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）7月に本部決定された。

同戦略においては、「今後3年間の諸施策の目標及び実施方針を示す」とされており、令和3年に計画期間を終えることを受け、次期のサイバーセキュリティ戦略（以下「次期戦略」という。）の策定に向けた検討が開始されている。2021年（令和3年）2月、「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方」が本部決定されるとともに、次期戦略の年度内の策定に向けたスケジュール案が示された。同年5月には「次期サイバーセキュリティ戦略の骨子」が本部決定された。

2 総務省の取組

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

＊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

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、「IoT・5Gセキュリティ総合対策2020[*6]」を公表した。2021年（令和3年）6月には、当面の主要な政策課題として、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・共有等の促進を掲げた「IoT・5Gセキュリティ総合対策2021（案）」に対する意見募集が実施された。

2 サイバーセキュリティ対策の強化

1 IoT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。実際にIoT機器を悪用したサイバー攻撃が発生しているほか、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2020年（令和2年）に観測したサイバー攻撃関連通信についても、約4割がIoT機器を狙ったものであるという結果が示されている。

こうした状況を踏まえ、IoT機器に対するサイバーセキュリティ対策を強化するため、2018年（平成30年）に情報通信研究機構法の一部改正を行った上で、総務省及びNICTでは、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」

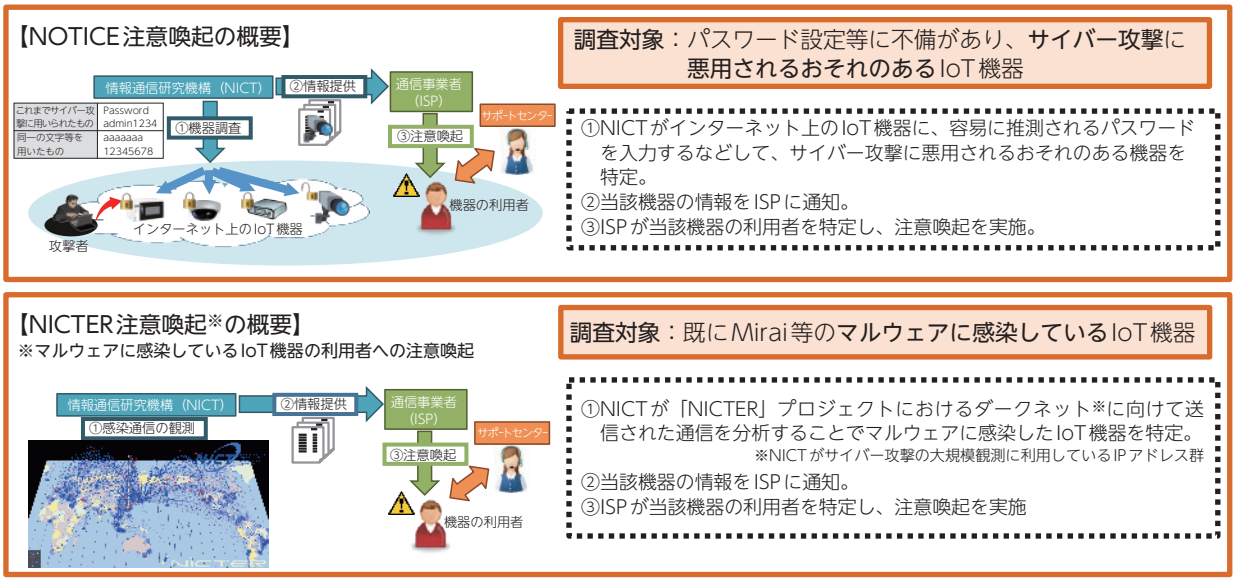
＊3　IoTセキュリティ総合対策 プログレスレポート2019：https://www.soumu.go.jp/main_content/000623344.pdf
＊4　IoT・5Gセキュリティ総合対策：https://www.soumu.go.jp/main_content/000641510.pdf
＊5　我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項［緊急提言］：https://www.soumu.go.jp/main_content/000666221.pdf
＊6　IoT・5Gセキュリティ総合対策2020：https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00126.html

等の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5-5-2-1）。

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。

NOTICEについては、おおむね月に1回の頻度で調査を実施している。2021年（令和3年）3月度は、取組に参加しているISP（66社）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、このうち注意喚起の対象となりISPに通知したものは約2千件であった。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190件となっている。なお、これら毎月の実施状況の詳細についてはNOTICEの特設Webサイトで周知している*7。

