# 第5節　サイバーセキュリティ政策の動向

## 1 概要

### 1 これまでの取組

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（平成26年法律第104号）が2014年（平成26年）に成立し、2015年（平成27年）、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。それ以降、経済社会の変化やサイバーセキュリティ上の脅威の増大などの状況変化も踏まえつつ、諸施策の目標及び実施方針を定める「サイバーセキュリティ戦略」が3年ごとに累次決定されており、2021年（令和3年）9月には新しい「サイバーセキュリティ戦略[*1]」が閣議決定された。これに基づきサイバーセキュリティ政策が推進されてきている。

重要インフラ防護に係る基本的な枠組みを定めた「重要インフラの情報セキュリティに係る第4次行動計画[*2]」（2017年（平成29年）4月サイバーセキュリティ戦略本部決定）において、情報通信分野（電気通信、放送及びケーブルテレビ）は、その機能が停止、又は利用不可能となった場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないものとして重要インフラ14分野の一つに指定されている。今後、関係主体の責務の明確化や障害対応体制の強化などの内容を含む次期行動計画が決定される予定であり、引き続き、重要インフラ所管省庁である総務省として、情報通信ネットワークの安全性・信頼性の確保に向けた取組が必要とされている。

総務省では、2017年（平成29年）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」を開催している。同タスクフォースでは、これまで、様々な状況変化や東京オリンピック・パラリンピック競技大会、新型コロナウイルス感染症への対応等も踏まえつつ、総務省として取り組むべき課題や施策を累次取りまとめてきたところであり、直近では、ICTインフラ・サービス等に関する対策を盛り込んだ「ICTサイバーセキュリティ総合対策2021[*3]」を2021年（令和3年）7月に策定した。これらを踏まえ、ICT分野におけるサイバーセキュリティ対策の推進に向け、諸施策に取り組んでいるところである。

### 2 今後の課題と方向性

新型コロナウイルスの感染症の感染拡大防止のために人の移動が制限され、テレワーク活用などが進展するなど、国民による社会経済活動全般のデジタル化の推進、すなわち、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、より一層重要な政策課題と認識されるようになった。

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、その基盤となるものであり、社会全体のデジタル改革・DX推進を進めるためには、国民一人ひとりがその基盤となるICTを安心して活用できるよう、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

＊1　サイバーセキュリティ戦略：https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021.pdf
＊2　重要インフラの情報セキュリティ対策に係る第4次行動計画（改定）；https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf
＊3　ICTサイバーセキュリティ総合対策2021：https://www.soumu.go.jp/main_content/000761893.pdf

ますます重要になっている。

サイバー攻撃関連の通信については、第3章第7節でみたとおり、依然多くの攻撃関連通信が観測されており、その内訳としてはIoT機器を狙ったものの割合が依然として最も多いことから、IoT機器に対するセキュリティ対策を引き続き強化していく必要がある。

社会全体のデジタル化の推進にあたり必要となるテレワークや無線LANなどの導入にあたっては、「セキュリティの確保」や「セキュリティ上の不安」などが引き続き最大の課題となっており、これらのセキュリティ確保も喫緊の課題である。

また、我が国のセキュリティ事業者は、その多くを海外のセキュリティ製品を導入・運用する形態であり、国内のサイバー攻撃情報などを国内のセキュリティ事業者が集められず、実データに基づいた研究開発を行うことができないために国産セキュリティ技術を作れず、国産技術が普及しないという状況に陥っていると考えられる。そのため、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、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。

