5-2-5　情報連携投資等の促進に係る税制（コネクテッド・インダストリーズ税制）の概要

【計画認定の要件】
①データ連携・利活用の内容
・社外データやこれまで取得したことのないデータを社内データと連携
・企業の競争力における重要データをグループ企業間や事業所間で連携
②セキュリティ面
必要なセキュリティ対策が講じられていることをセキュリティの専門家（登録セキスペ等）が担保
③生産性向上目標
投資年度から一定期間において、以下のいずれも達成見込みがあること
・労働生産性：年平均伸率2%以上
・投資利益率：年平均15%以上

課税の特例の内容

➢　認定された事業計画に基づいて行う設備投資について、以下の措置を講じる。

対象設備	特別償却	税額控除
ソフトウェア 器具備品 機械装置	30%	3% （法人税額の15%を限度）
		5%＊ （法人税額の20%を限度）

【対象設備の例】
データ収集機器（センサー等）、データ分析により自動化するロボット・工作機械、データ連携・分析に必要なシステム（サーバ、AI、ソフトウェア等）、サイバーセキュリティ対策製品　　等

最低投資合計額：5,000万円

※計画の認定に加え、平均給与等支給額の対前年度増加率≧3%を満たした場合。

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いるが、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ている。このため、2017年（平成29年）12月よりサイバーセキュリティタスクフォースの下に「情報開示分科会」を開催し、あくまで任意の取組であることを前提としつつ、民間企業のセキュリティ対策の情報開示に関する課題を整理し、その普及に必要な方策について検討を行った。本分科会における検討を踏まえ、2018年（平成30年）6月8日に「情報開示分科会報告書」を公表した。

同報告書を踏まえ、企業のサイバーセキュリティ対策に関する情報開示を行うに当たって参照可能な手引きの策定に着手し。2019年度（令和元年度）6月、「サイバーセキュリティ対策情報開示の手引き[*7]」を公表した。

4　国際連携に対する取組

サイバー空間はグローバルな広がりをもつことから、サイバーセキュリティの確立のためには諸外国との連携が不可欠である。このため、総務省では、サイバーセキュリティに関する国際的合意形成への寄与を目的として、各種国際会議やサイバー対話等における議論や情報発信・情報収集を積極的に実施している。

また、情報通信事業者等による民間レベルでの国際的なサイバーセキュリティに関する情報共有を推進するために、ASEAN各国のISPが参加するワークショップ、日本と米国のISAC（Information Sharing and Analysis Center）が意見交換するワークショップを引き続き開催した。2019年（令和元年）11月には、日本のICT-ISACと米国のIT-ISACが、サイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的とした覚書に署名した。このほか、ASEAN地域において、標的型攻撃対策ソリューションの適用性評価を行う実証実験を実施した。また、2017年（平成29年）12月の日ASEAN情報通信大臣会合[*8]の合意に基づき、2018年（平成30年）9月に日ASEANサイバーセキュリティ能力構築センター（AJCCBC：ASEAN Japan Cybersecurity Capacity Building Centre）をタイ・バンコクに設立した。現在、同センターにおいてASEAN各国の政府機関及び重要インフラ事業者を対象に実践的サイバー防御演習（CYDER）をはじめとするサイバーセキュリティ演習等を継続的に実施している。

＊7　サイバーセキュリティ対策情報開示の手引き：https://www.soumu.go.jp/main_content/000630516.pdf
＊8　日ASEAN情報通信大臣会合：https://www.soumu.go.jp/menu_news/s-news/01tsushin09_02000063.html

政策フォーカス

トラストサービスの在り方に関する検討状況

Society5.0においては、実空間とサイバー空間の融合がますます進み、実空間でのあらゆる営みがサイバー空間に置き換えられることとなる。その実現のためには、信頼してデータを流通できる基盤の構築が不可欠であり、データの改ざんや送信元のなりすましを防止し、データの信頼性を確保する仕組みであるトラストサービスの重要性が高まっている。このため、「プラットフォームサービスに関する研究会」の下「トラストサービス検討ワーキンググループ」（以下「トラストWG」）を開催し、2019年1月から同年11月まで合計15回の会合を重ね、事業者やユーザー企業などからユースケースなどのヒアリングなどを行いつつ、トラストサービスの制度化の在り方に関する検討を行ってきた。トラストWGにおいて、主に検討したトラストサービスは以下のとおりである（図表1）。

