ICT サイバーセキュリティ総合対策 2022

2022 年８月

総務省　サイバーセキュリティタスクフォース

目次

はじめに

サイバーセキュリティタスクフォース（座長 情報セキュリティ大学院大学学長 後藤厚宏）は、2020 年東京オリンピック・パラリンピック競技大会（以下、「2020 年東京大会」という。）の開催を見据え、サイバーセキュリティの課題を整理し､必要な方策を推進することを目的として 2017 年１月から開催している。その後、2021 年７月には「ICT サイバーセキュリティ総合対策 2021」（以下、「総合対策 2021」という。）を取りまとめた。

2020 年東京大会の終了を踏まえ、2022 年３月には、本タスクフォースの開催要綱を改正し、2020 年東京大会の成果や「サイバーセキュリティ戦略」（2021 年９月 28 日閣議決定）を踏まえつつ、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大などの動向に対応したサイバーセキュリティに係る課題の整理や、情報通信分野において講ずべき対策や既存の取組の改善など、引き続き幅広い観点から検討を行っていくこととなった。

本文書は､「総合対策 2021」の策定後、昨今の国際情勢の緊迫化を含め、サイバー攻撃リスクの拡大等の状況変化を踏まえた議論を経て､「ICT サイバーセキュリティ総合対策 2022」として、必要な改定を行ったものである。本文書を羅針盤として､総務省が関係機関や民間企業等と連携し､我が国のサイバーセキュリティ政策に率先して取り組むことを期待する。

Ⅰ　サイバーセキュリティを巡る最近の動向

１．サイバーセキュリティに関する政策動向

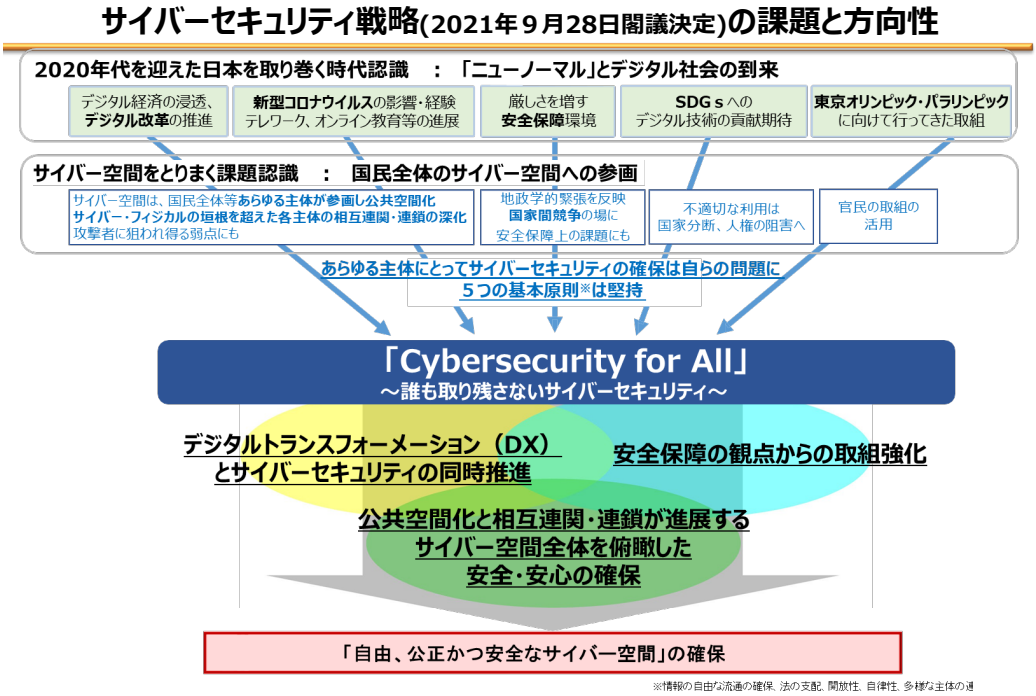
「総合対策 2021」においても記載されているとおり、政府においては、社会全体のデジタル・トランスフォーメーション（DX）や、サイバー空間の公共空間化に伴う「誰一人取り残さない」サイバーセキュリティの確保（“Cybersecurity for All”）に向けた取組が継続的に推進されている。

「総合対策 2021」策定後の政府内での主な動向は以下のとおりである。

・　サイバーセキュリティ戦略の策定

2021 年９月に「サイバーセキュリティ戦略」[1]が閣議決定された。同戦略においては、“Cybersecurity for All”をコンセプトに、サイバーセキュリティ基本法（平成 26 年法律第 104 号）[2]の目的達成のための施策として、①DX とサイバーセキュリティの同時推進、②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、③安全保障の観点からの取組強化が掲げられている。また、同戦略に基づき、官民連携に基づく重要インフラ防護の一層の強化を図るため、「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」[3]（2017 年４月 18 日サイバーセキュリティ戦略本部決定）の改定に向けた議論も進んでいる。

[1] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf
[2] https://elaws.e-gov.go.jp/document?lawid=426AC1000000104
[3] https://www.nisc.go.jp/pdf/policy/infra/infra_rt4_r2.pdf



・　デジタル庁の設置

2021 年９月にデジタル庁が設置された。デジタル社会形成基本法（令和３年法律第 35 号）[4]第 37 条第１項に基づき作成された「デジタル社会の実現に向けた重点計画」[5]（2022 年６月７日閣議決定）では「誰一人取り残されない、人に優しいデジタル化」を進めることとされており、デジタル化の基本戦略の１つとしてサイバーセキュリティの確保を含む「安全・安心の確保」が掲げられている。

・　経済安全保障推進法の成立

2022 年５月には、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第 43 号）が国会で成立の上、公布された。

総務省は、これらの政策動向を踏まえ、サイバー空間の基盤となる情報通信ネットワークの安全性・信頼性の確保及び利用者が安全・安心に利用できる情報通信サービスの実現に向けた施策を推進することが求められる。

[4] https://elaws.e-gov.go.jp/document?lawid=503AC0000000035_20210901_000000000000000

[5] https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/d130556b/20220607_policies_priority_outline_05.pdf

２．サイバーセキュリティ全般を巡る動向

「総合対策 2021」策定後のサイバーセキュリティ全般を巡る動向は以下のとおりである。

・　2020 年東京オリンピック・パラリンピック競技大会の終了

公益財団法人東京オリンピック・パラリンピック競技大会組織委員会によれば、2021 年７月から９月にかけて開催された 2020 年東京大会期間中を通し 4.5 億回のサイバー攻撃を観測したが[6]、関係者の努力の結果、幸い、大会運営に影響を及ぼすサイバー攻撃は確認されなかった。

2020 年東京大会における教訓を踏まえ、今後も我が国全体としてサイバー攻撃への対処能力の向上を図っていく必要がある。

・　サイバー攻撃リスクの拡大

国内では、2021 年下半期のランサムウェア被害の報告件数は、2020 年下半期に比べて約４倍[7]、2022 年７月のフィッシング報告件数は、2021 年７月に比べて約３倍[8]に増加しており、大規模サイバー攻撃観測網である NICTER において観測されたサイバー攻撃関連の通信数[9]も引き続き増加傾向（各 IP アドレスに約 18 秒に１回の通信）にある。また、2021 年 12 月には Apache Log4j の脆弱性を狙う攻撃が大量に観測された[10]ほか、2022 年２月には、マルウェア Emotet の感染再拡大も発生した[11]。

---

[6] 公益財団法人東京オリンピック・パラリンピック競技大会組織委員会第 47 回理事会資料
https://www.tokyo2020.jp/image/upload/production/47EBMeeting6.pdf

[7] 令和３年におけるサイバー空間をめぐる脅威の情勢等について（2022 年４月７日 警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

[8] 2022/07 フィッシング報告状況（2022 年８月３日 フィッシング対策協議会）
https://www.antiphishing.jp/report/monthly/202207.html

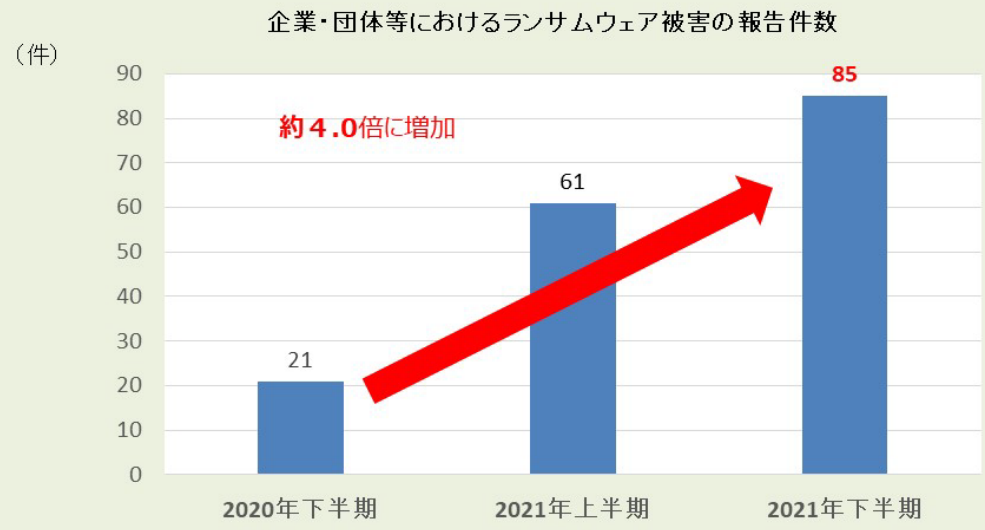
[9] NICTER 観測レポート 2021（2022 年２月 国立研究開発法人情報通信研究機構）
https://www.nict.go.jp/cyber/report.html

[10] Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起（2021 年 12 月 11 日 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC））
https://www.jpcert.or.jp/at/2021/at210050.html

[11] マルウェア Emotet の感染再拡大に関する注意喚起（2022 年２月 10 日 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC））
https://www.jpcert.or.jp/at/2022/at220006.html