## 2 情報通信ネットワークの安全性・信頼性の確保

### 1 IoTに関する取組

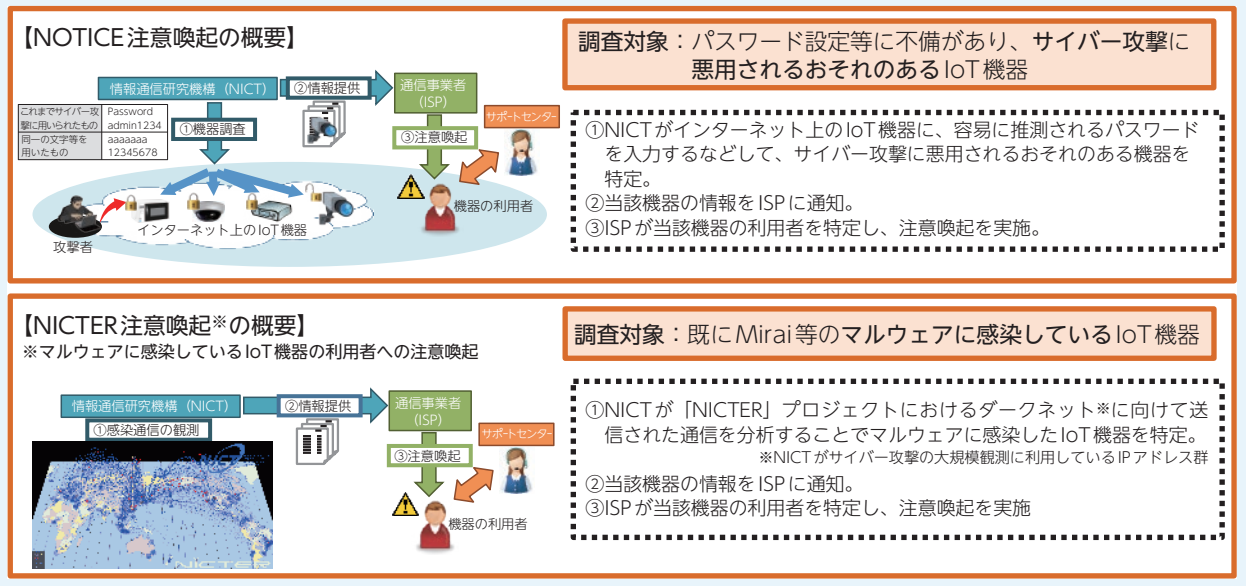
社会基盤としてのIoT化が進展する一方で、IoT機器については、管理が行き届きにくい、機器の性能が限られ適切なセキュリティ対策を適用できないなどの理由から、サイバー攻撃の脅威にさらされることが多く、その対策強化の必要性が指摘されている。実際にIoT機器を悪用したサイバー攻撃が発生しているほか、NICTが運用するサイバー攻撃観測網（NICTER）が2021年（令和3年）に観測したサイバー攻撃関連通信についても、依然としてIoT機器を狙ったものが最も多いという結果が示されている。

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[*4]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。この取組は、①NICTがインターネット上のIoT機器に対して、例えば「password」や「123456」等の容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を特定し、②特定した機器の情報をNICTからISPに通知し、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、という一連の取組である（図表4-5-2-1）。

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。この取組は、NICTが前述のNICTERで得られた情報をもと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で当該機器の利用者を特定することにより行っているものである。

＊4　国立研究開発法人情報通信研究機構法（平成11年法律第162号）

図表4-5-2-1　NOTICE及びNICTERに関する注意喚起の概要




## 2　電気通信事業者の積極的な対策に関する取組

今後、5Gの進展により様々な産業でIoT機器の利用が更に拡大することが予想される中で、IoT機器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、これまでの端末機器側の対策に加え、通信トラフィックが通過するネットワーク側でもより機動的な対処を行う環境整備が必要と考えられる[*5]。

このような状況を踏まえ、総務省では、「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」で、2021年（令和3年）11月に、電気通信事業者が平時からフロー情報を収集・蓄積・分析して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）の検知や、検知したC&Cサーバに関する情報の共有について、通信の秘密との関係上、それぞれ一定の場合に実施可能であると整理した[*6]。また、2022年度（令和4年度）からは、電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を実施する予定である。

そのほか、DDoS攻撃等のサイバー攻撃の送信元情報のISP間での共有や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」[*7]での情報共有や分析について、これまでは攻撃の発生後に攻撃の送信先であることが特定された場合に限られていたが、攻撃の発生前にも実施できるようにすることなどを内容とする電気通信事業法の一部を改正する法律案が2022年（令和4年）3月に国会に提出され、同年6月に成立するなど、DDoS攻撃等のサイバー攻撃への対処における電気通信事業者間の連携促進を図っている。

