サイバーセキュリティ対策に係る最新動向
～ICTサイバーセキュリティ総合対策2023～

総務省サイバーセキュリティ統括官付　参事官　小川　久仁子

サイバーセキュリティに関しては、攻撃者が圧倒的に有利の中で、攻撃が非常に巧妙化、多様化してきており、それに対応していく必要があります。関係省庁や関係機関とも連携しながら、さまざまな取組を進め、安心・安全なインターネットの環境、DXを守るためにできることを進めています。

サイバーセキュリティを取巻く動向

サイバー攻撃は、昔に比べて変化してきています。2000年頃は、省庁ホームページの改ざんなど、こんなことができるという、自己顕示的なところが強かったのですが、2010年頃からは、ランサムウェアの感染によって身代金を要求する経済犯的なものが出てきました。最近では、大規模なDDoS（Distributed Denial of Service）攻撃による通信障害とか、国家的なアクターが背景にある攻撃も増えてきており、安全保障上の観点も含めて、対応が必要な状況です。

典型的なサイバー攻撃を３つ紹介します。１つ目が、DDoS攻撃です。これは、例えばネットワークカメラや、ルーター、IoT機器などを大量にマルウェアに感染させ、そのマルウェアに感染した機器群を操作できるボットネットを形成して、攻撃者が攻撃目標を指示します。そうすると数万台から形成されるボットネットから一斉に標的に向かって攻撃が発生します。標的に対してたくさんの攻撃が一気に送られてくるので、例えばサーバの処理能力を超えてダウンしたり、大量の攻撃通信が通るため、その間の通信ネットワークにも障害が起こる事例も出ております。

ある意味で、このボットネットが、DDoS攻撃の、サイバー攻撃のインフラみたいになっており、これを減らすことが必要です。最近の事例としても、国土交通省が河川に設置していたカメラが200台ぐらいこのボットに感染して、大量の攻撃通信が出た事例もあります。また、2022年９月以降、ロシアを支持するハッカー集団との関係についての報道があった中央官庁に対するDDoS攻撃が断続的に発生したといった事例があります。

２つ目は、ランサムウェアの攻撃です。例えば、大阪の急性期総合医療センターへのランサムウェアの攻撃によって、カルテ情報などが暗号化されて見えなくなり、復旧にかなり時間がかかりました。また、名古屋港でランサムウェアに感染して、コンテナの搬入などが停止してしまった事例もあります。ランサムウェアの被害件数が増えてきている状況です。

３つ目は、メールを使っていると日々接するフィッシングの問題です。電子商取引、運送会社、あるいは銀行やカードといった金融系の有名企業の名前をかたる、フィッシングのメールがたくさん届いており、これにうっかり個人情報とかカー

ド情報、ID、パスワード等を書き込むと、それが攻撃者に渡って使われる場合があります。

国立研究開発法人の情報通信研究機構（NICT）は、大規模なサイバー攻撃観測網を、17年ぐらい前から運用しており、具体的には未使用のIPアドレスを30万個ほど観測しています。未使用のIPアドレスには本来は何の通信も来ないはずが、サイバー攻撃をしようとする人たちが、どんなポートが空いているか、どんな機器があるかを探索するような通信、攻撃に関する通信がインターネット空間の中を流れており、それが未使用のIPアドレスにも到着するため、それを観測してサイバー攻撃の状況を見ております。2022年には、１年間に5,226億パケットの攻撃通信が観測されており、１つのIPアドレスに17秒に１回の攻撃関連の通知があることになります。

サイバー攻撃の事例については、海外でも増大しており、アメリカでも例えば2021年５月に、石油パイプライン大手のColonial Pipelineがランサムウェアの攻撃を受けて、操業を一時停止して原油価格にも影響がありました。また、2022年２月以降のウクライナ戦争では、金融機関などに対するサイバー攻撃が発生しており、いわばハイブリッド･ウォーというような状況になっています。

2022年12月に公表された我が国の「国家安全保障戦略」では、昨今のこういう状況も踏まえ、地域全体としては武力攻撃に至らないけれども、重要インフラに対する安全保障上の懸念を生じさせる重大なサイバー攻撃の恐れがある場合に、能動的サイバー防御のための体制の整備を検討していくことが記載されています。また、内閣の「サイバーセキュリティセンター（NISC）」を発展的に改組することについても言及されています。

総務省の取組とICTサイバーセキュリティ総合対策2023

総務省におけるサイバーセキュリティの取組について紹介します。「サイバーセキュリティ戦略本部」が、政府全体の司令塔として設置されており、総務大臣も構成員になっています。重要インフラを守っていくことが重要で、総務省は情報通信と、地方公共団体を所管しているので、連携しながら取り組んでいる状況です。

サイバーセキュリティ戦略本部は、サイバーセキュリティ戦略を策定し、３年に１回、改定しています。2021年の９月に策定されたものでは「Cybersecurity for All」ということで、誰も取り残さないサイバーセキュリティのために、３つの柱があります。まず、DXとサイバーセキュリティの同時推進という「DX with Cybersecurity」があります。また、公共空間化したサイバー空間の安全、安心を確保していきます。さらに、ウクライナ戦争の前から意識された安全保障の観点からの取組強化が示されています（図表１）。

サイバー空間が、公共空間として非常に重要となり、その根幹は情報通信ネットワークであり、情報通信ネットワークがつながらなければ、サイバー空間を利用することができません。総務省は、情報通信サービス・行政を担当し、サイバー空間上の社会経済活動を支える土台となる情報通信ネットワークの安全を確保していくことが役割であり、重要だと思っております。

その観点から、総務省の有識者会議「サイバーセキュリティタスクフォース」で取り組むべき方針について、議論を進めてきております。そこで取りまとめた最新の計画が「ICTサイバーセキュリティ総合対策2023」であり、2023年８月のパブリックコメントを経て、取りまとめられました。