図表5-5-2-1　NOTICE及びNICTERに関する注意喚起の概要



2　人材育成に関する取組

サイバー攻撃が巧妙化・複雑化している一方で、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。そのため総務省では、NICTの「ナショナルサイバートレーニングセンター」を通じて、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

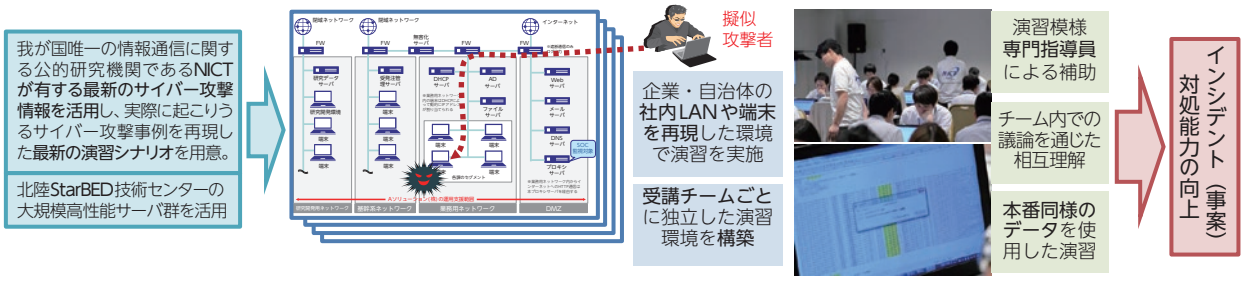
*7　NOTICE　実施状況：https://notice.go.jp/status

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（図表5-5-2-2）。2020年度（令和2年度）は、全国47都道府県で全106回の演習を実施し、延べ2,648名が受講した。2017年度（平成29年度）からの合計で11,413名が受講している。2021年度（令和3年度）は、従来からの初級及び中級の集合演習コースに加え、より高度なセキュリティ技術を習得可能な準上級のコースを追加するとともに、演習の全てをオンラインで実施するコースを追加した上で、従来と同規模で実施予定である

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サイバー攻撃を擬似的に発生させるなど、実機による攻防型演習等を行うことで攻撃対処手法を学ぶコロッセオ演習と、講義演習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、組織委員会とも緊密な連携を図りながら実施した。2020年度（令和2年度）が最終年度であるが、2017年度（平成29年度）からの合計として、コロッセオ演習で延べ571名、コロッセオカレッジで延べ1,717名の人材を育成した。

SecHack365は、日本国内に居住する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う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）を育成するプログラムである。NICTの持つ実際のサイバー攻撃関連データを活用しつつ、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。2020年度（令和2年度）は41名が修了し、2017年度（平成29年度）からの合計で171名が修了している。2021年度（令和3年度）以降も、引き続き同規模で実施予定である。

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



3　デジタル化の進展に伴うセキュリティ対策の促進に関する取組

ア　クラウドサービスのセキュリティ

2018年（平成30年）6月に、政府は「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成30年6月7日 各府省情報化統括責任者（CIO）連絡会議決定）を定め、クラウド・バイ・デフォルト原則を掲げる一方で、「未来投資戦略2018」（平成30年6月15日閣議決定）、及び「サイバーセキュリティ戦略」（平成30年7月27日閣議決定）において、クラウドサービスの安全性評価に関する検討の必要性が位置付けられた。

これを受け、同年8月から2019年（令和元年）12月にかけて、総務省と経済産業省が事務局となり、「クラウドサービスの安全性評価に関する検討会」を開催し、2020年（令和2年）1月にはパブリックコメントを経たとりまとめが行われた。また、これらの閣議決定等を踏まえ、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和2

年1月30日サイバーセキュリティ戦略本部決定）において、本制度の①基本的枠組み、②各政府機関等における利用の考え方、③所管と運用体制が決定された。

基本的枠組みを受け、2020年（令和2年）5月25日に本制度の最高意思決定機関として有識者と制度所管省庁（内閣官房（内閣サイバーセキュリティセンター・情報通信技術（IT）総合戦略室）・総務省・経済産業省）を構成員としたISMAP運営委員会を設置するとともに、同年5月26日に第1回ISMAP運営委員会を開催し、委員会において制度に関する各種規程等が決定され、制度が立ち上げられた。同年8月には当該規程等に基づいた審査を経たISMAP監査機関リストが公開された。2021年（令和3年）3月には、本制度で定められた基準に基づいたセキュリティ対策を実施していることが確認されたクラウドサービスのリストがISMAPクラウドサービスリスト*8として公開された。