## 3　テレワークのセキュリティに関する取組

テレワーク導入企業に対して実施したアンケートではセキュリティ確保が最大の課題とされてお

＊5　2021年（令和3年）に策定した「ICTサイバーセキュリティ総合対策2021」では、「サイバー攻撃に対する電気通信事業者の積極的な対策の実現」として、「インターネット上でISP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」としている。（https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html）
＊6　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 第四次とりまとめ：https://www.soumu.go.jp/main_content/000779208.pdf
＊7　電気通信事業法第116の2条第1項に基づき、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、2019年（平成31年）1月に一般社団法人ICT-ISACが認定されている。

り[*8]、総務省では、こうしたセキュリティ上の不安を払拭し、企業が安心してテレワークを導入・活用できるようにするため、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」[*9]を策定している。新型コロナウイルス感染症の感染拡大を契機として、テレワークを取り巻く環境が大きく変化しているほか、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、総務省では、2021年（令和3年）5月に、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行った。

また、中小企業などでは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るため、最低限のセキュリティを確実に確保することに焦点を絞った「中小企業など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。

## 4 トラストサービスに関する取組

Society5.0では、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などを防止する仕組みであるトラストサービス（図表4-5-4-1）の重要性が高まっている。

### 1 「トラストサービス検討ワーキンググループ」における検討

総務省では、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、同ワーキンググループでは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月の同ワーキンググループの最終取りまとめで、タイムスタンプとeシール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などを踏まえ、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、国の関与の下で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

### 2 国によるタイムスタンプ認定制度の整備

タイムスタンプについては、ワーキンググループの提言を踏まえ「タイムスタンプ認定制度に関する検討会」で更なる検討を行い、総務省では、2021年（令和3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）を制定し、国による認定制度を整備した。さらに、2022年度（令和4年度）の税制改正により、税務関係書類に係るスキャナ保存制度等において、民間（一般財団法人日本データ通信協会）の認定制度に係るタイムスタンプに代わり、国によ

＊8　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/
＊9　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/

る認定制度に係るタイムスタンプを位置づけることとなった*10。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、必要な取組を行うこととしている。

## 3 「eシールに関する指針」の策定

eシールについては、ワーキンググループの提言を踏まえ、2020年（令和2年）4月に立ち上げた「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」において、我が国におけるeシールの在り方などについて検討を行った。その後、2021年（令和3年）6月に検討会の取りまとめを公表するとともに、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・運用上の基準などについて整理した「eシールに係る指針*11」を策定した。