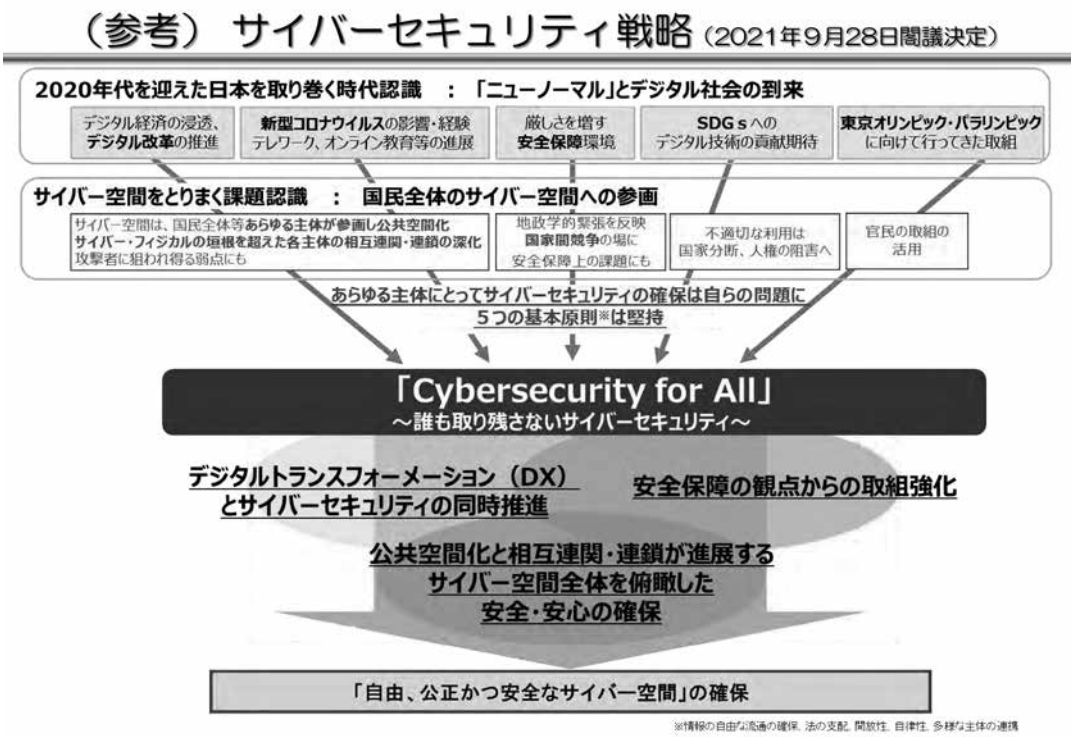
「ICTサイバーセキュリティ総合対策2023」では、サイバーセキュリティについての動向や情勢も踏まえ、４つの柱で取り組むことになっています（図表２）。

１つ目の柱が一番重要で、先ほども申し上げたように全体の土台となる「情報通信ネットワークの安全性・信頼性を確保」していくための取組です。２つ目が「サイバー攻撃の自律的な対処能力の向上」で、人材開発であるとか、わが国において分析能力を確保していくことです。３つ目と４つ目は、関係省庁とも協力していく点で「国際連携の推進」と「普及啓発の推進」です。

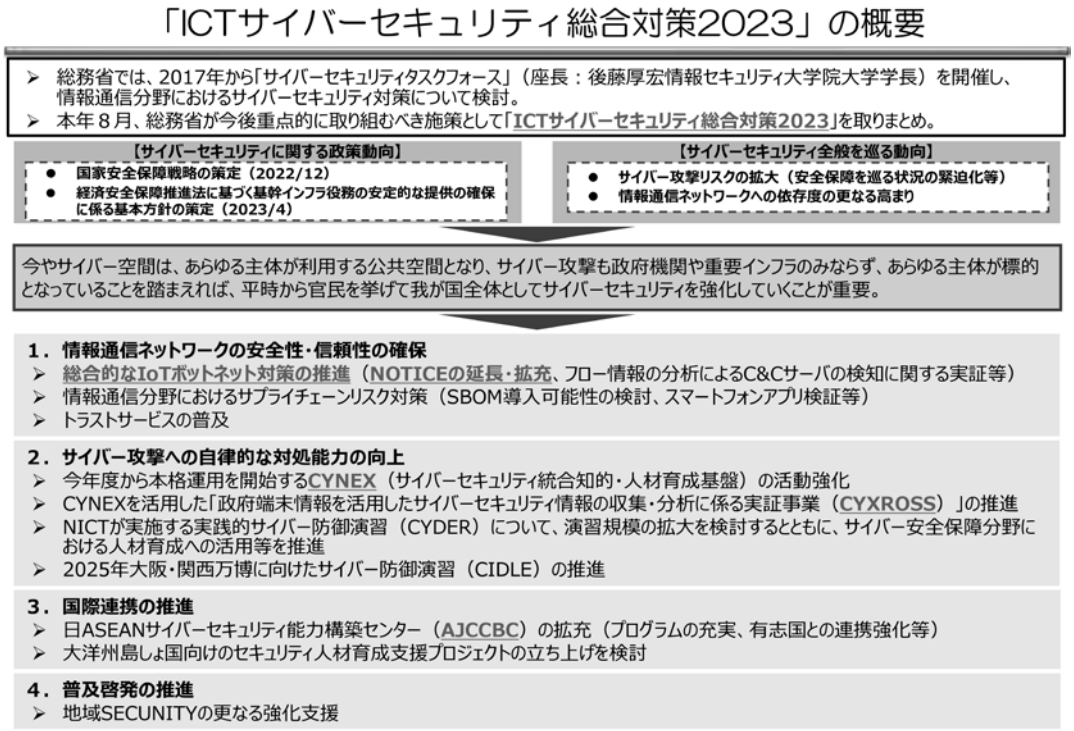
端末側の対策（情報通信ネットワークの安全性・信頼性の確保）

情報通信ネットワークの安全性信頼性の確保のために展開されている施策については、まず、先ほど申し上げたDDoS攻撃への対策として、IoTのボットネットに対する総合的な対策を検討しています。

図表１



図表２



総合的なIoTボットネット対策の実現に向けた１つ目が、端末側における対策で、従来から取り組んでいるNOTICEというプロジェクトを発展させて対応しています。

NOTICEの英文名称は「National Operation TOWARDS IoT Clean Environment」で、IoTの環境を、マルウェアに感染したボットがたくさんある状況ではなくて、よりきれいな環境にすることにより、サイバー攻撃の深刻化に対応することを目的に始められました。