イ　テレワークのセキュリティ

テレワークは、時間や場所を有効に活用でき、柔軟な働き方を実現するだけでなく、感染症の拡大予防や、災害発生時も含めた業務継続という観点からも有効かつ重要である。一方、テレワークの実施に当たっては、インターネットを利用したり、端末の持ち出しや私用端末の利用も想定されたりすること等から、組織内利用のみを想定していた従来のセキュリティ対策に加えて、テレワーク的な視点からも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して実施したアンケートでも、セキュリティ確保が最大の課題とされている*9。

総務省では、こうした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・活用していただくため、2004年（平成16年）から「テレワークセキュリティガイドライン」*10を策定している。感染症対応を契機として、テレワークによる勤務が一部の従業員に限ったものから、より一般的な形態になるなど、テレワークを取り巻く環境が変化しているほか、クラウドの活用進展やサイバー攻撃の高度化などセキュリティ動向の変化も生じていることから、実施すべきセキュリティ対策や具体的なトラブル事例などを全面的に見直す改定を2021年（令和3年）5月に行った。

また、中小企業等をはじめ、テレワークが幅広く浸透する中で、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も想定され、こうした場合でもガイドラインに沿ったセキュリティ対策は欠かせないものの、個別に十分な検討を行うことが現実的に難しい面もあるため、総務省では、最低限のセキュリティを確実に確保していただく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）」を2020年（令和2年）9月に策定し、2021年（令和3年）5月にガイドライン改定と合わせて改定を行った。

ウ　無線LANセキュリティ

無線LANは家庭や職場、外出先での公衆無線LANサービスに代表されるように幅広く利用が進んでいるが、適切なセキュリティ対策をとらなければ、無線LAN機器を踏み台にした攻撃や情報窃取が行われるおそれがある。そのため、総務省では、無線LANのセキュリティ対策について、利用者・提供者のそれぞれに向けたガイドラインを策定しており、2020年（令和2年）5月に、新技術や最新のセキュリティ動向に対応した改定版を公表している*11。

＊8　ISMAPクラウドサービスリスト：https://www.ismap.go.jp/csm?id=cloud_service_list
＊9　テレワークセキュリティに係る実態調査（2020年度2次実態調査）：https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
＊10 テレワークにおけるセキュリティ確保：https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
＊11 無線LANの安全な利用について：https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

無線LANの利用者に向けた「Wi-Fi利用者向け 簡易マニュアル」では、利用者が留意すべきセキュリティ対策として、①接続するアクセスポイントをよく確認、②正しいURLでHTTPS通信をしているか確認、③自宅に設置している機器の設定を確認、の3つのポイントを示した上でそれぞれについて解説を加えている。

無線LANの提供者に向けた「Wi-Fi提供者向け セキュリティ対策の手引き」では、飲食店や小売店等をはじめとする無線LANを提供する幅広い方々が、提供に当たってどのようなセキュリティ上のリスクがあり、どのようなセキュリティ対策をすればよいかを確認できるようにしている。

4 トラストサービスに関する取組

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等を防止する仕組みであるトラストサービス（図表5-5-2-3）の重要性が高まっている。また、新型コロナウイルス感染症拡大防止等の観点からテレワーク等の推進が一層求められており、あらゆるやり取りをデジタルで完結する要請が高まるなか、トラストサービスが重要な役割を果たすことがより一層期待されている。

総務省は、2019年（平成31年）1月に「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を立ち上げ、我が国のトラストサービスの在り方に関する検討を行い、2020年（令和2年）2月に最終取りまとめを提示してトラストサービスについて次の取組の方向性を示した。

① 電子データがある時刻に存在し、その時刻以降に改ざんされていないことを証明するタイムスタンプについては、民間の認定制度が運用されてきたものの、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あること等を踏まえ、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。

② 電子データの発行元の組織を簡便に確認することができるeシールについては、新しいサービスであり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ため、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。

③ 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、電子署名法の主務省（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等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。