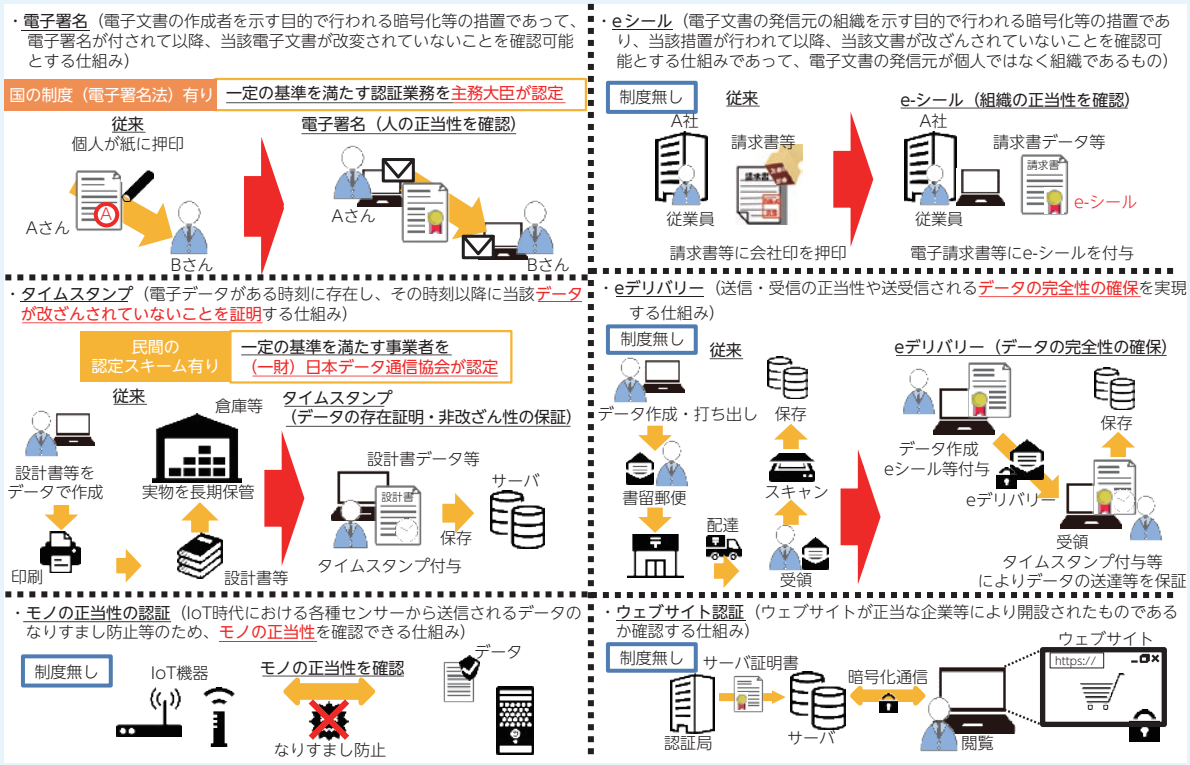
## 4 デジタル庁における検討状況

電子署名については、電子署名及び認証業務に関する法律（平成12年法律第102号）に基づく電子証明書の普及と制度の企画をデジタル庁が一体的に担うことが効果的とされたことを踏まえ*12、同法に関する事務が総務省及び経済産業省からデジタル庁に移管され*13、同庁が主導して電子署名の利用拡大や利便性向上の取組を行っている。政府全体の動向としては、デジタル社会推進会議令（令和3年政令第193号）に基づく「データ戦略推進ワーキンググループ」の下で、官民の様々な手続や取引についてデジタル化のニーズや必要なアシュアランスレベルの検討を行う「トラストを確保したDX推進サブワーキンググループ」が2021年（令和3年）11月に立ち上げられ、同サブワーキンググループで、タイムスタンプやeシールに関する総務省の取組の内容も踏まえつつ、トラストサービスの基盤となる枠組みについての議論が行われている。



＊10 2022年（令和4年）4月1日から2023年（令和5年）7月29日までの間は、従前どおり一般財団法人日本データ通信協会が認定する業務に係るタイムスタンプを付すことを可能とする経過措置が講じられる。
＊11 eシールに係る指針（https://www.soumu.go.jp/main_content/000756907.pdf）
＊12 デジタル改革関連法案ワーキンググループ作業部会とりまとめ（https://www.kantei.go.jp/jp/singi/it2/dgov/houan_wg/dai4/siryou2.pdf）
＊13 電子署名の法的効果に関する規定（私文書の真正な成立の推定など）は、引き続き法務省が所管する。

図表4-5-4-1　トラストサービスのイメージ




## 5　無線LANセキュリティに関する取組

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*14。

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、飲食店や小売店など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。

## 6　クラウドサービスの安全性確保に関する取組

### 1　政府情報システムにおけるクラウドサービスの安全性評価

政府では、クラウド・バイ・デフォルト原則の下、クラウドサービスの安全性評価について、「クラウドサービスの安全性評価に関する検討会」で検討を行い、「政府情報システムにおけるクラ

＊14　無線LANの安全な利用について：https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

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）で、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）6月、有識者と制度所管省庁（内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省）を構成員とするISMAP運営委員会で決定した各種規程等に基づき、「政府情報システムのためのセキュリティ評価制度」（英語名：Information system Security Management and Assessment Program（ISMAP））制度が立ち上げられた。2021年（令和3年）3月から、この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登録が始まり、2022年（令和4年）6月1日現在、合計34サービスがISMAPクラウドサービスリスト[*15]として公開されている。