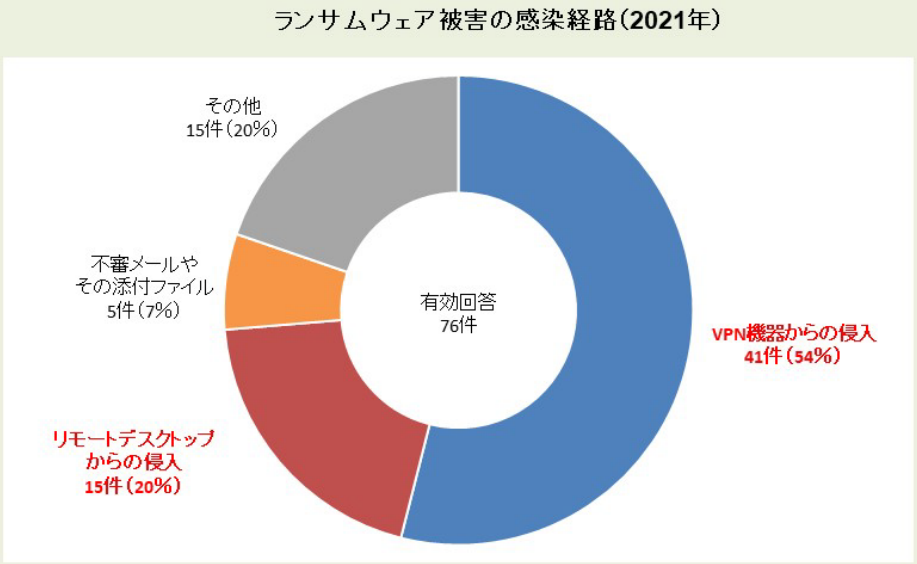
ランサムウェア攻撃の増加①

出典：「令和3年におけるサイバー空間をめぐる脅威の情勢等について」（令和4年4月　警察庁）より作成



ランサムウェア攻撃の増加②

出典：「令和3年におけるサイバー空間をめぐる脅威の情勢等について」（令和4年4月　警察庁）より作成

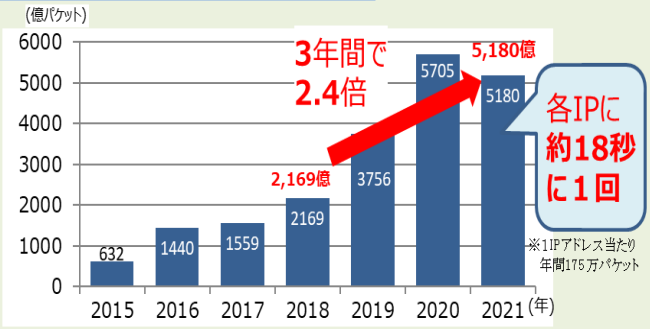


フィッシングの増加①

フィッシングメールの報告数とフィッシングサイトURL数

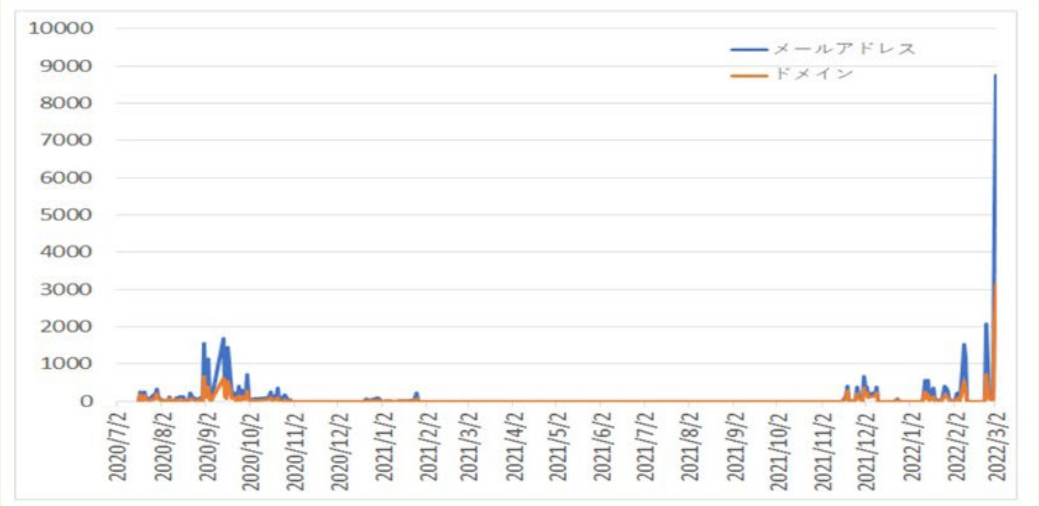
出典：フィッシング対策協議会

NICTERで１年間に観測されたサイバー攻撃関連の通信数



※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されたため、例外的にパケット数が多かったものと推測

Emotetに感染しメール送信に悪用される可能性のある .jpメールアドレス数の新規観測の推移 (外部からの提供観測情報、2022年3月3日更新)



JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」
https://www.jpcert.or.jp/at/2022/at220006.html
(2022年3月14日更新)

社会に大きな影響を与えたサイバー攻撃事例としては、2021 年 11 月に公立病院がランサムウェアに感染して電子カルテシステムが一時使用できなくなった事例や、2022 年２月に大手自動車メーカーのサプライチェーンに属する部品メーカーがランサムウェアに感染して当該大手自動車メーカー全体の工場稼働が停止した事例等が挙げられる。我が国全体として、地域や業種、事業規模を問わず、サイバー攻撃のリスクが高まっていると言える。

世界全体でも、ロシアによるウクライナ侵略等の国際社会における安全保障を巡る状況の緊迫化に伴って、各国で政府機関や重要インフラを狙った攻撃が多く発生している。米国及び EU 等は、2022 年２月に、ロシアがウクライナ侵略と同時に、欧州にある米国企業が管理する通信衛星用の地上アンテナ等に対してサイバー攻撃を行ったとして、同年５月に、ロシア政府を非難する共同声明を発表した。

また、米国では、2021 年５月にパイプライン企業がランサムウェアに感染してパイプラインを一時停止した事例などを受けて、同年 10 月に、日本を含

む 30 か国以上が参加するランサムウェアの脅威に対するための国際会議を開催し、ランサムウェアを「世界的な脅威」であるとする共同声明を発表した。

こうした状況を踏まえ、総務省を含む関係省庁では、重要インフラ事業者や地方公共団体等に対して、2022 年２月 23 日、３月１日、３月 24 日、４月 25 日の４度にわたって、①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復などを内容とするサイバーセキュリティ対策の強化を求める注意喚起を行った。政府機関や重要インフラ事業者、地方公共団体をはじめとする企業・団体等においては、引き続き、サイバー攻撃の脅威に対する認識を深めるとともに、適切な対策を講じることが求められる。

・　情報通信ネットワークの重要性の更なる高まり

新型コロナウイルス感染症の感染拡大は、我が国においてもデジタル化を大きく加速させる契機となった。テレワークやクラウドサービスの利用が更に拡大し[12]、また、ネットワークに接続される IoT 機器数も引き続き増加している[13]中、我が国のインターネット上を流通するトラヒックの推定量はここ３年で２倍以上に増加しており[14]、社会全体のデジタル活用（依存）がますます進展している。

上述のとおり、サイバー空間があらゆる主体が利用する公共空間となる中、デジタル化を支える情報通信ネットワークは、今や国民生活や経済活動の重要かつ不可欠な基盤となり、その重要性は更に一段と高まっている。2021 年 10 月に大手携帯キャリアにおいて通信サービス障害が発生して、延べ約 1290 万人が影響を受けた事例、同年９月に大手クラウドサービスにおいて障害が発生し、金融機関や航空会社のサービスが影響を受けた事例に見られるように、情報通信ネットワークの機能に支障が生じた場合には、社会・経済に多大な影響が及ぶ状況となっている。

また、前述した国際情勢の変化に伴い、サイバー空間自体が、国家間の競争・衝突の場となる中で、情報通信ネットワークは、サイバー攻撃の標的や経路、偽情報（Disinformation）を流布する場にもなり得るとともに、市民の間でリアルタイムに情報を共有するためのツールにもなり得るものである。

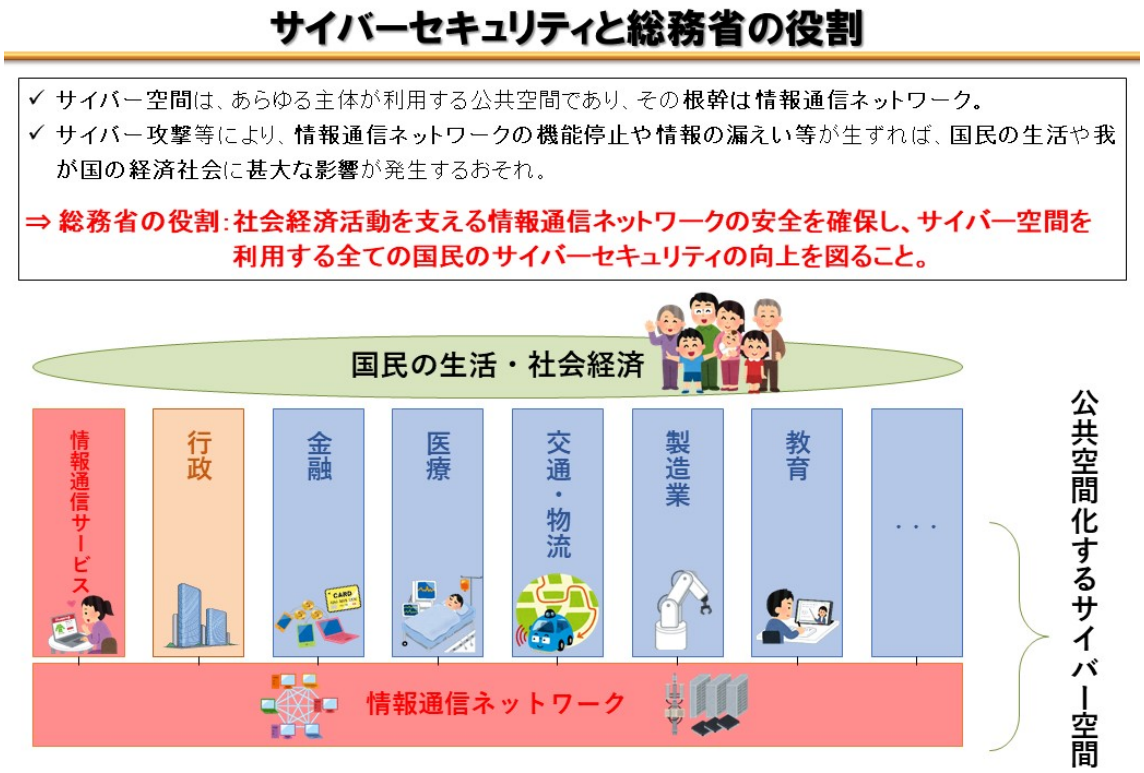
---

[12] 令和３年通信利用動向調査の結果（2022 年５月 27 日 総務省）
https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000158.html

[13] 情報通信白書令和３年版（総務省）図表 0-2-2-29　世界の IoT デバイス数の推移及び予測
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd105220.html

[14] 我が国のインターネットにおけるトラヒックの集計・試算 2021 年 11 月のトラヒックの集計結果（2022 年２月４日 総務省）
https://www.soumu.go.jp/main_content/000791761.pdf

このような状況のもと、情報通信ネットワークの安全性・信頼性を確保することは一層重要となっている。



Ⅱ　「ICT サイバーセキュリティ総合対策 2022」として今後取り組むべき施策

Ⅰで示した状況変化及び認識を踏まえ、「情報通信ネットワークの安全性・信頼性の確保」、「サイバー攻撃への自律的な対処能力の向上」、「国際連携の推進」及び「普及啓発の推進」の４点を柱として、総務省において今後重点的に取り組むべき施策を「ICT サイバーセキュリティ総合対策 2022」として取りまとめることとする。