当該提言を踏まえ、タイムスタンプについて、2020年（令和2年）3月に「タイムスタンプ認定制度に関する検討会」を立上げ、現行の「タイムビジネス信頼・安心認定制度」における課題やEU等の国際的な制度との整合性等を踏まえつつ、国による認定制度の創設に当たり検討が必要な論点について議論を行い、2021年（令和3年）3月に最終取りまとめを提示した。本検討会の取りまとめを踏まえ、総務省は同年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）」を公布し、国による認定制度を整備した。今後、国による認定制度を適切かつ確実に運用するとともに、タイムスタンプの利用の一層の拡大に向け、電子文書の送受信・保存において公的に有効な手段となるよう、必要な取組を行うこととしている。

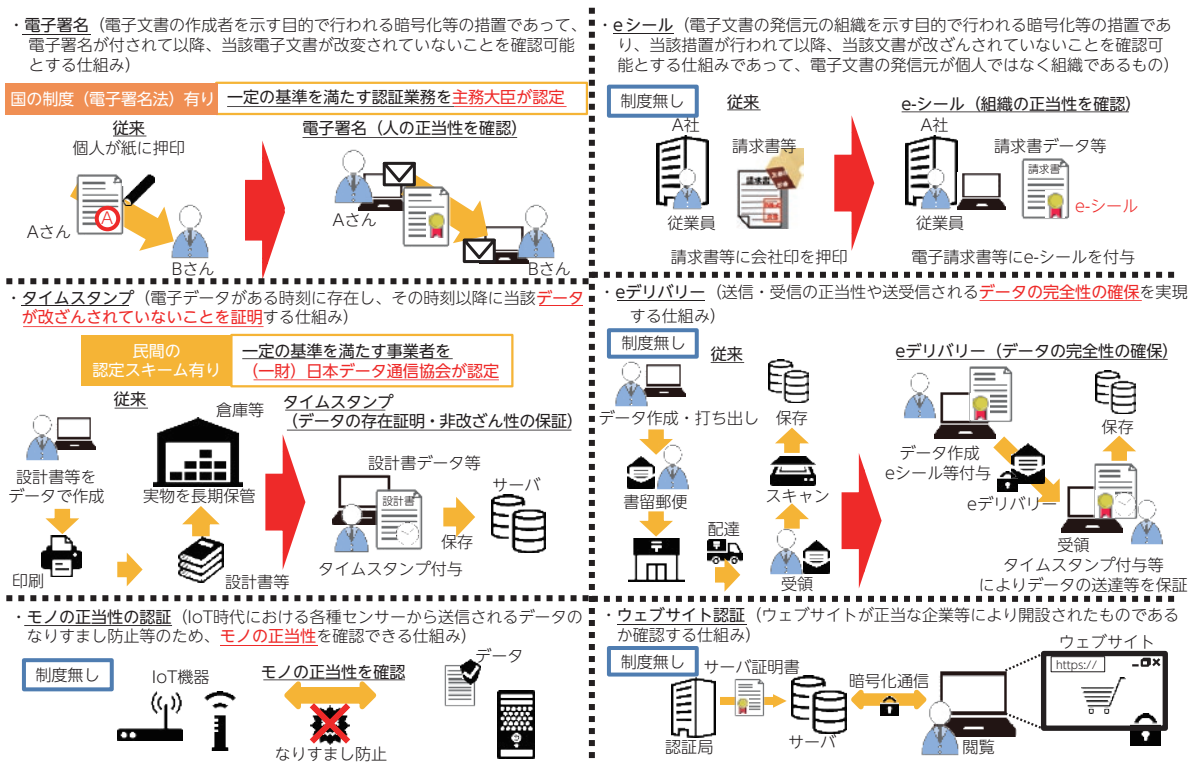
また、eシールについて検討を行う場として、「組織が発行するデータの信頼性を確保する制度

に関する検討会」を2020年（令和2年）4月に立ち上げた。まずはeシールの利用が有効と考えられるユースケースについて事業者へのヒアリングや広く一般を対象に提案募集等を実施した。その結果を踏まえつつ、実証等を通じて整理した技術的基準等についても参考にしながら、我が国におけるeシールの在り方等について検討を行った。そして、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の指針を策定し、関係者へ働きかけを行う等eシールの利用の拡大に向けた施策を実施していくこととしている。