### 2 「クラウドサービス提供における情報セキュリティ対策ガイドライン」の策定

総務省では、安全・安心なクラウドサービスの利活用推進のための取組として、クラウドサービス事業者における情報セキュリティ対策を取りまとめた「クラウドサービス提供における情報セキュリティ対策ガイドライン」を策定しており、2021年（令和3年）9月には、クラウドサービスの提供・利用実態等を踏まえた改定版（第3版）を公表している[*16]。また、昨今では、クラウドサービス利用者が適切にクラウドサービスを利用できていないことに起因し、結果的に情報流出のおそれに至る事案も発生していることから、利用者の適切なクラウドサービスの利用促進について、提供者・利用者を含む幅広い主体で検討しており、今後、クラウドサービスの提供・利用における適切な設定に関するガイドラインとして策定・公表する予定としている。

## 7 セキュリティ人材の育成に関する取組

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、SecHack365）を積極的に推進している。

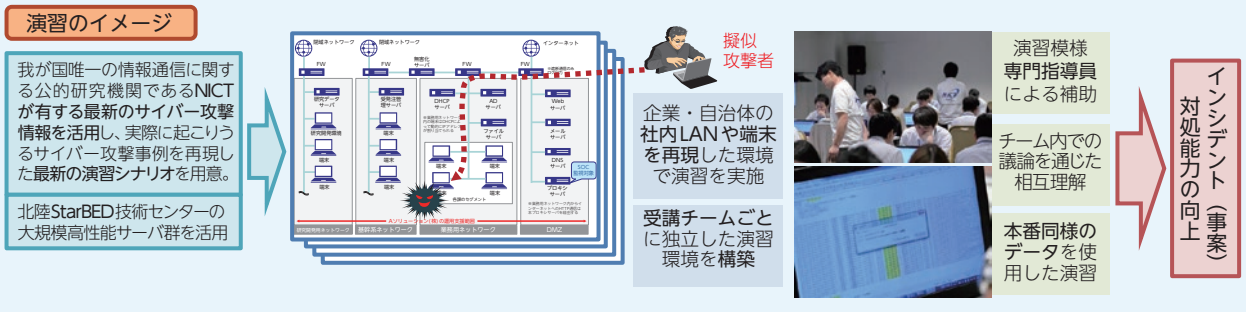
### 1 情報システム担当者を対象とした実践的サイバー防御演習（CYDER）

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など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り、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（図表4-5-7-1）。2017年度（平成29年度）からの合計で13,867名が受講しており、2021年度（令和3年度）から、従来の初級・中級の集合演習コースの実施に加え、サイバーコロッセオ[*17]の知見を活用した、より高度なセキュリティ技術を習得可能な準上級コースや、地理的・時間的要因などにより

＊15 ISMAPクラウドサービスリスト：https://www.ismap.go.jp/csm?id=cloud_service_list
＊16 クラウドサービス提供における情報セキュリティガイドライン（第3版）：https://www.soumu.go.jp/main_content/000771515.pdf
＊17 サイバーコロッセオ：東京オリンピック・パラリンピック競技大会に向けた大会関連組織のセキュリティ担当者などを対象者とした実践的サイバー演習。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など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、東京オリンピック・パラリンピック競技大会組織委員会とも緊密な連携を図りながら、2017～2020年度（平成29～令和2年度）の間実施し、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。

CYDERが受講できていない方への最低限の対応をするオンライン演習のコースを追加した（図表4-5-7-2）。

**図表4-5-7-1　実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）**




**図表4-5-7-2　令和3年度CYDER実施状況**

| コース名 | 演習方法 | レベル | 受講想定者（習得内容） | 受講想定組織 | 開催地 | 開催回数 | 実施時期 |
|---|---|---|---|---|---|---|---|
| A | 集合演習 | 初級 | システムに携わり始めた者（事案発生時の対応の流れ） | 全組織共通 | 47都道府県 | 68回 | 7月～翌年2月 |
| B-1 | | 中級 | システム管理者・運用者（主体的な事案対応・セキュリティ管理） | 地方公共団体 | 全国11地域 | 21回 | 10月～翌年2月 |
| B-2 | | | | 地方公共団体以外 | 東京・大阪・名古屋・福岡 | 13回 | 翌年1月～2月 |
| C | | 準上級 | セキュリティ専門担当者（高度なセキュリティ技術） | 全組織共通 | 東京 | 3回 | 翌年1月～2月 |
| オンラインA | オンライン演習 | 初級 | システムに携わり始めた者（事案発生時の対応の流れ） | 全組織共通 | （受講者職場等） | 随時 | 11月～翌年3月（6～8月に試験提供） |