NOTICEが導入された2018年頃には、IDやパスワードが例えばaaaaやadminといったように単純で脆弱なものに対して、それを破って感染を広げていくMiraiというマルウェアが流行していま

した。脆弱性があるID・パスワードの機器やシステムについて調査してID・パスワードを変更することも含めた対策を進めることがそもそもの始まりです。

このID・パスワードに脆弱性があるIoT機器について、NICTが継続して毎月調査を行っております。脆弱性のある機器の機種についての調査を行った上で、通信事業者を通じて機器の利用者に注意喚起を行っています。最近では、通信事業者への通知件数が、毎月5,000件程度となっています。

一般に他者がID・パスワードを入力して行なうログイン試行については不正アクセス禁止法では禁止されておりますが、NICTがID・パスワードに脆弱性があるIoT機器を見付けるためにログイン試行をすることは、NICT法の規定に基づき「特定アクセス行為」として時限付きで例外的に認められています。

また、既に感染してしまっているIoT機器も多く存在しているため、感染通信を出しているIoT機器について観測し、通信事業者を通じて、機器の利用者に注意喚起しています。最近ではこれが１日平均1,000件程度ですが、感染状況によってかなり増減します。

このように、脆弱性がある機器への注意喚起と感染している機器への注意喚起を通じて、利用者からの被害申告を待つことなく、プッシュ型で支援を実施しています。また、調査対象のプロトコルなども徐々に増やし、脆弱性を発見できる範囲を増やしています。

NOTICEのプロジェクトには、現時点で79社のISPに参加いただいています。NOTICEの成果の一つとして、国内の1.13億IPアドレスについて毎月の調査をする体制を整えることにより、サイバー攻撃に悪用される可能性のある脆弱性のあるIoT機器の実態や感染状況についてよく把握できるようになったことが挙げられます。

NOTICEプロジェクトに参加している通信事業者の協力も受けて利用者に注意喚起を行うことなどにより脆弱性のあるIoT機器を一定程度減らしてきています。また、レンタルルーター等について一気に何千台も脆弱性を解消した事例やインターポール（国際刑事警察機構）から、国内のEmotet感染端末の情報提供があり、警察庁と連携してこのNOTICEの枠組みを用いて利用者に注意喚起を実施したこともあります。

更に、NOTICEの調査プロセスの中で、脆弱性があるファームウェアを搭載しているIoT機器を200モデル以上発見し、メーカーに通知して対応を依頼するとともに、国内の脆弱性対策データベースにも登録いただくなど、IoTの環境がきれいになるように、関係の方々と協力しながら取り組んできています。

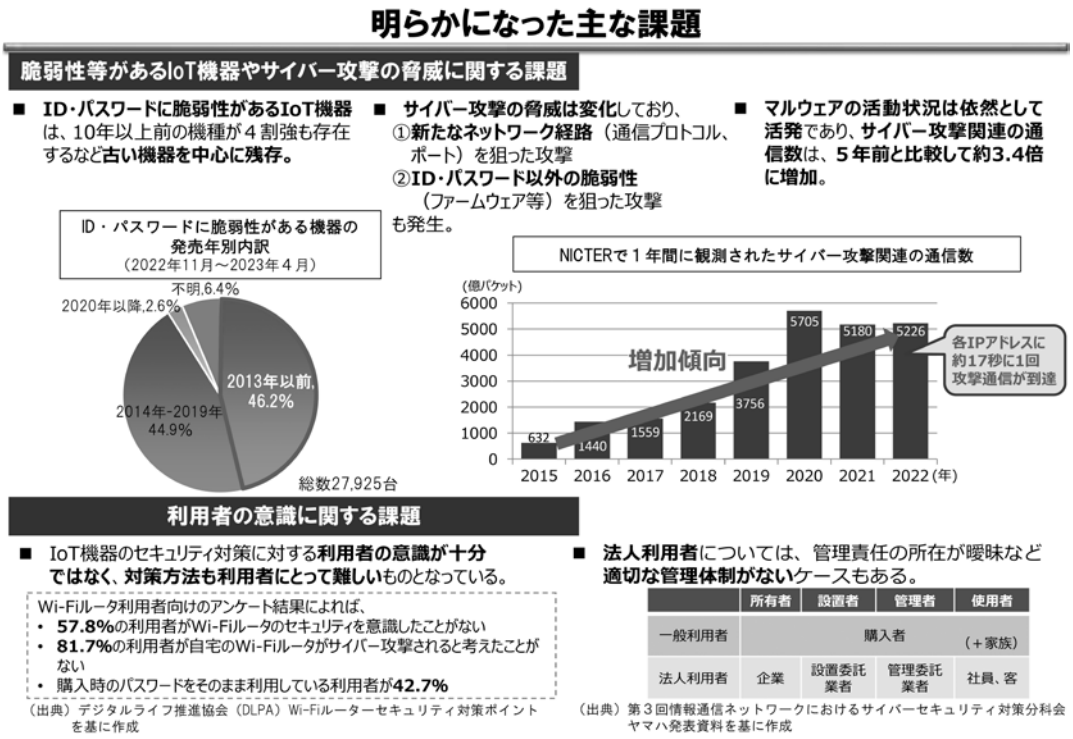
NOTICEプロジェクトの実施を通じて課題として見えてきたものとして（図表３）、IoT機器のライフサイクルの長さであり、ID・パスワードに脆弱性があるIoT機器を発売年で分析すると、10年前の2013年よりも前に発売されたものが46.2％を占めています。パソコンなどのように数年で買い換えるライフサイクルと比べ、IoT機器については壊れるまで相当長く使われる場合も多いことが分かってきました。そのため、場合によってはメーカーのサポートが終了したものであっても使われてしまい、脆弱性が残っている機器がいつまでもなくならないといったような問題が指摘されます。

一方、ID・パスワードに脆弱性があるIoT機器を発売年で分析すると、2020年以降に発売されたものは僅か2.6％となっています。2020年に電気通信事業法に基づくIoT機器の技術基準の改正が行われ、初期パスワードからの変更を促す機能やソフトウェアの更新機能などが規定されました。その効果もあり、脆弱性のあるIoT機器として2020年以降に発売された新しい機器は発見される台数が減っており技術基準の改正による一定の効果があるものの、まだ古い機器が残っていてその対策が必要という状況です。