電子署名については、規制改革推進会議における紙や押印を前提とした制度や慣習の見直しの議論の中で、使い勝手の改善に関する課題が指摘された。こうした指摘を踏まえ、リモート署名について、2020年（令和2年）5月の成長戦略WGにおいて回答書を公表し、リモート署名における電子署名法上の位置づけを示した。また、新しく登場したクラウド技術を活用した立会人型電子署名（利用者の指示に基づきサービス提供者自身の署名鍵による暗号化等を行う電子契約サービス）については、電子署名法における取扱いが不明確であったことから、同年7月に「電子署名法2条1項に関するQ＆A[*12]」を、同年9月には「電子署名法3条に関するQ&A[*13]」を公表した。

政府全体の動向としては、内閣官房が中心となり検討が進むデータ戦略の中でも、データ基盤の整備に加え、基盤を離れ流通するデータの信頼性を確保するトラストサービスについて基盤となる枠組みの構築が謳われており、総務省での検討内容を共有する等緊密な連携を図っていくこととしている。

図表5-5-2-3　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）

＊12 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（https://www.soumu.go.jp/main_content/000697715.pdf）
＊13 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（電子署名法第3条関係）（https://www.soumu.go.jp/main_content/000705576.pdf）

5 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協議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）との意見交換会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、2020年度、ASEAN地域において、生体認証等を活用したセキュリティ対策ソリューションの適用可能性の実証実験・調査を実施した。

一方、2017年（平成29年）12月の日ASEAN情報通信大臣会合[*14]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として、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オンライン形式又は実地形式にて継続的に実施している。これに加え、昨今のコロナ禍の状況を踏まえ、2020年度より、同センターにおいてオンライン形式で学習可能な自己学習教材等の提供を開始しており、ASEAN各国におけるサイバーセキュリティ能力の向上に取り組んでいる。

同時に、総務省においては、ASEAN各国のISP事業者を対象とした日ASEAN情報セキュリティワークショップを定期的に開催しており、情報共有の促進及び連携体制の構築・強化を図っている。とりわけ、2020年度以来、総務省が構築した日ASEAN間のサイバーセキュリティに係るオンライン上の情報共有基盤が運営されており、関係者間の連携強化に資することとなっている。

＊14 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

サイバーセキュリティ統合知的・人材育成基盤（CYNEX）

経済社会のデジタル化が急速に進展する中で、サイバー攻撃は年々巧妙化・複雑化しており、国民の安全・安心に関わるような事態も生じている。このような状況下において、サイバーセキュリティの確保は個人や企業、そして国家の基幹をも守るものであり、その対応能力を強化していくことは重要な政策課題となっている。

こうした中で我が国のセキュリティ事業者においては、海外のセキュリティ製品を導入・運用する形態が主流となっている。このため、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。また、海外事業者の製品を使用することで、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。この状況を別側面から見ると、①国内でのサイバー攻撃関連の実データが集まらず、②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、③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、④良い技術を作れないため国産技術が普及せず、①'国産技術が普及しないからサイバー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。

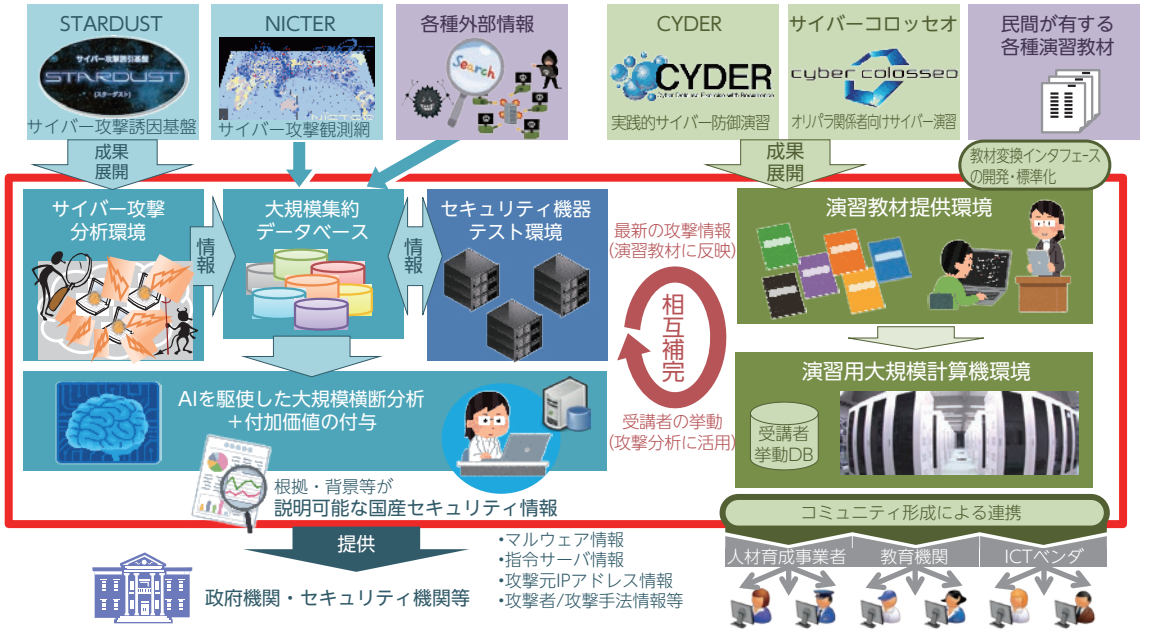
このように国内のセキュリティ事業者においては、実データが集まらないためコア部分のノウハウや知見を蓄積することができず、我が国がグローバルレベルの情報共有において一層の貢献を果たし、国際的に通用するエンジニアの育成をより効果的に実施することが難しくなっている。一方で、利用者側企業においても、セキュリティ製品やセキュリティ情報を適切に取り扱える人材が不足している状況がある。我が国においてセキュリティ人材が充足しているとの回答は約1割であり、人材不足は深刻な状況である。