１．情報通信ネットワークの安全性・信頼性の確保

（１）情報通信ネットワークのサイバーセキュリティ対策の推進

Ⅰで述べたように、サイバー空間を支える情報通信ネットワークは、国民生活や経済活動の基盤となるものであり、デジタル活用の進展とともに、その重要性が増している。「サイバーセキュリティ戦略」においても、国民が安全で安心して暮らせるデジタル社会の実現のため、「安全かつ信頼性の高い通信ネットワークを確保するための方策を検討する」こととされている。総務省では、これまでも、情報通信ネットワークのサイバーセキュリティ対策を推進してきたが、サイバー攻撃の大規模化・巧妙化・複雑化も踏まえ、今後、電気通信事業者を通じたネットワーク側の対策及び利用者を通じた端末（IoT）側の対策

を中心として、施策を充実させることが求められる。また、広く普及が進むクラウドサービスや 5G サービスのセキュリティ確保、国内各地域において構築が進みつつあるスマートシティのセキュリティ確保、放送設備のセキュリティの確保に加えて、これらを横断する課題としてのサプライチェーンリスク対策等の取組を強化することが必要である。

ア. 電気通信事業者による積極的サイバーセキュリティ対策の推進

【現状】

（サイバー攻撃に対する電気通信事業者の積極的な対策）

2021 年 11 月に、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、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ついて検討を行う「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、①平時におけるフロー情報[15]の収集・蓄積・分析による C&C サーバ[16]である可能性が高い機器の検知については正当業務行為、②フロー情報を収集・蓄積・分析して検知した C&C サーバに関する情報の共有については通信の秘密の保護規定に直ちに抵触するとまではいえないとの整理[17]を行った。

[15] ネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラヒックに係るデータのうち、IP アドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報。

[16] Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと。

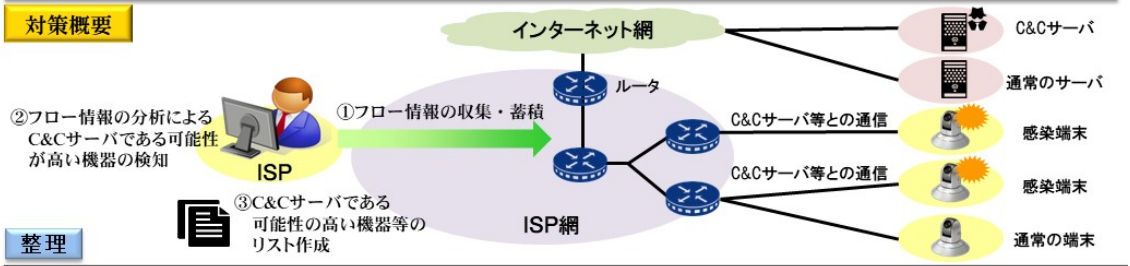
[17] 「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ」（2021 年 11 月）
https://www.soumu.go.jp/main_content/000779208.pdf

検討課題（１）平時におけるフロー情報の収集・蓄積・分析によるC&Cサーバである可能性が高い機器の検知

論点

ISPがサイバー攻撃に予防的に対処するため、平時から、ISPが、自らのネットワーク内の通信トラフィックに係るデータを収集・蓄積・分析し、C&Cサーバである可能性が高い機器の検知を行うことが考えられる。具体的には、現状多くのISPにおいて、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IPアドレス及びポート番号等の情報（フロー情報）を、通信の傾向把握のために収集・活用しているところであるが、これを分析して未知のC&Cサーバの検知を行うことが考えられる。このような取組は、通信の秘密との関係上どのように整理が可能か。

対策概要



整理

以下のことから、本件対策は、正当業務行為として違法性が阻却される。

「目的の正当性」：本件対策は、DDoS攻撃等のC&Cサーバを起点とするサイバー攻撃が発生する前から未知のC&Cサーバ等を検知し、その検知した情報をもとに、各ISPにおいて適切な対処ができるようにすることにより、自己の電気通信役務の提供への重篤な支障の発生を未然に防止し、または、その被害の拡大を最小限に抑え、電気通信役務の円滑な提供を確保するための措置であり、目的の正当性を認めることができる。

「行為の必要性」：サイバー攻撃の複雑化・巧妙化が進んで攻撃の頻度は高まり、ISPの提供する電気通信ネットワークに対するC&Cサーバを起点としたサイバー攻撃がいつ行われてもおかしくない状態にさらされている等、現在の電気通信ネットワークを取り巻く状況においては、行為の必要性が認められる。

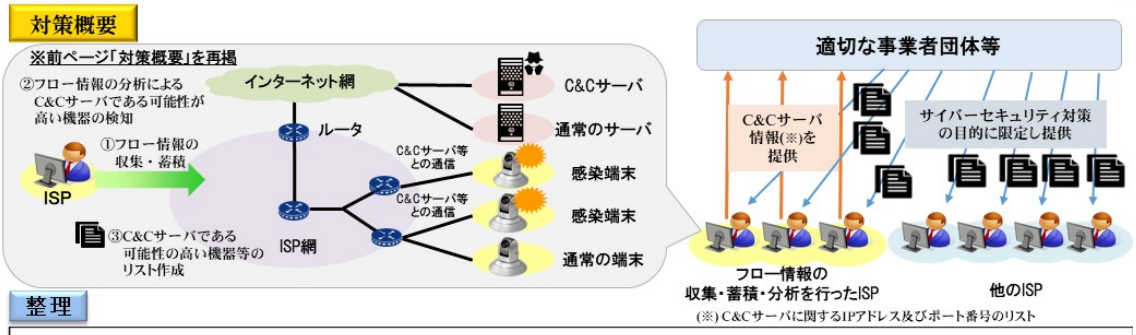
「手段の相当性」：必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報をC&Cサーバ検知以外の用途で利用しない場合には、手段の相当性が認められる。

検討課題（２）フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有

論点

各ISPがサイバー攻撃に対処できるようにする観点から、一のISPが自らの電気通信ネットワーク内のフロー情報の収集・蓄積・分析によって検知したC&Cサーバに関する情報（IPアドレス、ポート番号）を、適切な事業者団体等に提供することが考えられる。このような取組は、通信の秘密との関係上どのように整理が可能か。

対策概要



整理

本件において対象とされるC&Cサーバに関する情報は、必要最小限のフロー情報について、C&Cサーバを検知する目的のみのために集合的に分析した結果として得られたC&Cサーバに関するIPアドレス及びポート番号を取りまとめてリスト化したものである。すなわち、個別の通信と切り離され、個々の通信がいつ誰に対して行われたかといった個々の通信の構成要素を明らかにすることにつながらないものである。

したがって、このように、C&Cサーバに関するIPアドレス及びポート番号のリストの情報のみを、サイバーセキュリティ対策を行うために必要最小限の情報として、適切な事業者団体等に提供することは、通信の秘密の保護規定に直ちに抵触するとまではいえないと考えられる 。

上記の整理も踏まえ、2022 年度において、以下について、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に関する総合実証を実施している（令和３年度補正予算）。

- 電気通信事業者におけるフロー情報分析による C&C サーバの検知技術
- 電気通信事業者をはじめとするサービス提供者側からの継続的な対策を講じるための必要事項を整理するべく、自動巡回による機械的処理を活用した悪性 Web サイト（フィッシングサイト等）の検知技術・共有手法
- 現在のインターネットを構成する根幹技術である BGP や DNS、電子メールに関する効果的な脆弱性対策の手法として標準化されており、国際的にも実装が進みつつあるにも関わらず、我が国では導入が進んでいない RPKI[18]や DNSSEC[19]、DMARC[20]等のネットワークセキュリティ技術の導入に係る技術的な課題の解決

（電気通信事業者におけるガバナンス確保）

電気通信事業者におけるサイバー攻撃や情報漏えい等のリスクの高まりを踏まえ、総務省では、2021 年５月に「電気通信事業ガバナンス検討会」を設置し、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についての議論を行った。同検討会における報告書[21]に基づき、①利用者の利益に及ぼす影響が大きい電気通信役務を提供する電気通信事業者に対する特定利用者情報の適正な取扱いの義務付け、②電気通信事業者間連携によるサイバー攻撃対策の促進（会員である電気通信事業者が、DDoS 攻撃等のサイバー攻撃の送信先となった場合に加えて、攻撃の準備行為の標的となった場合も、認定協会業務の対象とするもの）、③重大事故等のおそれがある事態に関する報告制度等の規定を含む、「電気通信事業法の一部を改正する法律」が第 208 回国会において成立した。

【今後の取組】

（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推進）

2022 年度に実施する、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に関する実証事業については、以下のとおり、成果を踏まえて新たな内容を盛り込みつつ、2023 年度も引き続き実証事業を継続することが適

---

[18] RPKI（Resource Public-Key Infrastructure）：自律ネットワークの IP アドレスや AS 番号を電子証明書で検証し、通信経路の乗っ取り等を防止する技術

[19] DNSSEC（DNS Security Extensions）：ドメインネームと IP アドレスの紐付けを電子証明書で検証し、サーバのなりすまし等を防止する技術

[20] DMARC（Domain-based Message Authentication Reporting and Conformance）：電子メールの送信元ドメインの正しさを検証し、なりすまし等の場合は自動的に処理する技術

[21] 「電気通信事業ガバナンス検討会　報告書」（2022 年 2 月）
https://www.soumu.go.jp/main_content/000794590.pdf

当である。

- フロー情報分析による C&C サーバ検知の手法については、検知精度の高度化を図るとともに、検知結果の電気通信事業者間の共有の実証を行う。
- 悪性 Web サイトの検知技術・共有手法については、悪性 Web サイト情報の収集・分析を継続するとともに、収集・分析結果を実際のセキュリティサービス等に活用した際の効果検証を行う。
- RPKI、DNSSEC、DMARC 等のネットワークセキュリティ技術については、我が国では広く電気通信事業者等に普及するには至っていない状況にあるところ、実証事業によって、技術的な観点にとどまらない普及の方策等を検討する。

また、通信の秘密に配慮しつつ、より迅速な電気通信事業者によるサイバー攻撃対策を実現するために、今後、既存の法的整理に関する現状及び課題や諸外国における法制度の状況を整理した上で、制度改正の必要性も含め検討を行うことが適当である。

（電気通信事業者におけるガバナンス確保）

電気通信事業ガバナンス検討会等における議論を踏まえ、第 208 回国会で成立した「電気通信事業法の一部を改正する法律」について、必要な下位法令の整備を行う。

イ．情報通信分野におけるサプライチェーンリスク対策

【現状】

（5G の脆弱性の検証手法等の確立と体制整備）

総務省において、2019 年度より 2021 年度にかけ、5G ネットワークにおけるセキュリティ確保に向けた調査検討を実施した。本件事業では、

- 様々な社会産業やミッションクリティカルな領域での 5G 活用の期待の高まりとともにモバイル通信サービスの安全性や信頼性への要求が一層高まっていること
- 5G を含むモバイル通信サービスのセキュリティは、個々の機器のセキュリティだけではなく、ネットワーク全体を踏まえた各オペレータの運用に依存する部分も大きいこと
- 5G SA やインターフェースのオープン化も見据えると、ネットワークはソフトウェア化が進むとともに、機器ベンダーも多様化しており、OSS プロジェクトでの進展も見られること