更に、最近ではID・パスワード以外の脆弱性、例えば、ソフトウェア、ファームウェアの脆弱性を狙った攻撃が多く発生するようになってきており、こちらについても調査して対策が必要な状況です。

また、利用者の意識に関する課題があります。IoT機器のセキュリティ対策の必要性があることに関する利用者の意識は高くなく、また、対策方法も利用者にとって難しい場合があります。例えば、80％の利用者の方々は自宅のWi-Fiルーターがサイバー攻撃されうることを考えたことがないという調査結果もあり、対策の必要性についてもう少し意識をしていただくようにしていく必要も

図表３



あると思います。

更に、法人利用者については、管理責任の所在が曖昧なことについても課題であり、IoT機器の所有者、設置者、管理者と使用者がそれぞれ違う場合があり、注意喚起を行なっても対策いただくことが難しい場合があることも分かってきました。

このような状況を踏まえ、今後の大きな柱として、第一にサイバー攻撃の踏み台となり得るIoT機器に対する観測能力について、維持強化していくことが重要です。そのため、NICTにおけるIoT機器の調査について、ID・パスワードに脆弱性があるIoT機器の調査とともに、脆弱性があるファームウェアを搭載しているIoT機器の調査、さらに、既に感染してしまったIoT機器の調査と、この３つを総合的に取り組んでいけるような形にします。また、IoT機器のライフサイクルが長いということ、サイバー攻撃の状況も変化していくということも踏まえ、ID・パスワードの脆弱性があるIoT機器の調査について、５年間の時限を延長した上で、機動的に今後も取り組めるようにしていきます。

第二に、観測結果を踏まえた対策としては、個別の利用者への注意喚起を引き続き行い、実効性が上がるようにします。その一環として、電気通信事業者向けのガイドラインを策定し、技術基準に適合していない機器が何度も注意しても接続されている場合などに法令上可能とされている接続拒否について、どういう場合に行うことができるか等も含めて示すことにより実効性を上げることも検討していきます。

更に、より上流の工程で対応することこそが重要です。NICTの調査結果をもとに脆弱性があるIoT機器について条ウ提供や助言を行うことが制度的に位置づけられることとなり、総合的な対処を推進できるようにします。総合的な対処の推進として、例えば、メーカーと連携してメーカーによるファームウェアの更新や機器の機能改善やサポート期限の明示、システムインテグレーターと連携して企業にIoT機器を設置する際に適切に対処していただくなど、関係者と連携を進められるように検討します。

2023年５月からNOTICEのステアリングコミッティを作って、NICTの調査結果等に基づき関係者が連携した取組みを始めており、戦略的に重点的に取組むべきことを検討していきます。このステアリングコミッティーにはNICT、NOTICEの参加　のISP、ICT-ISAC（ICT Information Sharing And Analysis Center）、総務省が参加していますが、今後、IoT機器メーカーやSIer（システム　インテグレーター）などの関係者にも参画いただいて、取組を進めていきたいと考えています。

ネットワーク側の対策（情報通信ネットワークの安全性・信頼性の確保）

端末側の取組に加え、ネットワーク側の取組も重要だと考えております。

ボットネットの話をしましたが、実際に攻撃者が、乗っ取った端末に対して外部から指令を行う時に使うのが、C&C（Command and Control）サーバです。C&Cサーバと通信しながら各端末は攻撃者からの指令を受けて攻撃をしますので、C&Cサーバがどこにあるのかを割り出して通信をさせないようにすれば攻撃通信も起こらなくなるため、C&Cサーバの実態を把握していくことが重要になります。

このC&Cサーバとの通信は、通信事業者のネットワークを通ります。通信事業者のトラフィック中でIPアドレスとタイムスタンプという情報を１万分の１ぐらいのサンプリングで抽出したフロー情報というものがあり、これを通信事業者が今でもネットワーク維持管理のために取得しています。このフロー情報のデータを統計的に相関分析等をすることによって、C&Cサーバである可能性が高い機器を検知するということが可能であることから、通信の秘密との関係について制度的整理を行いC&Cサーバの検知を行なうことが可能となっています。通信の秘密との関係は、「電気通信事業におけるサイバー攻撃の適正な対処の在り方に関する研究会」の「第四次とりまとめ」で、電気通信事業者が平時において通信のフロー情報を用いて分析して、C&Cサーバを検知することが正当業務行為として認められています。また、検知したC&CサーバのIPアドレスとポート番号をICT-ISACなどの信頼がおける事業者団体にサイバーセキュリティ対策のために提供できることが整理されています。

この整理に基づいて、2022年度と2023年度に、C&Cサーバを実際に通信事業者のフロー情報を用いて検知するとともに、検知結果について事業者間で共有するための実証事業を行っています。フロー情報からC&Cサーバを見つける方法には、グラフマイニングという方法、機械学習を用いた手法などがあります。2022年の実証でもC&Cサーバを数多く検出し、マルウェア系統のMirai系であるとか、Emotet系であるとか、そういうものに関係するC&Cサーバと想定される場合などについても分析ができています。また、通信事業者によって検出できるC&Cサーバにも違いが見られることから、複数の通信事業者が連携して情報を共有する仕組みができればより多くのことが分かるようになるのではないかと期待されています。なお、検知したC&Cサーバの所在国の推定では、日本から来ているものも当然ありますが、ヨーロッパ、アメリカから来ているものもたくさんあります。

一般にC&Cサーバの情報は、いわゆるオシント情報（Open Source Intelligence：オープンソースインテリジェンスの略であり、特定の情報要件に対処する目的で、一般に入手可能な情報を収集し、利用し、適切な対象者に適時に普及させた情報）で公表された情報もありますが、公表されるまでに一定の時間がかかります。今回のフロー情報によるC&Cサーバの検知においては、オシント情報で公表されるよりも前に検知されたものも沢山あることから、今後より早い対応を可能とする利点等も含めこの試みは期待されています。