令和3年度から新規開設

## 2 若手セキュリティ人材の育成プログラム（SecHack365）

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・開発などを1年かけて継続的かつ本格的に指導する。2021年度（令和3年度）は41名が修了し、2017年度（平成29年度）からの合計で212名が修了している。

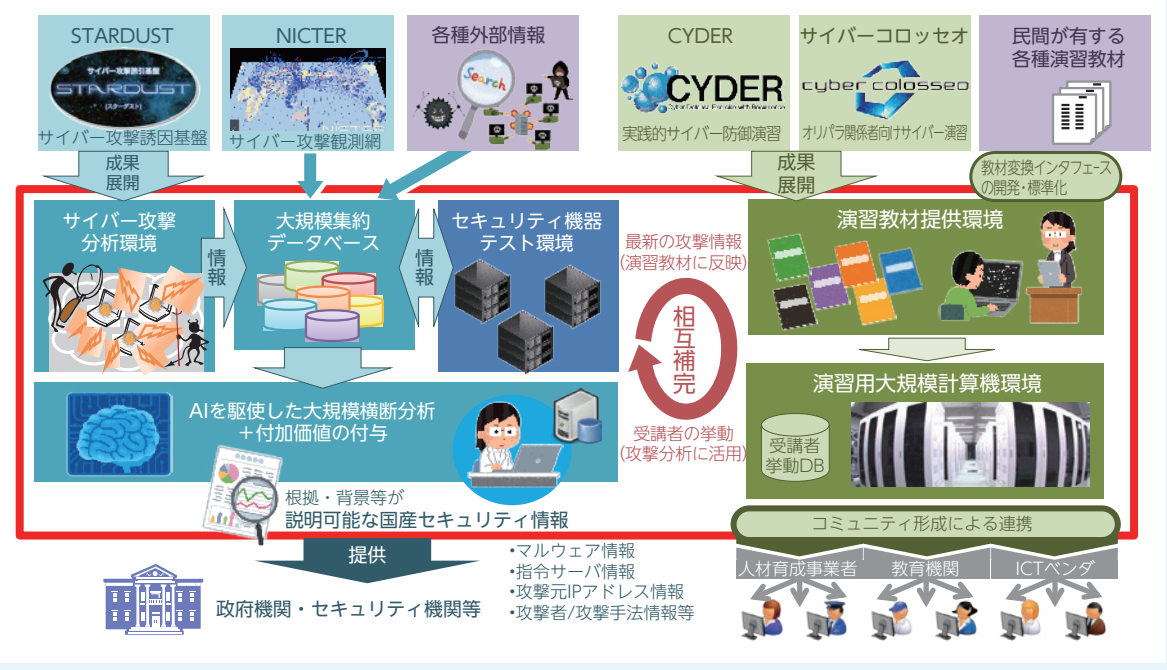
## 8 「サイバーセキュリティ統合知的・人材育成基盤（CYNEX）」の構築

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。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などの収集・分析などが十分にできていない。また、海外のセキュリティ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で、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。

その結果、国内のセキュリティ事業者では、コア部分のノウハウや知見の蓄積ができず、また、グローバルレベルの情報共有における貢献や国際的に通用するエンジニアの育成を効果的に実施することが難しくなっている。利用者側企業でも、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。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。

総務省では、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NICTと連携し、NICTが培ってきた技術・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）から進めており、2022年（令和4年）から試験運用を開始している（図表4-5-8-1）。