等を踏まえ、足下で入手可能な個々の機器の脆弱性の技術的検証ではなく、仮想化基盤や管理系などを含む 5G 全体を考えた技術的検証を実施し、オペ

レータが留意すべきセキュリティ課題を洗い出してその対策の普及を図るとともに、検証能力を含む 5G のセキュリティに関する国内への技術的蓄積を図ることとした。

具体的には、5G セキュリティに関する標準化機関や海外政府当局等の検討動向を調査するとともに、5G ネットワークのセキュリティに係る技術的検証を行うため、検証環境として、国立研究開発法人情報通信研究機構(NICT)において、5G ネットワークをエミュレート可能な仮想化基盤を構築し、同検証環境上での 5G ネットワークに対する脅威や脆弱性等の技術的検証を実施した。検証結果については対策要件等を整理し、2022 年４月、事業の成果文書として「5G セキュリティガイドライン第１版 [22]」を公表したところである。

(5G の脆弱性情報や脅威情報等の共有の枠組み)

一般社団法人 ICT-ISAC（ISAC は Information Sharing and Analysis Center の略）の 5G セキュリティ推進グループにおいて、ローカル 5G を提供する事業者やローカル 5G を利用する主体にとって参考となる、ローカル 5G のセキュリティガイドラインを 2022 年３月に策定・公表した。

(5G のセキュリティ対策の促進のための政策的措置)

総務省では、特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律 [23]（令和２年法律第 37 号）に基づき、サイバーセキュリティ上のサプライチェーンリスク対策や機器や設備の供給安定性等の観点を含む指針に沿って、5G システムの開発供給計画及びその導入計画を認定し、税制上の優遇措置を講じている。また、全国 5G の特定基地局の開設計画の認定時及びローカル 5G の免許時に、サプライチェーンリスク対応を含む十分なサイバーセキュリティ対策を講ずることを条件として付しており、産業振興的な枠組み、制度的な枠組みの両面から 5G のセキュリティ確保を推進している。さらに、5G オペレータがサービス提供を維持するために必要なベンダーをはじめとする 5G 技術サプライヤを含むサプライチェーン全体のセキュリティ確保については、既述の「5G セキュリティガイドライン第１版」において、オペレータによるサプライヤの選択プロセス、調達プロセス及びソリューションといったライフサイクル全体にわたってのデューデリジェンスとして取り組んでいく必要がある旨、考え方が示されたところである。

【今後の取組】

[22] https://www.soumu.go.jp/main_content/000812253.pdf

[23] https://elaws.e-gov.go.jp/document?lawid=502AC0000000037

（5G セキュリティガイドラインの普及等）

2022 年４月に公表した「5G セキュリティガイドライン第１版」について、国内の 5G オペレータへの普及を図り、5G ネットワークのセキュリティの確保を進めるべきである。その際、オペレータ等によるデューデリジェンスを促し、ベンダーをはじめとする 5G 技術サプライヤを含め、5G サービスのサプライチェーン全体のセキュリティ確保に取り組むことが適当である。また、ITU-T SG17 における標準化対象の一つとして、同ガイドラインをベースとした勧告化の提案を進めていくべきである。さらに、NICT に構築された 5G セキュリティ検証環境については、今後も NICT や我が国の産業界において活用がなされるよう、検討を進めていくことが重要である。これらの推進に当たっては、国際的にも進展の見られる基地局設備のインターフェースのオープン化や基地局設備自体の仮想化（いわゆる OpenRAN や vRAN）、コアや MEC を含めたクラウド（IaaS）利用も念頭に置くことが適当である。

（5G のセキュリティの促進のための政策的措置）

引き続き 5G の制度面において、サイバーセキュリティ上のサプライチェーンリスク対策等の安全性・信頼性等が確保された 5G の導入促進を行うことが必要である。

（情報通信分野における SBOM 導入の可能性の検討等）

Apache Log4j など広く利用されているソフトウェアの構成部品の脆弱性への対処が重要となる中、ソフトウェア製品の構成部品を管理して脆弱性に迅速に対応することを可能とする仕組みである SBOM（Software Bill of Materials）について、情報通信分野における導入の可能性を検討していくことが適当である。また、広く普及する通信用アプリケーション等に関する利用上の注意の在り方を検討していくことが適当である。

ウ. IoT におけるサイバーセキュリティの確保

【現状】

（NOTICE 注意喚起）

2018 年の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）[24]の改正により、NICT の業務に、パスワード設定等に不備のある IoT 機器の調査等を５年間（2024 年３月 31 日まで）の時限措置として追加した。これに基づき、2019 年２月より、NICT が IoT 機器を調査し、電気通信事業者（ISP、インターネットサービスプロバイダ）を通じて利用者への注意喚起を行うプロジェクト「NOTICE」を実施しており、2021 年度までに、約 36000 件の注意

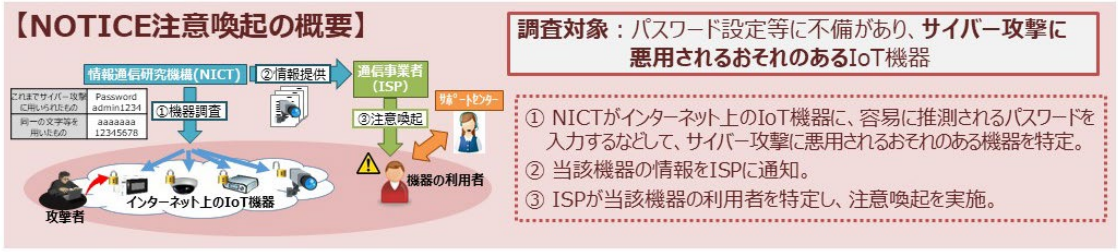
[24] https://elaws.e-gov.go.jp/document?lawid=411AC0000000162

喚起対象を ISP に通知した[25]。

NOTICE における注意喚起は、telnet 及び SSH によるアクセスに限られていたが、http/https によるアクセスに対するパスワード設定等に不備のある IoT 機器の調査に必要となる、ID・パスワードの自動入力を行うためのプログラムの開発をはじめとした準備が整ったことから、2022 年３月から、http/https についても注意喚起に向けた予備調査を開始した。さらに、パスワードの設定不備以外に関する対処としては、リフレクション攻撃に悪用されるおそれのある IoT 機器への対処のための予備調査を開始した。

（NICTER 注意喚起）

2019 年６月より、既にマルウェアに感染している IoT 機器を NICT の「NICTER」プロジェクトで得られた情報を基に特定し、ISP を通じて利用者へ注意喚起を行う取組を実施しており、2019 年６月からの期間全体において１日平均約 200 件の注意喚起対象を ISP に通知した。



（端末設備等規則の改正等）

電気通信事業法（昭和 59 年法律第 86 号）[26]の枠組みの中で、IoT 機器を含む端末設備のセキュリティを確保するため、端末設備等規則（昭和 60 年郵政省令第 31 号）[27]の一部改正を実施し、2020 年４月に施行している。あわせて、民間の任意の認証制度として、一般社団法人重要生活機器連携セキュリティ協議会（CCDS）において、IoT 機器のセキュリティ要件を定め、認

[25] これらの取組状況については、次の URL にて公表している。
https://notice.go.jp/status

[26] https://elaws.e-gov.go.jp/document?lawid=359AC0000000086

[27] https://elaws.e-gov.go.jp/document?lawid=360M50001000031

証するプログラムを実施している。

【今後の取組】

NOTICE や NICTER 注意喚起等の既存の取組を継続するとともに、NOTICE については、2022 年度から http/https に関する注意喚起を開始し、またリフレクション攻撃に悪用されるおそれのある IoT 機器への対処について、今後、検知された機器数等の予備調査の結果を踏まえた上で ISP と調整し、早急に開始する。依然として IoT 機器を狙ったサイバー攻撃が多い現状に鑑みると、NOTICE や NICTER 注意喚起について、注意喚起対象の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・高度化の検討を行うのに並行して、NOTICE が２年後に実施期限を迎えることも踏まえつつ、IoT 機器などの脆弱性調査・注意喚起等の更なる対応について、制度や国による予算支援の必要性の検討が必要である。

各 ISP から利用者への注意喚起に関しては、電子メールだけでなく郵送・架電・往訪等による効果的な注意喚起を継続することが求められる。IoT 機器の利用者（回線契約者）に対する注意喚起に加えて、IoT 機器を設置・運用する事業者（SIer 等）やマンションインターネット事業者等に対しても、積極的な注意喚起を行うことが必要である。

また、各 ISP からの注意喚起だけではなく、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活用した注意喚起を通じて、IoT 機器のセキュアな設定（パスワード設定、ファームウェア更新等）についてのきめ細かな注意喚起を進めることや、ソフトウェア脆弱性等を有する IoT 機器（例：VPN 機器、サポート期限切れ機器等）を特定し、直接的な注意喚起を行う手法について検討を進めることが適当である。

これらの検討に当たっては、IoT 機器の設計・製造・販売段階で、製造事業者における IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させ、新たに接続される脆弱な IoT 機器を増やさない取組や、IoT 機器利用者が、利用する機器の脆弱性を自主的に確認できるようにサポートする方法を検討するなど、利用者目線に立った取組を検討することが今後重要である。

また、法令に基づく技術基準に加え、民間団体がセキュリティ要件のガイドラインを策定し、当該要件に適合した IoT 機器に対して適合していることを示すマークを付す認証（Certification）の仕組みを構築している。このような任意の認証がより広範に普及するなど民間においても自主的な取組が進むことが期待される。

エ. クラウドサービスにおけるサイバーセキュリティの確保

【現状】

（提供事業者向けガイドラインの改定等）

クラウドサービスにおけるサイバーセキュリティの確保に関しては、2014年に策定したクラウドサービス提供事業者向けの「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」[28]について、SaaS や IaaS の特性を踏まえた全体の構成見直しや責任共有モデルの考え方、管理策の見直しなどを行い、2021 年９月に第３版として改定した。

また、クラウドサービスの設定ミスに起因する情報漏えいや障害といった事故が多発している[29]ことから、2021 年度、有識者及び事業者を交えて、過去の情報漏えい等の事故の原因や、クラウドサービス利用者及び提供者において実施されている設定ミスを防止するための取組について調査・分析を行った上で、クラウドサービス利用者及び提供者において実施することが望ましい取組の検討を行った。

（ISMAP の運用）

政府機関が利用するクラウドサービスの安全性評価の仕組みとして、内閣官房（NISC・IT 室（現在のデジタル庁））、総務省及び経済産業省において、2020 年６月に「政府情報システムのためのセキュリティ評価制度」（ISMAP）を立ち上げた。2021 年３月に 10 サービスが初めて登録されて以降、2022 年６月１日現在、あわせて 34 サービスが登録されている[30]。