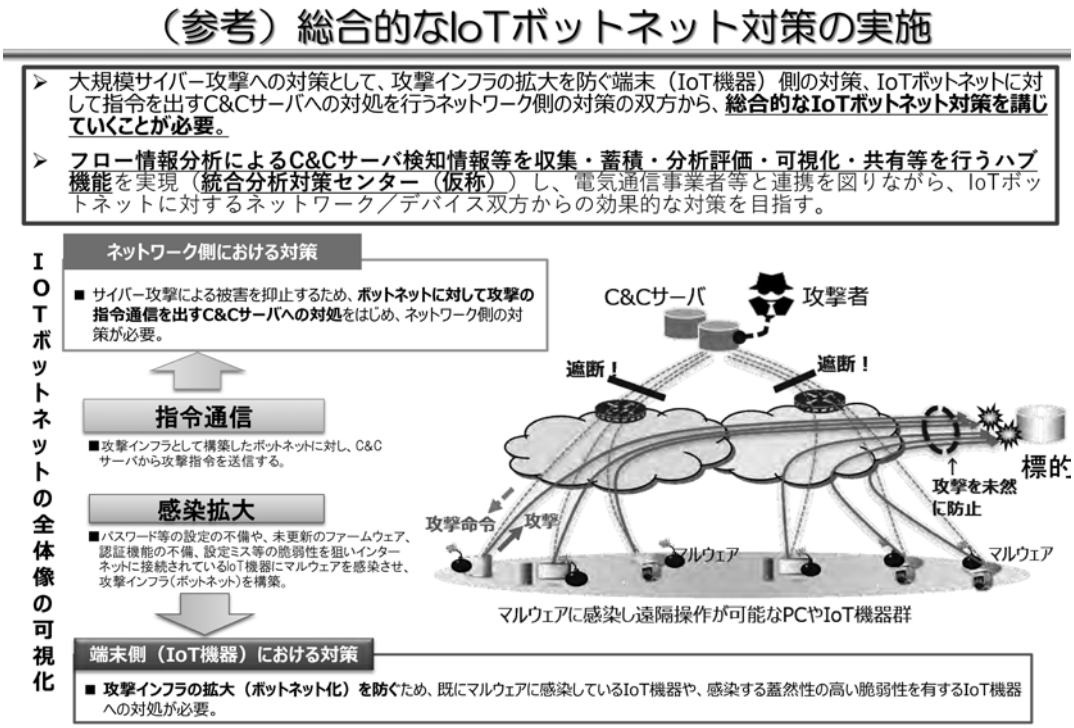
このように、端末側でNOTICEの取組を進めていくとともに、ネットワーク側でC&Cサーバを割り出して対策するなど、両方を連携した形で行うことにより、総合的なIoTボットネット対策が進むことが期待されます。今後とも、関係の事業者にもご協力いただきながら、このボットネット、攻撃側のインフラの状況を可視化して、適切な対応が打てるように取組みを推進していければと思っています（図表４）。

その他の対策（情報通信ネットワークの安全性・信頼性の確保）

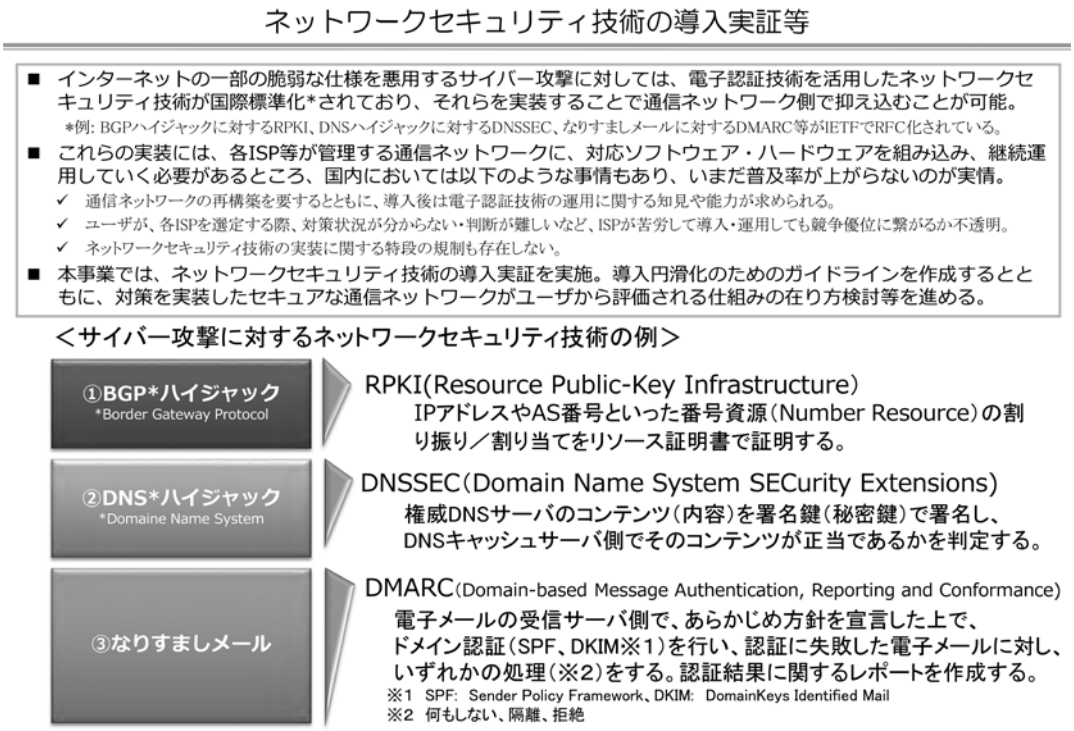
その他にも、さまざまな情報通信ネットワークにおけるサイバーセキュリティ対策を行っております。

例えば、脆弱な仕様を悪用するサイバー攻撃に対しては、電子認証技術を活用したネットワークセキュリティの技術が国際標準化されており、それらを実装することによって、通信ネットワーク側で抑え込むことが可能になっております。このネットワークセキュリティ技術として大きく３つあり（図表５）、たとえばBorder Gateway Protocol（BGP）経路のハイジャックに対してResource