図表4-5-8-1　サイバーセキュリティ統合知的・人材育成基盤（CYNEX）



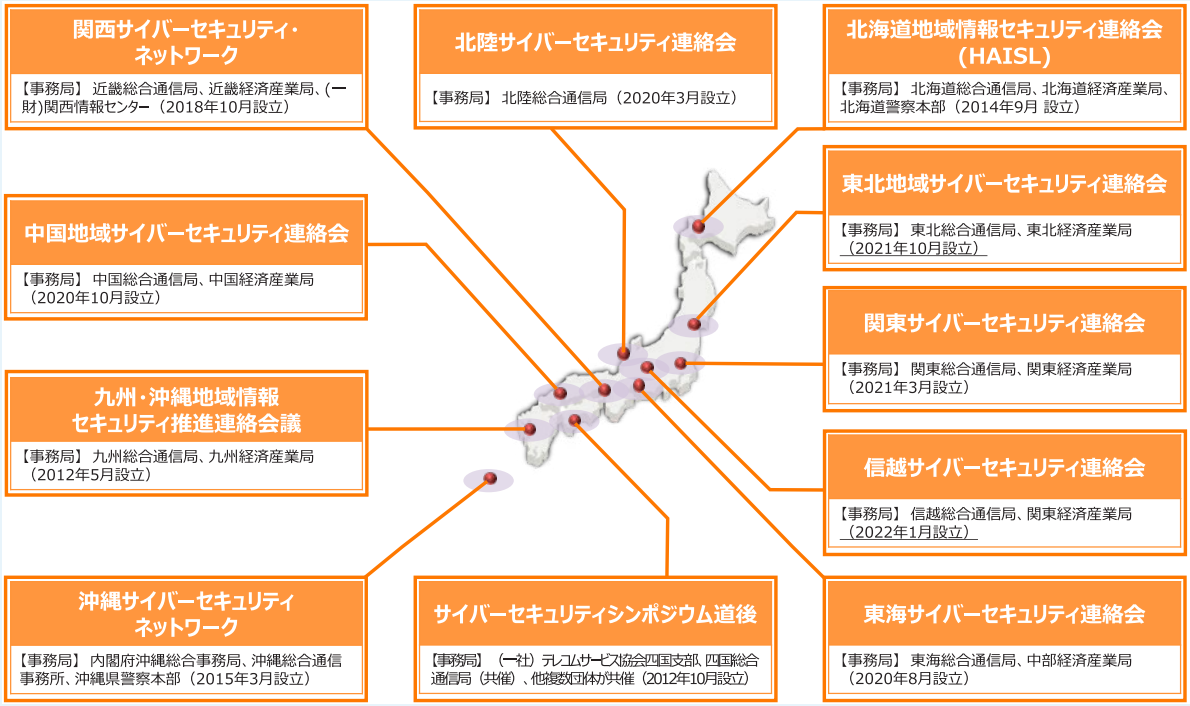

この先端的基盤の構築により、我が国のサイバーセキュリティ情報を幅広く収集・分析し、更にその情報を活用して国産セキュリティ製品の開発を推進するとともに、高度なセキュリティ人材の育成や民間・教育機関などでの人材育成支援を行うことが可能となる。これにより、我が国におけるサイバーセキュリティ対策のより一層の強化を目指している。

## 9 地域に根付いたセキュリティコミュニティ（地域SECUNITY）の形成促進

我が国の情報通信サービス・ネットワークの安全性や信頼性の確保の観点からは、全国規模や首都圏でサービスを提供している事業者だけでなく、地域単位で情報通信サービスを提供している事業者におけるサイバーセキュリティの確保も重要な課題である。他方、地域の企業や地方公共団体では、首都圏や全国規模で展開する企業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などの理由により、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おそれがある。

総務省では、このような関係者間でのセキュリティに関する「共助」の関係を構築したコミュニティ（「地域SECUNITY」）について、2021年度（令和3年度）までに、総合通信局等の管区を基準とした全11地域での設立を完了した（図表4-5-9-1）。今後は、地域全体への活動の展開や、セミナーなどの開催に加えて幅広い層への普及啓発の取組の拡大に向けて、2022年度（令和4年度）も引き続き同様にイベント開催などの支援を実施していく。

図表4-5-9-1　各地域におけるセキュリティコミュニティ




## 10 国際連携に関する取組

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などでの議論や情報発信・情報収集を積極的に実施している。

また、情報通信事業者など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、日米・日EU間でのISAC（Information Sharing and Analysis Center）との意見交換会などを開催している。

ASEAN地域では、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 Center）を中心に、ASEAN地域のサイバーセキュリティ能力の向上に資する取組を行っている*18。同時に、総務省では、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。



＊18 第4章第8節参照