(1) 電子データを作成した本人として、ヒトの正当性を確認できる仕組み：　電子署名（個人名の電子証明書）
(2) 電子データがある時刻に存在し、その時刻以降に当該データが改ざんされていないことを証明する仕組み：タイムスタンプ
(3) 電子データを発行した組織として、組織の正当性を確認できる仕組み：　e シール（組織名の電子証明書）
(4) ウェブサイトが正当な企業等により開設されたものであるか確認する仕組み：　ウェブサイト認証
(5) IoT 時代における各種センサーから送信されるデータのなりすまし防止等のため、モノの正当性を確認できる仕組み：モノの正当性の認証
(6) 送信・受信の正当性や送受信されるデータの完全性の確保を実現する仕組み：e デリバリー

トラストサービスの活用は、企業内や企業間における紙のやりとりをデジタルに置き換え、データの積極的な利活用を可能とすることを通じて、大幅な業務効率化等の効果を実現するものと期待される。トラストWGでの試算（㈱三菱総合研究所による試算）では、トラストサービスの導入により、例えば経理系業務について、大企業1社あたり、10.2 万時間／月かかっている業務が、5.1 万時間／月へ、小企業1社あたり、502 時間／月かかっている業務が、151 時間／月へ大幅に削減されることが示された。また、トラストサービスの市場規模について、2018年における我が国の市場規模は合計94億円と推計され、成長ケースでは、1,035億円に達すると推計されとの試算が得られた（図表2）。

一方で、現状のトラストサービスの利用状況は、経団連デジタルエコノミー推進委員会所属企業へアンケートを実施した結果によれば、回答企業のうち、9割以上の社が文書・データ等の送受信や保存の場面で何らかの電子化を行っているものの、トラストサービス（電子署名・タイムスタンプ）を利用している社は半数程度にとどまっている。

トラストサービスの利用が一部にとどまっている要因として、ユーザー企業からは、上記アンケートやトラストWGでのヒアリングにおいて、例えば、タイムスタンプについては、民間の認定制度では、サービスの永続性に不安がある、安心して利用するには公的な認定制度によりサービスの信頼性を担保することが必要、国際的な通用性に不安があり国としての認定制度があれば、海外事業者とのやりとりにおける契約の迅速化が期待される、さらにeシールについては、eシールの利用が法令上認められる送付時の要件を満たすのかが不明確、利用するに当たっての手間やコストが課題といった指摘があった。

また、海外に目を転じてみれば、特に欧州において、デジタル・シングル・マーケットの基盤を支えるものとして、包括的なトラストサービスを規定するeIDAS（electronic IDentification, Authentication and trust Services Regulation）規則が制定されており、銀行・保険などの金融業界、不動産業界などで、主にKYC（オンラインでの顧客の本人確認）や契約・行政手続き（公共調達・入札）等の場面において、電子署名やタイムスタンプ等の利用が進んでいる。今後国際的なデータ流通がますます加速することが見込まれる中、トラストサービスの在り方の検討において、国際的な通用性の確保も重要な観点となっている。

こうした状況を踏まえ、2020年2月にプラットフォームサービスに関する研究会の最終報告書が取りまとめられ、一定のサービス提要の実態又は具体的なニーズの見込みがあり、利用者がより安心して利用できる環境の構築に向けた課題が顕在化しているタイムスタンプ、eシール及びリモート署名について、次の取組の方向性が示された。

① タイムスタンプについては、技術やサービス内容が確立されており、一般社団法人日本データ通信協会による民間の認定制度が15年間運用されてきたが、国の信頼性の裏付けがないことや、国際的な通用性への懸念が更なる普及を妨げている一因となっていることを踏まえ、国が信頼の置けるタイムスタンプサービス・事業者を認定する制度を創設することが適当である。
② eシールについては、新しいサービスであり、その導入促進のためには利用者が安心して利用するため、信頼