【今後の取組】

引き続き、「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」の普及促進を図るとともに、クラウドサービスの設定ミスを防止するための取組の検討については、「クラウドサービス利用・提供における適切な設定のためのガイドライン（仮称）」として、広く意見募集を行った後、2022 年中に策定・公表した上で、今後、特に利用者に向けて、分かりやすく啓発していくことが重要である。

---

[28] https://www.soumu.go.jp/main_content/000771515.pdf

[29] 国内では、2021 年２月に、地方公共団体が利用する SaaS サービスにおいて、権限設定の誤りによって情報が第三者からアクセス可能な状態であった事例が発生した。なお、IBM の調査（2020 年）では、2019 年に発生した情報漏えい事案のうち 85%以上はクラウドサービスの設定ミス等によるものであったとされている。
https://newsroom.ibm.com/2020-02-11-IBM-X-Force-Stolen-Credentials-and-Vulnerabilities-Weaponized-Against-Businesses-in-2019

[30] 最新のクラウドサービスリストは ISMAP ポータルサイトを参照。
https://www.ismap.go.jp/

また、ISMAP については、セキュリティ上のリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みとして、影響度が低いと評価される業務・情報に用いられるSaaSを対象とするISMAP for Low-Impact Use（ISMAP-LIU、仮称）を2022年中に策定するなど、政府機関における安全なクラウドサービスの利用促進に向けて、制度の充実化及び見直しに継続して取り組む必要がある。

オ. スマートシティにおけるサイバーセキュリティの確保

【現状】

我が国では、関係省庁の連携の下、Society5.0の先行的実現の場として、補助事業等を通じてスマートシティを推進している。2020年には、内閣府の戦略イノベーション創造プログラム（SIP）において定義されたスマートシティリファレンスアーキテクチャに基づいて、総務省がスマートシティのセキュリティ対策の指針として策定した「スマートシティセキュリティガイドライン」について、多様な主体の関与、多様なデータの連携などのスマートシティの特徴を踏まえ、2021年６月に第2.0版として改定した[31]。政府のスマートシティ関連事業においては、2022年度から全ての事業において、同ガイドラインに基づいて作成した「スマートシティセキュリティ導入チェックシート」を応募書類の一部として位置付け[32]、セキュリティ対策について意識させるきっかけを作ることで、各地域における積極的なセキュリティ対策を促進している。また、各国における類似の取組との整合を図るため、海外の政府機関との意見交換の取組を行っている。

加えて、スマートシティ官民連携プラットフォーム（事務局：国土交通省）のスマートシティのセキュリティ・セーフティ分科会の活動において、セキュリティ対策の先進事例について官民で情報共有を行った。

【今後の取組】

「スマートシティセキュリティガイドライン（第2.0版）」について、引き続き、国内における普及促進及び国際的な制度調和に向けた海外の政府機関との意見交換の取組を行う。また、スマートシティの先進自治体や都市OSベンダー等の関係者との意見交換を通じて、国内外のスマートシティセキュリティに関するベストプラクティスなども参考としながら、随時必要な見直しを行っていくことが適当である。

[31] https://www.soumu.go.jp/main_content/000757799.pdf
[32] https://www8.cao.go.jp/cstp/stmain/r4_smartcity.html

カ. ICT-ISAC を通じた情報共有

【現状】

サイバーセキュリティ上の脅威が複雑化・巧妙化し、ICT 環境が高度化・複雑化している中、ISP を含む通信事業者のみならずソフトウェアベンダーや情報関連機器製造事業者などの幅広い分野から構成される ICT-ISAC を通じた分野横断的な情報共有が重要である。また、情報共有に際しては、その処理や分析の自動化により、セキュリティの現場をサポートし、迅速かつ的確な対策に繋げていくことが効果的である。総務省では、2019 年度から 2021 年度にかけ、これに関連した実証事業を実施している。その結果、刻々と公表される脆弱性情報について、様々な情報ソースと機械学習を用いることによって、その深刻度を自動的に判断する技術の有効性や、情報共有基盤との連携可能性について実証がなされた。また、ICT-ISAC が運営する情報共有基盤において、脅威情報に加え、脆弱性情報も共有・配布することにより、脅威への対策と脆弱性への対策の両方を高度に自動化できるコンセプトの有効性と技術的なフィージビリティがあることが確認されている。

【今後の取組】

2021 年度まで実施した上記の総務省実証事業の成果を含め、高度化された情報共有基盤の有効活用により、より迅速なサイバーセキュリティ対策が取られるよう、関係者による取組や利用の普及を促進することが必要である。

ICT-ISAC における情報共有基盤を用いた脅威情報の共有については、引き続き、活性化を促していく必要がある。また、脆弱性の深刻度の自動的な評価技術については、システムの有効活用も含め、ICT-ISAC を中心とした利用普及を促進していくべきである。

さらに、同一の情報共有基盤で脅威情報と脆弱性情報を取り扱うことによりサイバーセキュリティ対策の高度な自動化を行うコンセプトについては、その社会実装に向け、今後、実際に提供されている脆弱性情報データベースやソフトウェア資産管理ツール側との連携が求められる。総務省としても、SBOM の今後の普及動向も踏まえつつ、本件実証事業の関係者と脆弱性情報データベースやソフトウェア資産管理ツールの関係者との連携状況を引き続きフォローしていくべきである。

キ. 放送設備におけるサイバーセキュリティ対策

【現状】

2019 年２月の情報通信審議会答申を踏まえ、放送設備に関するサイバーセキュリティ対策の確保を技術基準に位置づけるとともに、放送設備に関する定期状況報告の際、サイバー事案に起因する事故報告を明記して報告を求

めることを内容として、放送法施行規則[33]（昭和 25 年電波監理委員会規則第 10 号）等を改正し、2020 年３月に施行した。なお、これまでに国内でサイバー攻撃に起因する放送停止事故は報告されていない。

【今後の取組】

今後とも、放送法施行規則等の制度を着実に運用していくとともに、放送設備の IP 化・クラウド化等の技術動向も踏まえ、放送における可用性確保の重要性を考慮した上で更なるサイバーセキュリティ対策の必要性を検討することが必要である。

ク. Beyond 5G・6G に向けたサイバーセキュリティの検討

【現状】

Beyond 5G・6G[34]に向けては、国際標準化機関等を舞台に、将来のサイバー空間のガバナンスやルール形成に大きな影響を与え得る情報通信アーキテクチャを左右しうる議論が行われているところ、その一部においては、我が国が掲げる「自由、公正かつ安全なサイバー空間」の在り方と必ずしも整合的ではないと考えられる提案も行われている。

【今後の取組】

5G に関しては、イに挙げた既存施策を着実に実施する。その上で、来る Beyond 5G・6G において開発・採用される技術について、多様な通信サービスを安全かつ安定的に信頼して利用できるよう、セキュリティ・バイ・デザインの考え方が反映されることが重要である。サイバー空間に関する将来動向を把握し、新たな研究開発要素も含め、国として推進すべきセキュリティ面での取組を検討することが適当である。この点、特に、情報通信アーキテクチャに関する国際的な議論の動向の主体的把握に努めるとともに、将来のサイバー空間のガバナンスやルールに、我が国が掲げる価値観が反映されるよう積極的に関与していくことが適当である。こうした観点から、インターネット・コミュニティとの連携等を進め、主要な国際標準化団体等における関連する議論の動向を把握するとともに、そうした議論への我が国からの参加や国内における議論の活性化を促進していくべきである。なお、我が国が掲げる「自由、公正かつ安全なサイバー空間」の在り方と必ずしも整合的ではないと考えられる国際標準の提案は、既存のインターネットの TCP/IP 等

[33] https://elaws.e-gov.go.jp/document?lawid=325M50080000010

[34] 5G の特長の更なる高度化に加えて、あらゆる機器が自律的に連携し、最適なネットワークを構築する自律性、地球上のどこでも通信を可能とする拡張性、セキュリティ・プライバシーが常に確保される超安全・信頼性、データ処理量の激増に対応できる超低消費電力、といった機能を実装した次世代の移動通信システム。

のアーキテクチャに内在する脆弱性の存在を強調し、それを解決するための案として主張される場合もある。その一方、アの実証事業でも念頭に置くRPKI や DNSSEC、DMARC のように、既存のインターネットのアーキテクチャを前提に、そこに内在する脆弱性を緩和するための技術の標準化も進んでいる。国際場裡における議論に効果的に対応していくためには、これら技術のメカニズムや効果、国内外の普及状況等を踏まえた関与が求められる。

（２）トラストサービスの普及

サイバー空間と実空間が高度に融合した Society5.0 の実現のためには、「誰が」、「何を」、「いつ」という実空間の構成要素を正しくサイバー空間でも再現することが必要であり、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の感染拡大に伴い、あらゆるやりとりをデジタル完結する要請が高まる中、データを安心・安全に流通できる基盤の構築が不可欠であり、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ところである。

【現状】

トラストサービスについては、2020 年２月に公表された「プラットフォームサービスに関する研究会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[35]」において示された方針に基づき、タイムスタンプ・e シール・電子署名のそれぞれについて検討を行ってきた。

タイムスタンプについては、上記取りまとめにおいて、国による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示されたことから、国が信頼の置けるサービス・事業者を認定する仕組みを設けることが適当とされた。これを受け、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）[36]」を公布し、国によるタイムスタンプの認定制度を整備した。さらに令和４年度税制改正により、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、国による認定制度に係るタイムスタンプが位置づけられた。e シールについては、2021 年６月に「e シールに係る指針[37]」

---

[35] プラットフォームサービスに関する研究会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
https://www.soumu.go.jp/main_content/000668595.pdf

[36] 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）
https://www.soumu.go.jp/main_content/000742664.pdf

[37] e シールに係る指針

を公表し、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[38]。電子署名については、2020 年７月に「電子署名法２条１項に関する Q&A[39]」を、同年９月には「電子署名法３条に関する Q&A[40]」を公表する等、電子署名の定義の明確化を図った。

また、デジタル庁「データ戦略推進ワーキンググループ」の下に設置された「トラストを確保した DX 推進サブワーキンググループ」において、包括的データ戦略（2021 年６月 18 日閣議決定）[41]を踏まえてサイバー空間における取引・手続に必要なトラストの信頼度（アシュアランスレベル）を整理するとともに、政府・地方自治体における手続や民間サービスへの適用の方策について検討した。