図表４



図表５



Public-Key Infrastructure（RPKI）という技術、またDomain Name System（DNS）ハイジャックとか、DNSポイズニングとかいったDNSに対する攻撃については、Domain Name System Security Extensions（DNSSEC）とよばれる信頼がおけるDNSサーバかどうかということを確認する技術があります。更に、なりすましメールに対しては、Domain-based Message Authentication, Reporting and Conformance（DMARC）というドメイン認証技術が有効だと言われています。

これらの技術については、わが国において、必ずしも普及率が高くない部分があり、このネットワークセキュリティ技術が普及していくように、関係の事業者とも連携しながら、検討と取組を進

めています。

RPKIについては、日本国内でも、Route Origination Authorization（ROA）という経路ハイジャック抑止となる経路認証技術は導入が70%ぐらい進んでいますが、Border Gateway Protocol（BGP）の経路情報の検証のRoute Origin Validation（ROV）という技術についてはまだ導入が４%程度で、こちらの導入も進めていくことが重要です。

DNSSECについては、日本の普及状況は15%にとどまり、最近ではDNSサーバを使ったサイバー攻撃が多くなっているため、普及率を上げていくことが必要です。

DMARC技術では、送信ドメイン認証の技術であるSender Policy Framework（SPF）やDomain Keys Identified Mail（DKIM）を使ってなりすましメールかどうかを認証する技術があり、それを活用してなりすましメールを削除するようセキュリティ・ポリシーを設定可能です。DMARC技術は、日経255企業の中でも30%の導入率で、たとえば米国の88%、オーストラリア77%、デンマーク100%と比べると、まだ低い状況です。

内閣府の消費者委員会からも、フィッシングメールの受信防止対策として、DMARCは有効だとして、この普及率を上げることが必要だという意見が出されています。総務省としても、物流団体の連合会や全銀協に対してDMARCの導入に関する依頼文を送付するとともに、経産省とも連携してクレジットカード事業者に対してDMARCの導入をはじめとするフィッシング対策強化を要請するなど働きかけを進めております。

総務省の今年度の取組としては、中小のISPを含めて通信事業者にこれら技術導入を進めていただくため、RPKIとDNSSECとDMARCと３つの技術について、それぞれ、体験コース、実験コース、導入検証コースを設け、実際に技術に触れ、知り、導入に向けて検討いただくという取組をしております。また、今後、導入方法についてのガイドラインについても、いただいたご意見等も踏まえつつ検討しております。

「サプライチェーンリスクに対する取組み」としては、Software Bill of Materials（SBOM）の導入があります。オープンソースのソフトウェアをつなぎ合わせてソフトウェアを作ることも多く、その部品の中に脆弱性があると、ソフトウェア全体が脆弱になってしまうことがあります。ソフトウェアの部品それぞれに信頼性が置けるかどうかを確認できるような仕組みとしてSBOMがあり、他産業の導入例を見ながら、通信分野でどのように導入を進めるかを調査しています。

スマートフォンのアプリケーションの中には、利用者の意図に反してそのプライバシー性の高い情報を外部送信するケースもあります。アプリケーションについて技術的に解析し検証を行う観点から、アプリの挙動についての動的解析、ソースコードも読み解いて分析する静的解析に関する技術的実証を進めています。

クラウドサービスの普及が進んでいますが、利用者側の設定ミスによって、個人情報や、秘密にすべき情報が外部に見えてしまう等問題が発生する場合もあるため、設定ミスを抑止・防止するための対策を取っていく必要があります。クラウドサービスの利用者側と提供者側の双方でそれぞれどういう対策を取ればいいのかをまとめて、ガイドラインを策定し、2022年秋に公表しております。

また、政府が調達する際に信頼がおけるクラウドサービスを調達する必要があるため、政府情報システムのためのセキュリティ評価制度、Information System Security Management and Assessment Program（ISMAP）という制度を総務省、経産省、NISC、デジタル庁と４省庁で連携して運用しています。現在約50サービスがISMAPリストに登録されており、各政府機関とともに地方自治体などにも参照いただければと考えています。

このISMAP制度については、影響度の低い業務に用いられるSaaSサービスに対してよりライトな仕組みとしてISMAP-LIU（for Low-Impact Use）を2023年秋に導入しました。ISMAPの制度全体については、不断に今後も見直しを進めていく予定です。

トラストサービスについては、わが国はData Free Flow with Trust（DFFT）を提唱しており、それを支えるものとして、送信元のなりすましや、データの改ざんを防止する仕組みの重要と考えております。

様々なトラストサービスあり、電子署名については、電子署名法をデジタル庁が所管しています。

タイムスタンプについては、総務大臣が認定制

度を設けており、現在３者が認定されています。このタイムスタンプは、電子帳簿等保存制度において総務大臣による認定制度に基づくタイムスタンプを使ったファイルを使えると位置づけられ活用されております。

更に、個人の署名・実印の代わりとなりうる電子署名に対し、いわば組織の角印（実印）としてある組織が発行した文書であることを証明するものとしてeシールが位置づけられます。総務省は2021年６月に「eシールに係る指針」を公表しており、2023年９月にeシールに係る検討会を設置して国による認定制度の創設を含めて議論していく予定です（図表６）。