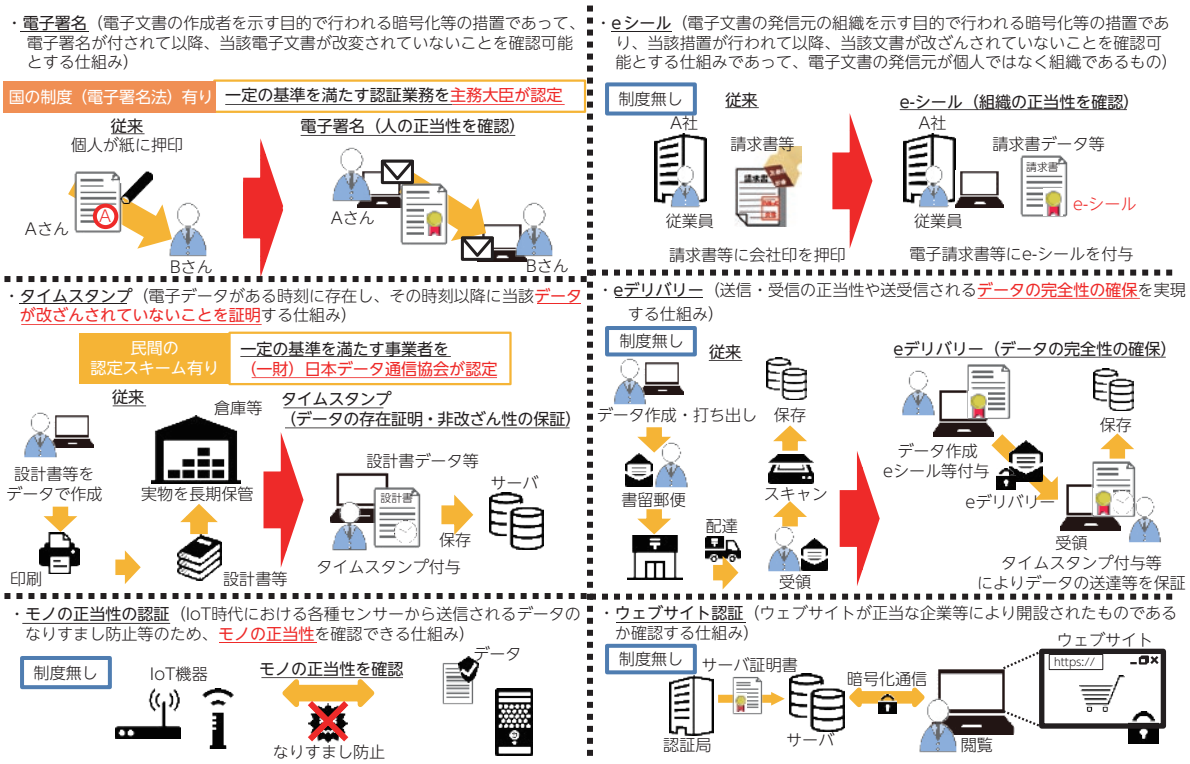
のおけるサービス・事業者に求められる技術上・運用上の基準の提示や、それを満たすサービス・事業者について利用者に情報提供する仕組みが重要である一方、サービス内容や提供するための技術などが確立されていないことから、国の関与の下、信頼の置けるサービス・事業者に求められる技術上・運用上の基準を策定し、これに基づく民間の認定制度を創設することが適当である。

③　今後利用拡大が期待されるリモート署名については、リモート署名に関する技術的なガイドラインが民間団体において策定されることを踏まえ、利用者によるリモート署名の円滑な利用を図るため、当該団体のガイドラインの策定・公表や自主的な適合性評価の仕組みの整備を受け、主務省（総務省、経済産業省、法務省）において、当該ガイドライン等の精査や当該ガイドライン及び適合性評価の仕組みの運用状況のモニタリングなどの取組を進めながら、リモート署名の電子署名法上の位置付けについて検討を行うことが適当である。