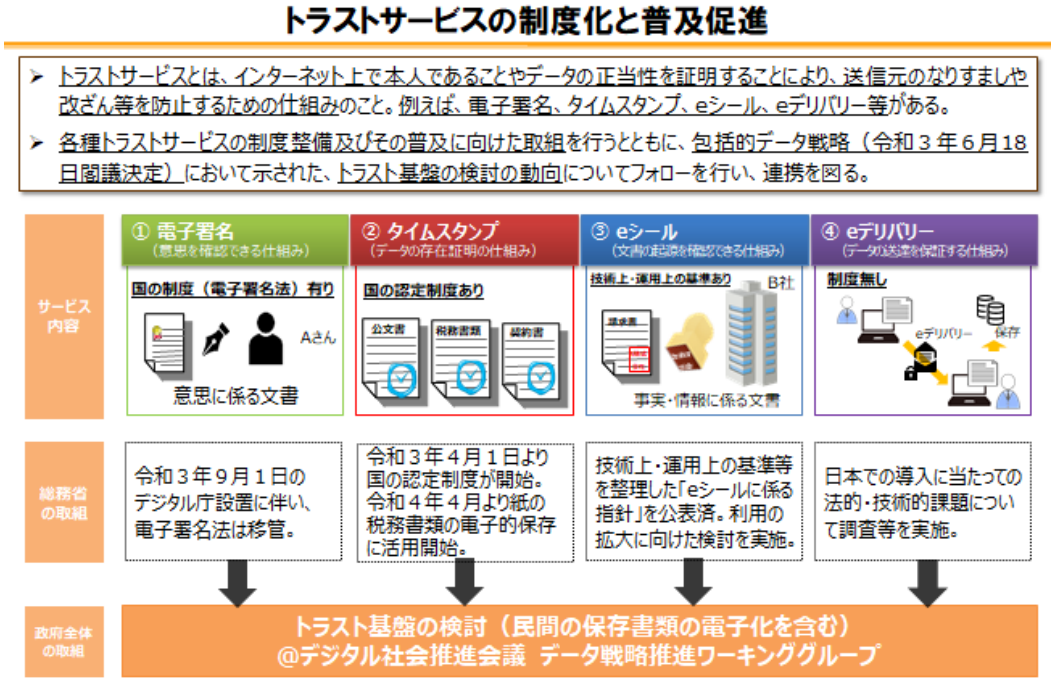
https://www.soumu.go.jp/main_content/000756907.pdf

[38] タイムスタンプについては、2004 年 11 月に「タイムビジネスに係る指針～ネットワークの安心な利用と電子データの安全な長期保存のために～」を公表したことで、2005 年２月に一般財団法人日本データ通信協会が「タイムビジネス信頼・安心認定制度」を開始し、タイムスタンプに関する民間の認定制度が創設された。

[39] 電子署名法２条１項に関する Q&A
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/517ca59b-6ea4-4179-a338-8d1b51a4d40b/20210901_digitalsign_qa_01.pdf

[40] 電子署名法３条に関する Q&A
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/517ca59b-6ea4-4179-a338-8d1b51a4d40b/20210901_digitalsign_qa_02.pdf

[41] 包括的データ戦略（2021 年６月 18 日閣議決定）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/02063701/policies_data_strategy_outline_02.pdf



【今後の取組】

引き続き、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、とりわけトラストを確保する枠組みの実現に向けた検討の動向を踏まえながら、各種トラストサービスの普及に向けた取組を行う。具体的には、改ざんの有無等を簡便に確認することができ、業務効率化や生産性の向上、ひいては DX の推進に寄与することが期待されるトラストサービスの普及に向け、民間における取組を支援するほか、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）等データ流通の信頼性の確保に向けた検討を行うことが適当である。

２．サイバー攻撃への自律的な対処能力の向上

（１）CYNEX（サイバーセキュリティ統合知的・人材育成基盤）等の推進

サイバーセキュリティは国家の基幹を守るもので、国際競争力の強化のほか、経済安全保障の観点からもサイバーセキュリティ産業の強化・育成は必須である。他方、我が国のサイバーセキュリティ製品・サービスは、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[42]。そのため、製品・サービスの開発に必要なノウハウや知見の蓄積が困難となっている。また、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、人材育成を全て国で実施することは困難である[43]ため、民間事業者や教育機関等における自立的な人材育成が求められる。しかしながら、演習用の環境構築やシナリオ開発には高度な知識や技術力、そして基盤となる計算機環境が必要であり民間企業・教育機関のみでは十分に対応できていない。これらについては、「サイバーセキュリティ戦略」においても、「こうした状況を打破する取組の一環として、サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築」、「社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し（中略）産学に開放する」と記載がなされている。これらの状況を踏まえ、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、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。

【現状】

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 においては、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等を実施しており、NICT が有するこれらの技術・ノウハウ[44]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（サイバーセキュリティ統合知的・人材

---

[42] 令和４年版情報通信白書第３章第７節「２我が国におけるサイバーセキュリティの現状」によれば、2020 年の国内企業シェアは 12%となっている。
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/n3700000.pdf

[43] NRI セキュアテクノロジーズの調査によれば、セキュリティ人材について、どちらかといえば不足している、あるいは不足していると回答した割合が米国 12.9%、英国 11.6%であるのに対して、我が国では 90.4%となっている。https://www.nri.com/-/media/Corporate/jp/Files/PDF/news/newsrelease/cc/2022/220208_1.pdf

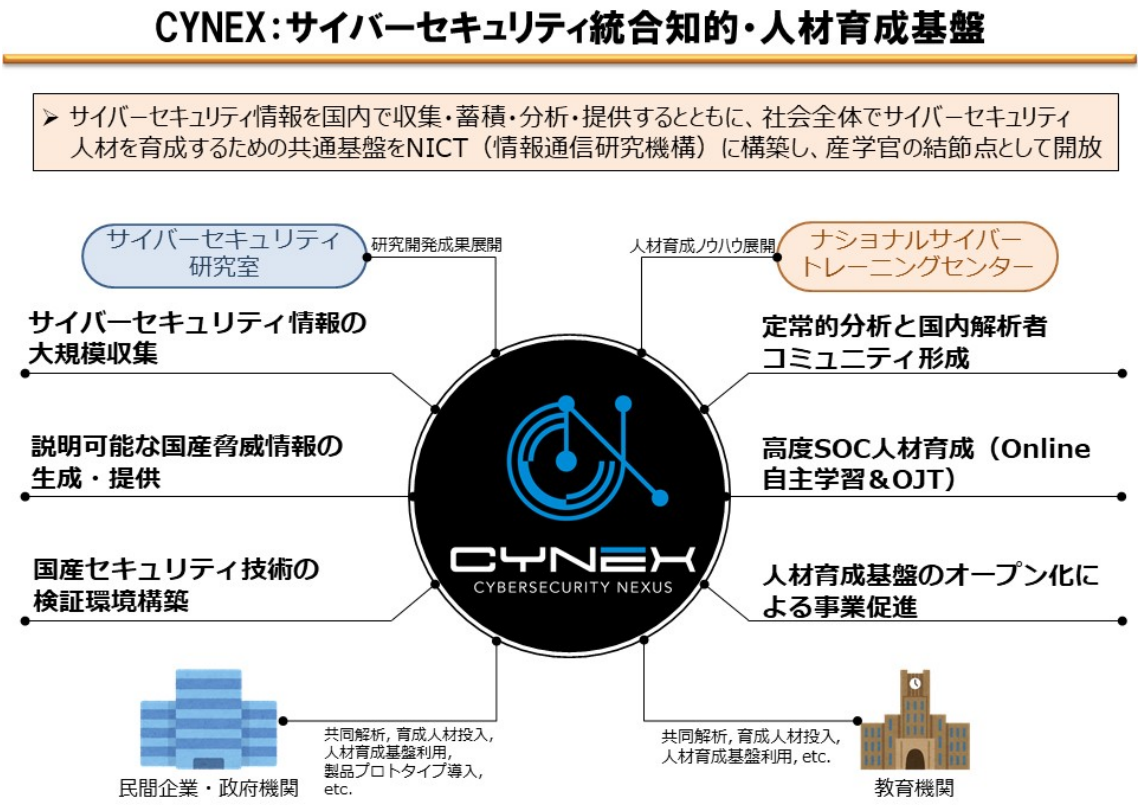
[44] 世界的にも有数の規模を誇るサイバー攻撃観測網（NICTER）や、模擬的な企業ネットワーク上でマルウェア解析が可能なシステム（STARDUST）を保有し、また、研究開発だけでなく、実践的サイバー防御演習（CYDER）により NICT による人材育成を実施している。

育成基盤）となる CYNEX を令和２年度３次補正予算及び３年度予算で構築し、2022 年から試験運用を開始し、CYNEX の更なる高度化に取り組んでいる。また、サイバーセキュリティに係る製品開発や人材育成等を進める大学、企業等の組織に事業連携の声掛けを行い、37 組織が参画することとなった。

【今後の取組】

（情報収集・分析）

CYNEX では、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等にも留意しつつ、2023 年度の本格運用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必要がある。また、その計画・進捗については、本タスクフォースに適宜報告をし、方向性について最新のセキュリティ動向等を踏まえた議論を深めていく必要がある。



また、NICT は、CYNEX が産学官の組織にとって利用したいと思える環境となるよう関係者との密な意見交換を行い必要な改善を施すとともに、利用する全ての組織にとっての拠り所となるコミュニティの形成を積極的に図ることが求められるほか、産学官の参画組織がサイバー攻撃の収集・分析等に関してより深い関係性と信頼性が築ける運営が期待される。

なお、CYNEX 等では、利用者が自身で構築しているネットワーク内の機器

にはアプローチできておらず、未知のマルウェア等を様々なネットワーク利用者の実利用環境から察知・収集することは、迅速な対処の分析につながる重要かつ有効な手段である。このことから国内のマルウェア感染状況を利用者等からもリアルタイムかつ横断的な集約を可能とし、その分析結果を当該利用者等に対して迅速に通知するとともに、分析結果は国内のベンダー等がIoT機器やセキュリティ製品の開発に活かせる国内循環型のセキュリティ情報フレームワークについて検討する必要がある。

（人材育成）

社会全体でのサイバーセキュリティ人材の育成を推進するため、サイバーセキュリティの人材育成に関し、演習の実施に関する様々な要素（データセット、演習用ミドルウェア、計算機リソースなど）を総合的にカバーする、オープン型の新たな人材育成プラットフォームや、産学官の連携によってプラットフォーム上で利用可能な演習用教材等の共用コンテンツの拡充も図りつつ、当該プラットフォームを積極的に活用するためのコミュニティの支援も行いながら、2023 年度の本格運用に向けて取組を進めていく必要がある。

（２）研究開発の推進

巧妙化・複雑化したサイバー攻撃の増大、サプライチェーンの複雑化・グローバル化に伴うリスクの増大による様々な脆弱性を対象とする攻撃等について、適切に検知・対処するため、新たな脅威の発生可能性など、安全保障の観点を含め我が国をとりまく現下の課題認識に基づき、我が国において、サイバーセキュリティに係る実践的な研究開発の推進が求められる。また、研究開発の推進に当たっては Beyond 5G をはじめとするネットワーク技術の高度化などデジタル技術の進展に応じた観点や、人の誤認識につけ込むサイバー攻撃手法の高度化を踏まえ、人の認識や行動特性に応じたユーザブルセキュリティの見地も重要であり、中長期的な技術トレンドを視野に入れた柔軟な対応が求められる。