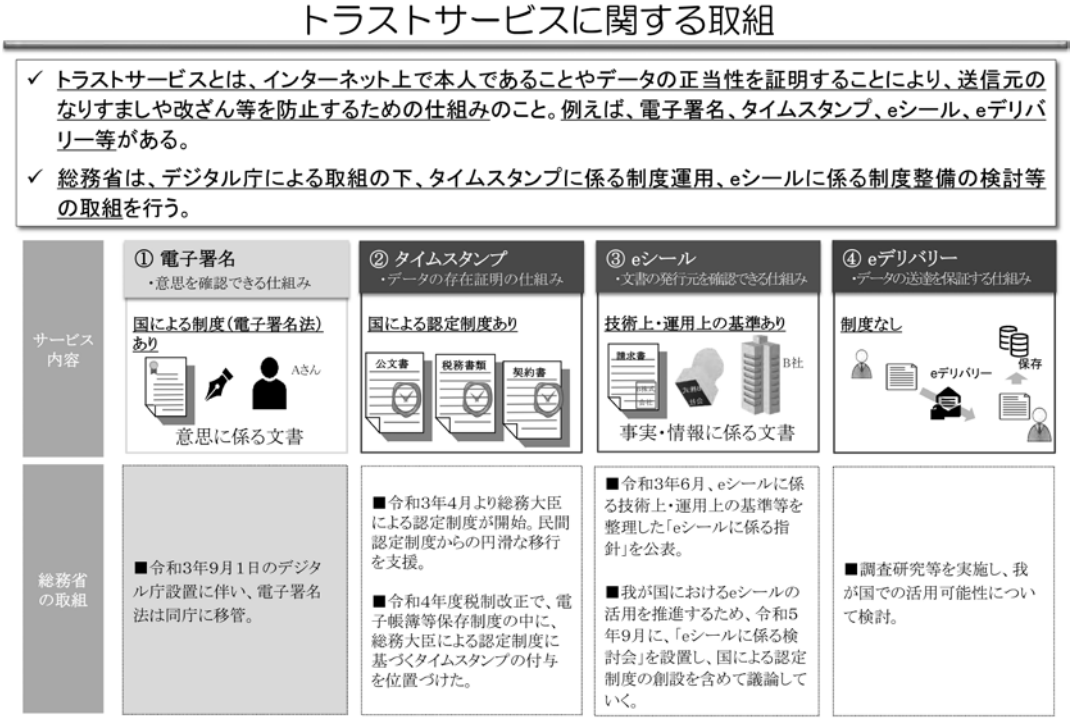
「サイバーセキュリティに関する自律的な対処能力の向上」については、NICTにおいて、CYNEX（サイバーセキュリティ統合知的・人材育成基盤）という取組をしております。今年度から本格始動しており、特にサイバーセキュリティの研究開発のために情報を集めて分析をする体制を強化するとともに、人材育成についても進める結節点となることを目指しています（図表７）。

情報収集が必要な背景としては、サイバーセキュリティ対策に関し我が国が「データ負け」の状態となっていることが問題として指摘されます。例えば、我々が使用するクラウドサービスやサイバーセキュリティ対策サービスの大半が海外製のものであり、国内に対するサイバー攻撃に関する情報であってもこれら海外事業者に情報が集約されており必要に応じてこれらの情報を海外事業者から購入する状況になりつつあると指摘されます。そのため、日本国内に対するサイバー攻撃に関する情報を、国内においても情報として把握・集約して、分析できる体制を維持強化することが、重要になっています。

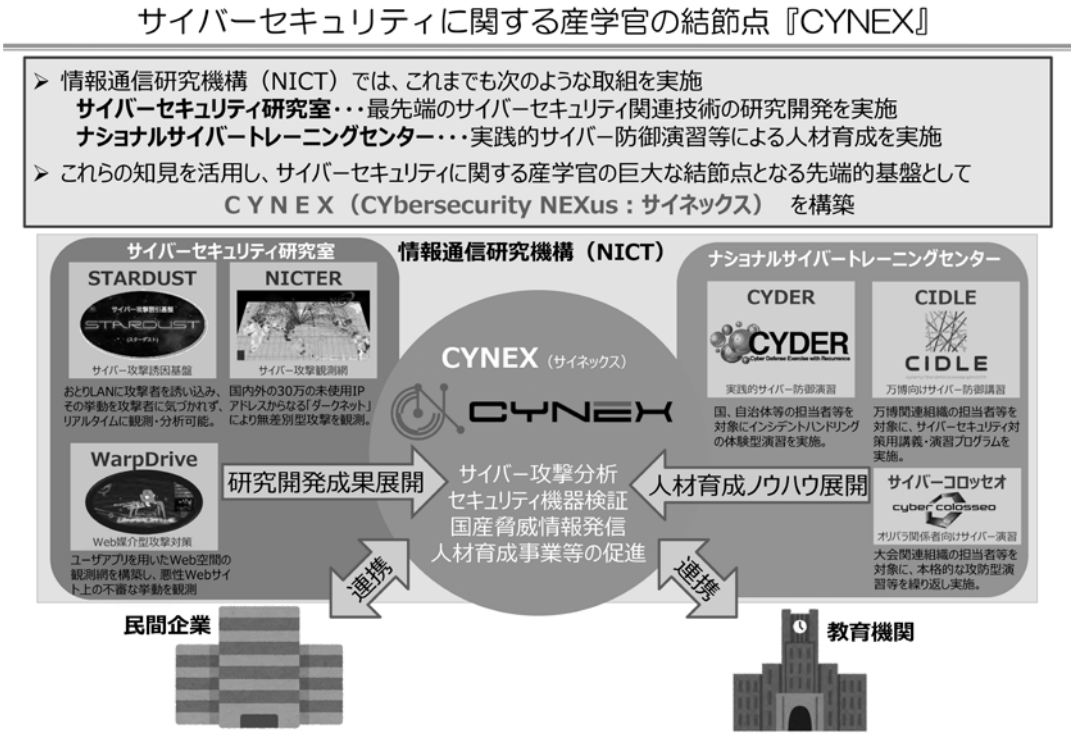
NICTにおけるCYNEXでは、サイバー攻撃について情報を集めた上で共同で解析をするコミュニティを作ることや、国産のセキュリティ製品のテストをしています。更に、SOC（Security Operation Center）人材のような高度な人材の育成をするとともに、研修向けの演習基盤を開放して国内でセキュリティ人材の育成事業を活性化しようと考えています。

更に、「データ負け」の状況に対応するために、CYXROSS（政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業）という取組も推進しようとしています。政府LANは今後クラウドベースになっていく中で、海外事業者のセキュリティサービスの提供は受けつつも、日本国内でどんな攻撃が起こっているのかを日本国内でも把握し情報を集約できるように、安全性、透明性を検証可能なセンサーを、政府端末に導入した上で、政府関係機関が、NICTが情報

図表６



図表７



図表８

集約し、分析した情報を使って、サイバー攻撃対策を行うという構想です。

令和５年度から、まず総務省の約7,000台の端末に導入し、情報を集約して分析していく予定です。今後多くの政府機関に入れていただいて、分析を強化していきたいと考えています。

人材育成については、サイバー攻撃に対応していくための重要性から、NICTに「ナショナルサイバートレーニングセンター」を設置して、大きく３つの柱で取り組んでいます（図表８）。