また、トラストサービスの普及を促進するためには、電子文書の送受信・保存について規定している法令を所管する省庁において、有効な手段として認められるトラストサービスの要件をそれぞれの省令・告示等で具体的に規定するよう、所管省庁に働きかけることが有効との提言もなされた。

最終取りまとめを踏まえ、総務省においては、「タイムスタンプ認定制度に関する検討会」を2020年3月、「組織が発行するデータの信頼性を確保する制度に関する検討会」を同年4月に立上げ、タイムスタンプ及びeシールのそれぞれについて、認定の仕組みに関する具体的な検討を行うこととしている。

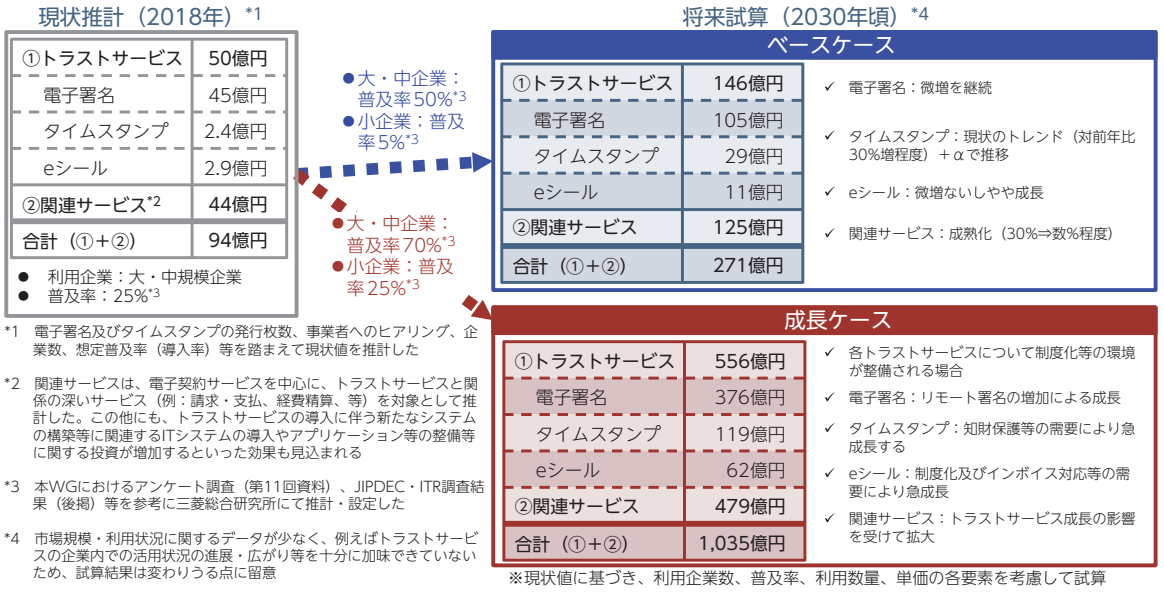
図表１　トラストサービスのイメージ



（「トラストサービス検討ワーキンググループ最終取りまとめ」より）

図表２　トラストサービス及び関連サービスの市場の現状推計と将来試算

● トラストサービス（電子署名、タイムスタンプ、eシール）の市場規模は2018年に約50億円と推計され、2030年頃には146億円（ベースケース）、556億円（成長ケース）に達すると試算された



*1　電子署名及びタイムスタンプの発行枚数、事業者へのヒアリング、企業数、想定普及率（導入率）等を踏まえて現状値を推計した

*2　関連サービスは、電子契約サービスを中心に、トラストサービスと関係の深いサービス（例：請求・支払、経費精算、等）を対象として推計した。この他にも、トラストサービスの導入に伴う新たなシステムの構築等に関連するITシステムの導入やアプリケーション等の整備等に関する投資が増加するといった効果も見込まれる

*3　本WGにおけるアンケート調査（第11回資料）、JIPDEC・ITR調査結果（後掲）等を参考に三菱総合研究所にて推計・設定した

*4　市場規模・利用状況に関するデータが少なく、例えばトラストサービスの企業内での活用状況の進展・広がり等を十分に加味できていないため、試算結果は変わりうる点に留意

（「トラストサービス検討ワーキンググループ最終取りまとめ」より）