【現状】

（NICT における研究開発）

NICT において、観測データの拡充を目指し、無差別型攻撃観測技術や標的型攻撃観測技術の高度化、機械学習等の AI 技術を用いたマルウェア感染活動の早期検知技術やセキュリティアラートの自動グルーピング等によるトリアージ技術等に関する研究開発を実施した。また、パーソナルデータなど機密性の高いデータを複数組織間で互いに開示することなく安全に解析することができるプライバシー保護連合学習技術について、金融機関を対象に

社会実装を進め、その効果を検証するとともに継続学習を進めている。さらに差分プライバシーなどを用いたセキュリティ強化手法の研究開発を実施している。加えて、あらゆる計算機で解読不可能な安全性を実現する量子暗号を活用した量子セキュアネットワーク技術等の研究開発を実施している。

これらの研究開発の成果については、例えば、標的型攻撃観測技術の高度化では、並行ネットワーク構築機能の強化を進めたサイバー攻撃誘引基盤（STARDUST）の外部利用を推進し、10 以上の機関に利活用されるなど社会実装および成果展開を推進した。

（大学や民間企業における研究開発の支援等）

このほか、2022 年度に、大学や民間企業において、国の研究開発プロジェクトとして、以下の研究開発を実施している。

- 2020～2022 年度「電波の有効利用のための IoT マルウェアの無害化/無機能化技術等に関する研究開発」
- 2020～2024 年度「グローバル量子暗号通信網構築のための研究開発」
- 2018～2022 年度「衛星通信における量子暗号技術の研究開発」
- 2021～2025 年度「グローバル量子暗号通信網構築のための衛星量子暗号通信の研究開発」
- 2021～2024 年度「安全な無線通信サービスのための新世代暗号技術に関する研究開発」

また、総務省等においては、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト CRYPTREC[45] を実施しており、この中で NICT は暗号技術の安全性評価において重要な役割を果たしている。

【今後の取組】

（NICT における研究開発）

NICT においては、第５期中長期目標・計画にしたがって、研究開発を着実に推進し、ICT を取り巻く諸課題やサイバー攻撃の状況を常に踏まえながら、情報通信関連では国内唯一の国立研究開発法人として産学との連携のもと研究開発を更に牽引することが求められる。

サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・

[45] Cryptography Research and Evaluation Committees の略。総務省及び経済産業省が共同で運営する「暗号技術検討会」と、NICT 及び IPA が共同で運営する「暗号技術評価委員会」及び「暗号技術活用委員会」で構成される。

分析・可視化・対策技術、大規模集約された多種多様なサイバー攻撃に関する情報の横断分析技術、新たなネットワーク環境等のセキュリティ向上のための検証技術の研究開発を実施していく必要がある。

また、社会の持続的発展において欠くことの出来ない情報のセキュリティやプライバシーの確保を確かなものとするため、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施し、その安全性評価を行うとともに、安全な情報利活用を推進し、国民生活を支える様々なシステムへの普及を図ることが求められる。加えて、量子暗号をはじめとする量子セキュアネットワーク技術や、ノード内の信号処理も量子的に行う完全な量子ネットワークの実現を目指した量子ノード技術の研究開発を推進する必要がある。

（大学や民間企業における研究開発の支援等）

IoT マルウェアの挙動検知及び駆除技術、マルウェアに感染した IoT 機器を無害化・無機能化する技術の開発を目的とした「電波の有効利用のための IoT マルウェアの無害化/無機能化技術等に関する研究開発」は取組を進めることが求められる。

また、安全な衛星通信ネットワークの構築を可能とし、盗聴や改ざんが極めて困難な量子暗号通信を超小型衛星に活用するための技術の確立に向け、「衛星通信における量子暗号技術の研究開発」や、量子コンピュータ時代において国家・重要機関間の機密情報を安全にやりとりするための、距離に依らない堅牢な量子暗号通信網の実現に資する、地上系の量子暗号通信の更なる長距離化技術の確立に向けた「グローバル量子暗号通信網構築のための研究開発」について、継続的に取り組む必要がある。

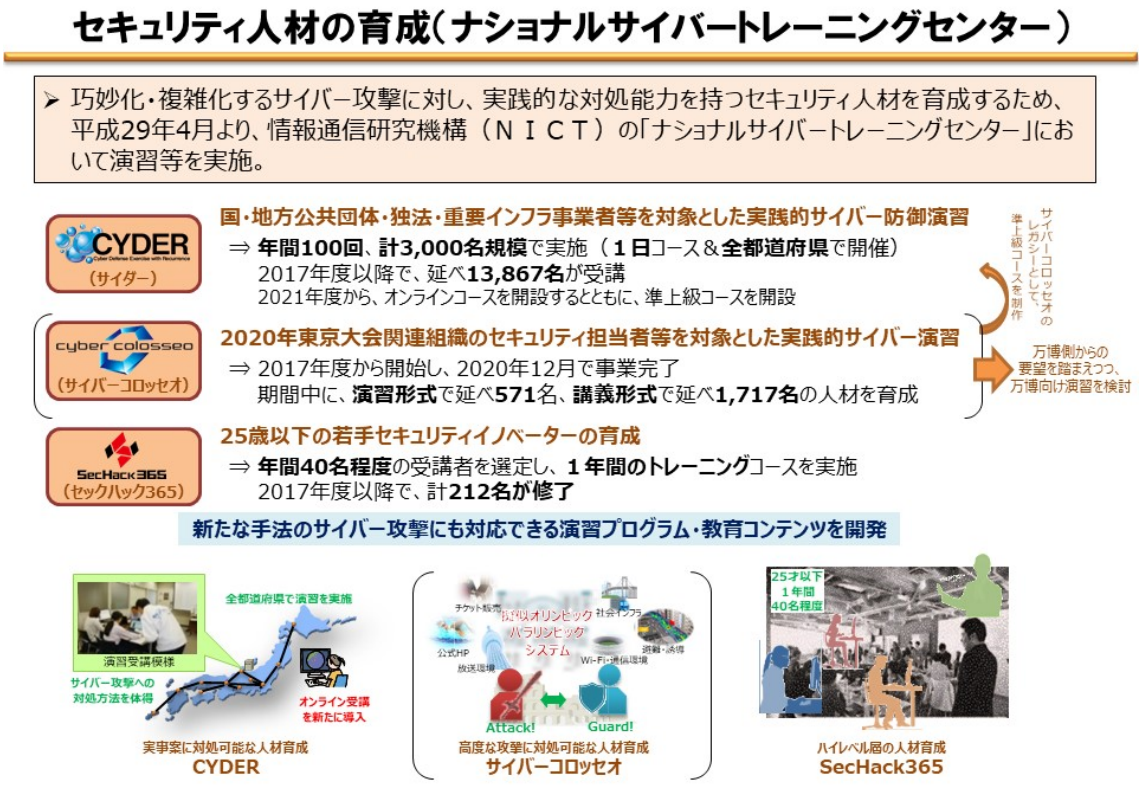
加えて、数百～数千 km といった大陸間スケールでの量子暗号通信網を構築できる機能を検証する衛星系と地上系を統合した量子暗号通信網実現のための技術の確立に向けた「グローバル量子暗号通信網構築のための衛星量子暗号通信の研究開発」も継続が求められるほか、暗号技術に関する研究開発として、「安全な無線通信サービスのための新世代暗号技術に関する研究開発」において、5G 等のための超高速・大容量に対応した共通鍵暗号方式技術や耐量子計算機暗号の機能付加技術等の研究開発に取り組むことが重要である。

これらについて、国及び国民の安全・安心の確保、産業競争力の強化等の観点から、重要な情報を安全に保管する手段として、機密性・完全性等を有し、かつ市場化を見据えて国際競争力の高い、量子通信・暗号に関する研究

開発を引き続き実施する必要がある。さらに、研究開発成果の社会への還元という観点で、総務省及び NICT において、量子コンピュータが現代暗号に及ぼす影響の把握に努めるとともに、2022 年度末を目途とする電子政府推奨暗号リスト（CRYPTREC 暗号リスト）の 10 年に一度の全面改定に向けた検討を継続することが必要である。また、耐量子計算機暗号（PQC）の標準化や実装状況のフォローを行いつつ、耐量子計算機暗号に関するガイドラインを策定し、暗号技術利用者に対する理解増進に努めるとともに、今後利用が拡大すると想定される IoT 機器等に用いられる「軽量暗号」や、暗号状態で情報処理が可能な「高機能暗号」についてもガイドラインを作成することが重要である。

（３）人材育成の推進

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。同様の認識を踏まえ、「サイバーセキュリティ戦略」においても、「「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要」とされている。このため総務省では、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。また、地域のコミュニティや企業、教育機関等と連携して、セキュリティ人材を自立的に育成していくためのエコシステムの確立に向けた実証を行っている。こうした取組を引き続き実施し、深化させることが求められる。



ア．実践的サイバー防御演習（CYDER）の実施

【現状】

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、2017 年度から、行政機関等の実際のネットワーク環境を模した大規模仮想 LAN 環境を構築の上、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）を実施（全都道府県で年間 100 回、計 3000 名規模）し、2021 年度は、演習を 105 回実施し、計 2454 名が受講した（2017 年度からの合計で 13867 名が受講）。また、2021 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、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を追加するとともに、地理的・時間的要因等により CYDER が受講できない者への最低限の対応としてオンライン演習のコースを追加した。

【今後の取組】

サイバー攻撃は年々増加していることから、社会全体としてサイバーセキュリティ対応力を強化することは急務であり、実際のインシデント発生時に対応を行う情報システム担当者等に対する人材育成の取組は特に重要である。防災訓練と同様に定期的に演習を経験することで実対応時の能力向上を

図るよう、CYDERによる人材育成を引き続き実施する必要がある。

特に、地方公共団体には未受講の団体もあることから、そのような団体が我が国におけるサイバーセキュリティ対策上の穴とならないよう、受講の促進を図っていく必要がある。また、地理的・時間的要因等によりCYDERが受講できない者への対応として、出前講習、サテライト講習の試行及びオンライン演習について今後も積極的に進めていく必要がある。なお、オンライン演習の実施に当たっては、集合演習に比べて十分な演習効果が発揮されるように引き続き受講効果向上のための改善を行っていくことが必要である。

イ. 大規模イベント向け実践的サイバー演習の実施

【現状】

高度化・多様化するサイバー攻撃に備え、2020年東京大会の適切な運営を確保することを目的として、大会関連組織のセキュリティ担当者等を対象とした、高度な攻撃に対処可能な人材の育成を行う実践的サイバー演習「サイバーコロッセオ」は、2017年度から、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実施し、2020年度で目標とする人材育成を完了した（実機演習を伴った演習（コロッセオ演習）で延べ571名、講義演習形式による演習（コロッセオカレッジ）で延べ1717名の人材を育成）。終了後、本演習内容を2020年東京大会のレガシーとして継続的に活用するべく、CYDERのプログラムに準上級コースとして組み込んだ。