サイバーセキュリティ人材については、幅広い層において不足しているが、従来から人材育成のための対策を講じているシステム担当者等に加え、戦略を立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求められている状況にある。また、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とから、こうした人材についても不足を解消していく必要がある。

このような人材不足の一因としては、人材育成の仕組みや基盤が不十分であることが挙げられる。特に演習用の環境構築や演習シナリオ開発には高度な知識や技術力、基盤となる計算機環境が必要であり、個々の企業では十分に対応できない。また、国内では対応する基盤が十分でないため、基盤が整備されている海外の演習教材に依存することとなり、結果として日本特有の事例が十分に反映できない状況がある。

以上を踏まえ、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ためには、国内でのサイバーセキュリティ情報生成や、人材育成を加速するエコシステムの構築が必要である。このため、総務省では、情報通信技術を専門とする国内唯一の公的研究機関として、サイバーセキュリティに関する国内トップレベルの研究開発を実施している国立研究開発法人情報通信研究機構（NICT）と連携し、NICTがこれまで培ってきた技術・ノウハウを中核として、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤「サイバーセキュリティ統合知的・人材育成基盤」、通称「CYNEX（サイネックス）」の構築を2021年（令和3年）から進めている。

図表1　サイバーセキュリティ統合知的・人材育成基盤（CYNEX）



本基盤の構築により、我が国のサイバーセキュリティ情報を幅広く収集・分析し、更にその情報を活用して国産セキュリティ製品の開発を推進するとともに、高度なセキュリティ人材の育成や民間・教育機関等での人材育成支援を行うことが可能（詳細は以下のとおり）となる。これにより、我が国におけるサイバーセキュリティ対策のより一層の強化を目指している。

○国産セキュリティ情報の収集・蓄積・分析・提供

NICTでは実際の企業ネットワークを模擬した環境を用意し、攻撃者を誘い込みその挙動を観測するSTARDUSTを運用しており、この技術を拡充し、NICTだけでなくセキュリティ事業者が最新のサイバー攻撃状況を分析することができる環境を構築する。また、その他幅広くサイバーセキュリティ情報を収集・蓄積し、これらビッグデータについて機械学習技術等を用いて横断的に分析することで、高信頼性で即時的なセキュリティ情報を生成・提供する。

○セキュリティ機器テスト環境

セキュリティ事業者において、実際にセキュリティ機器がサイバー攻撃に対してどのような挙動を示すかということは重要な情報であるため、収集・蓄積した最新のサイバー攻撃情報を活用し、セキュリティ製品のサイバー攻撃への対応状況をセキュリティ事業者がテストできる環境を提供する。

○高度解析人材の育成

本基盤において収集・蓄積する他に類を見ない規模のサイバーセキュリティビッグデータについて、それを活用する機会や技術を提供することで、多種多様な情報を多角的・横断的に解析し、高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成する。

○人材育成のための基盤提供

NICTがこれまで実施してきたセキュリティ演習（CYDER等）に関する知見や演習環境を教育機関・民間事業者等に開放し、民間演習教材の活用を図ることで、民間等が演習実施主体となった自律的なセキュリティ人材育成を推進する。