１つ目の柱としては、CYDER（サイダー）と呼ばれる、国や地方公共団体とかを対象とした、実践的なサイバー防御演習です。年間100回、3,000

人の規模で、全国全ての都道府県においてこの演習をやっております。実際に実機を操作をし、例えば自治体等がランサムウェア等のサイバー攻撃を受けた時に、どのように対応すればいいのか、チームで対応しながら学ぶコースで、評判が高いものです。

２つ目の柱が、CIDLE（シードル）として、2025年の開催に向けて準備されている大阪関西万博における対応のための「万博向けのサイバー防御講習」です。2020年東京オリンピック/パラリンピック大会の際に実施した「サイバーコロッセオ」のレガシー等も活用して今回も協力していきます。

３つ目の柱が、若手人材を対象とした「セキュリティイノベーター育成プログラム」としてのSecHack365（セックハックサンロクゴ）となります。

国際連携の推進

サイバー空間には国境がなく、サイバーセキュリティの確保のためには、国際連携が重要だと考えています（図表９）。

有志国との二国間連携とか、多国間の連携もそれぞれ重要であり、その取組を進めていますが、重視しているのが、図表９の④のところです。

ASEANとの協力により、開発途上国に対する能力構築支援として、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）を設立して、多くのASEAN関係者に、日本国内で実施している能力構築のCYDERを英語化して、受講していただいています。

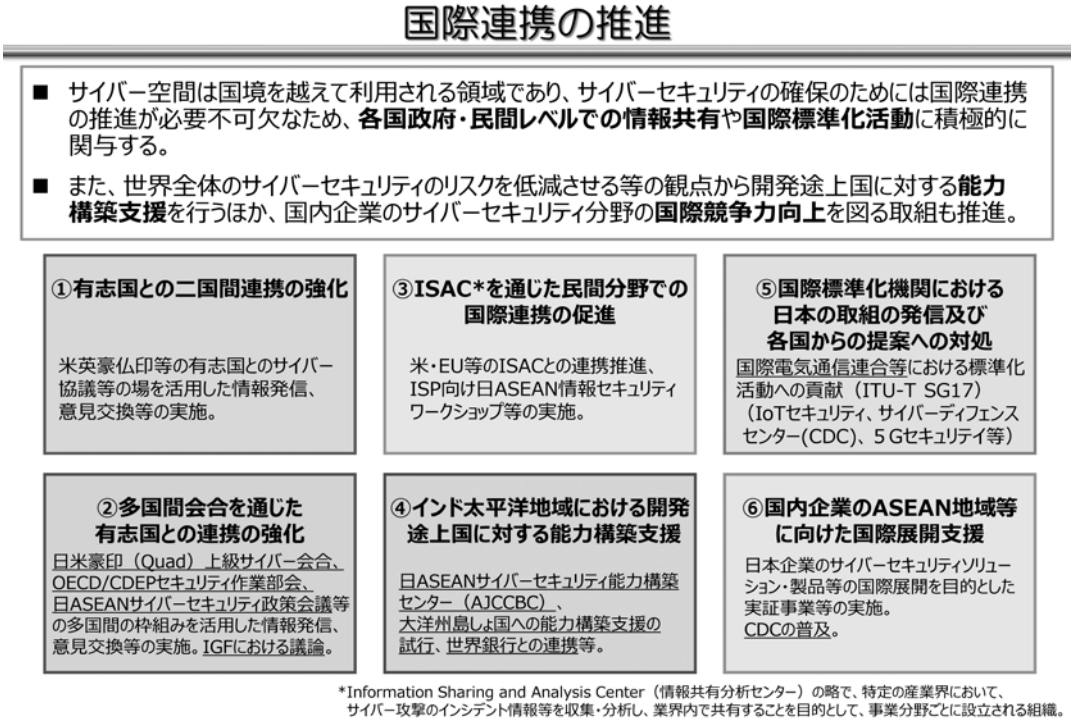
AJCCBCには、今までに1,200人を超える参加があり、サイバーセキュリティの演習としては、CYDERの英語版による実施や、マルウェア解析やデジタルフォレンジックといったプログラムもあります。この他、Cyber SEA Gameということで、学生や若手技術者がサイバー攻撃の対処能力を競い合うゲーム形式の大会も、年１回開催しております。

CYDERを英語化したプログラムは非常に好評で、今後、太平洋島しょ国の能力構築支援のため、2023年冬から太平洋島しょ国の国々への研修を試行的に開始する予定です。そのほか、世界銀行との連携を通じた取組みの検討も進めており、2023年10月に京都で開催される「インターネットガバナンスフォーラム」の中でも能力構築支援の取組みに関してご紹介する予定です。

セキュリティに関する普及啓発

普及啓発についても、従来からいろんな取組を

図表９



しております。

総務省が作成している「スマートシティセキュリティガイドライン」は、2023年度に見直しをする方向で検討しています。

「テレワークセキュリティガイドライン」については、2004年に最初に策定し、2020年のコロナ禍以降、テレワークも一般的に普及してきた状況も踏まえて、2021年に改訂版を出しました。また、「中小企業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）」についても、2022年５月に改訂版を出しました。

「地域に根付いたセキュリティコミュニティ（地域SECUNITY）」の形成を促進しようとしており、地方ではサイバーセキュリティの対策に関する情報が不足しているということで、これに対応するために、経産省、総務省と、また地方公共団体、都道府県県警などが連携して、取組を進めています。地域の企業向けに、定期的なセミナー、インシデント演習、セキュリティ関連の情報提供などを行っています。

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」は、2023年３月に公表しております。サイバー攻撃被害を受けた組織が、どこからどのような攻撃を受けたのかという情報を、専門機関の間で共有していれば、二次被害を防ぐことができます。情報共有がうまくいくために、情報共有を進めるためのガイダンスを策定しました。

「無線LANのセキュリティガイドライン」についても、利用者向けと提供者向けを公表しています。

「国民のためのサイバーセキュリティサイト」は、以前からサイトを改定しており、総務省のホームページの中で一番閲覧数が多いものです。このサイトについても、今後も分かりやすく見直していきたいと思っています。