【今後の取組】

2020年東京大会時より更に高度化・多様化すると見込まれるサイバー攻撃に備えるべく、2025年日本国際博覧会側からの要望を踏まえつつ、2025年開催の大阪・関西万博の適切な運営を確保するために、「サイバーコロッセオ for 万博（仮）」として、高度な攻撃にも対処可能な人材の育成を、関連組織のセキュリティ担当者等を対象に実施できるよう検討することが適当である。

ウ. SecHack365の実施

【現状】

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、2017年度から、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「SecHack365」を実施している。2021年度は41名が修了し、2017年度からの合計で212名が修了した。

【今後の取組】

本取組の特徴は、NICT の持つサイバーセキュリティの研究資産を活用しながら、実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導する点にあり、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、本取組を進める必要がある。さらに、優秀な参加者には、国際的な場でのトレーニングに関しても検討する。

エ. 地域人材エコシステムの形成

【現状】

サイバーセキュリティ事業者が都市部に集中し、地域においては、サイバーセキュリティに関する雇用の受け皿が無いことから、若年層がサイバーセキュリティ関連業界を目指さず、地域におけるサイバーセキュリティ人材が更に不足するといった悪循環が生じている。他方で、都市部に集中するサイバーセキュリティ事業者が過度に集中する業務の一部をアウトソーシング（外部発注）する動きがある。そのため、沖縄県において、就業の場の確保と就業につながる研修を一体的に行い、地域における人材エコシステムの形成を図るモデル事業を実施した。本事業内において、エコシステムの自走に必要となる育成カリキュラム等を構築し、本カリキュラムを基に研修等を提供することで IoT セキュリティエンジニアおよび現地講師を育成したほか、他地域に展開する際の地域要件の整理を行った。

【今後の取組】

モデル事業対象地域（沖縄県）における人材エコシステムの確立・自走を図る。また、その成果を他地域にも容易に横展開できるよう、過年度に作成した研修コンテンツや研修プログラム（提供企業や使用するテキスト等）を整理の上、パッケージ化及び展開先の地域要件を踏まえた具体の対象地域について、検討を進めていく。

３．国際連携の推進

サイバー空間は国境を越えて利用される領域であることから、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、各国政府・民間レベルでの本分野における情報共有や国際標準化活動への積極的な関与を進めていく必要がある。

また、国際的なサイバーセキュリティ上の弱点を減らし、日本を含む世界全体のリスクを低減させる等の観点から、インド太平洋地域を含む開発途上国に対する能力構築支援を行い国際的な人材育成への貢献を図るほか、国内企業のサイバーセキュリティ分野における国際競争力の持続的な向上を図る取組も推進することが重要である。

ア．有志国との二国間連携の強化

【現状】

総務省が主催する ICT 分野の政策対話や外務省が主催するサイバー協議等において、米国をはじめとする G7 各国を中心に総務省のサイバーセキュリティ政策（IoT セキュリティ、5G セキュリティ）の積極的な発信や意見交換を実施したほか、各会合を通じて日 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）への教材提供を呼びかけた。その成果として米国、英国及びスイスより教材提供の申し出があり、各国からの教材提供を通じて、AJCCBC のコンテンツの充実化に繋がっている。

【今後の取組】

引き続き、情報の自由な流通の確保を基本とする考えの下、当該理念を共有する国を中心に、能力構築支援や国際標準化の分野における連携強化のための関係性構築に取り組むことが適当である。

イ．多国間会合を通じた有志国との連携の強化

【現状】

OECD（経済協力開発機構）では、主に WPSDE（デジタル経済セキュリティ作業部会）における政策議論に参加しているほか、日 ASEAN サイバーセキュリティ政策会議等、多国間の枠組みにおけるセキュリティ関係の議論に積極的に参画した。また、2021 年９月の第２回日米豪印首脳会合において日米豪印サイバー上級会合を設立することで合意した。

WPSDE では、新規勧告の作成において、日本の意見を発言・提出するとともに、副議長として会合の進行に寄与するなど、プレゼンスを発揮した。

日 ASEAN 政策会議においては、AJCCBC における新規コンテンツ等の紹介

を行い、各国から参加者を募集し、AJCCBC の活性化を図った。

また、日米豪印首脳会合共同声明（2022 年５月 24 日）[46]において、「日米豪印サイバーセキュリティ・パートナーシップ」[47] が公表され、同パートナーシップのもと、日米豪印各国及びインド太平洋地域におけるパートナーの能力構築を強化するためのそれぞれの取組の調整を加速させることとなった。

【今後の取組】

2023 年の G7 及び IGF（インターネットガバナンスフォーラム）の国内開催、Quad の枠組みを通じた日米豪印の連携や、日 ASEAN サイバーセキュリティ政策会議を通じた ASEAN との関係強化を踏まえ、引き続き、情報の自由な流通の確保を基本とする考えの下、当該理念を共有する国を中心に、連携強化のための関係性構築に取り組むことが適当である。

ウ. ISAC 間を通じた民間分野での国際連携の促進

【現状】

サイバー攻撃は国境を越えて行われるため、サイバーセキュリティ対策においては、脅威情報（攻撃情報）等の国際的な共有を行うことにより、国際レベルでの早期の攻撃挙動等の把握が必要不可欠である。そのため、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 において、国際的な ISAC 間等の連携を促進していく必要がある。

ICT 分野では、ICT-ISAC と 2019 年に協力覚書を締結した米国 IT-ISAC 及びその関係機関との連携について、引き続き定期会合の開催等を通じて強化している。また、米国以外の国・地域等との連携も促進しており、2021 年度には EU との ISAC 関連団体との意見交換会を開催した。また日米欧間で会合を行い、今後具体的な協力に向け調整を続けていくことになった。

また、ASEAN 各国を対象とした ISP 向け日 ASEAN 情報セキュリティワークショップを開催し、2020 年度より ASEAN 各国の ISP との情報共有体制も構築している。

【今後の取組】

ICT-ISAC と米国 IT-ISAC 間における効果的な情報共有の在り方について、日本側及び米国側関係者との議論を重ね、情報共有の自動化、共有する情報の種類、情報の活用方策等について引き続き検討を進めることが重要である。

---

[46] https://www.mofa.go.jp/mofaj/fp/nsp/page1_001188.html

[47] https://www.mofa.go.jp/mofaj/files/100347900.pdf

加えて、EU をはじめとする他の国・地域の ISAC 関連組織との連携を引き続き促進することが求められる。

また、ASEAN 各国の ISP との間では、民間レベルでのサイバーセキュリティに関する脅威情報の共有を促進するために構築した情報共有基盤を活用したワークショップを実施し、具体的な共有基盤の活用方策の検討を進めていくとともに、当該ワークショップの場を活用して、日本のサイバーセキュリティ製品・サービスの展開支援を行うことも肝要である。

エ. インド太平洋地域における開発途上国に対する能力構築支援

【現状】

ASEAN 各国との協力関係を強化するため、2018 年９月にタイのバンコクに設立した AJCCBC において、CYDER[48]等を通じて、ASEAN 各国のセキュリティ人材の育成支援を実施した（2022 年までに 700 名程度を目標。2022 年４月現在 787 名が参加）。また、オンライン環境で受講可能なプログラムの拡充、有志国（スイス）との第三者連携、国内企業により開発された SOC アナリスト演習・スレットハンティング演習の提供等を実施した。

[48] 「CYDER」の詳細は P33 参照。

【今後の取組】

アジア地域においては引き続き ASEAN 各国との協力関係の強化が必要である。具体的には、AJCCBC における CYDER 等の実施を通じ、ASEAN のセキュリティ人材の育成支援を引き続き進める必要がある。同時に、AJCCBC における研修内容の発展を図る観点から、オンライン・オンサイト環境で受講可能なプログラムを拡充しつつ、更なる有志国との第三者連携や国内企業との連携を強化することが重要である。

さらに、「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」[49]（2021 年 12 月サイバーセキュリティ戦略本部決定）の方針に則り、AJCCBC で行われる研修等への参加者のすそ野の拡大や、ASEAN 以外のインド太平洋地域における能力構築支援について検討を進める必要がある。

オ. 国際標準化機関における日本の取組の発信及び各国からの提案への対処

【現状】

2016 年 7 月に IoT 推進コンソーシアムにおいて策定された「IoT セキュリティガイドライン」[50]の国際標準への反映等に向けて、ITU-T SG17 及び ISO/IEC JTC1 SC27 における IoT セキュリティに係る国際標準化の議論に積極的に貢献している。なお、同ガイドラインは、ISO/IEC JTC1 SC27 では、2022 年 6 月に ISO/IEC 27400[51]として発行された。

2021 年 10 月には、ITU-T SG17 で議論されていた、日本発のサイバーセキュリティノウハウである CDC（サイバーディフェンスセンター）が、ITU 勧告 X.1060 として発行された。

また、「自由、公正かつ安全なサイバー空間」という基本的な理念に必ずしも整合的でない動きが見られる現状も踏まえつつ、必要な調査や連携強化の取組を実施している。

【今後の取組】

IoT セキュリティに係る国際標準化が ITU-T で議論されているところであり、関係府省庁と連携し、こうした活動に積極的に貢献していくことが重要である。また、5G セキュリティをはじめとしたⅡ１（１）の「情報通信ネットワークの安全性・信頼性の確保」に係る分野の具体的施策について、必要に応じて国際連携の場で共有するとともに、国際標準化等の可能性について

[49] https://www.nisc.go.jp/pdf/policy/kokusai/cs-tojyokokushien2021.pdf
[50] https://www.soumu.go.jp/main_content/000428393.pdf
[51] https://www.iso.org/standard/44373.html

継続的に検討することが重要である。

また、サイバーセキュリティ分野の国際標準化動向について、前述の「自由、公正かつ安全なサイバー空間」という基本的な理念に必ずしも整合的でない動きが見られる現状も踏まえつつ、我が国として注力すべき分野や具体的な課題等について調査を行うとともに、積極的な対処のために必要な連携強化に向けて継続的に取り組んでいく必要がある。

カ. 国内企業の ASEAN 地域等に向けた国際展開への支援

【現状】

ASEAN 地域を中心に、国内企業のサイバーセキュリティ製品・ソリューションの海外への展開を支援するための実証事業や調査等を実施している。

2021 年度には、ベトナムにおいてセキュアなファイルの授受による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・調査が実施された。

過去の実証事業では、現地法人を持つ大企業による受注実績がある一方、現地法人を持たない中小企業からは、海外展開を単独で行うことは困難との声も多い。

【今後の取組】

「ICT 国際競争力強化パッケージ支援事業」や「グローバル・デジタル連結性の実現に向けた日米連携事業」等の取組を通じ、我が国における ICT の知見やノウハウを含めた成功事例の海外展開や日本の製品・サービスの海外プロモーションを推進するほか、引き続き中小企業の海外展開を含めた効果的な支援の在り方の検討を行うことが重要である。加えて、情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携といったサイバーセキュリティ戦略上の基本原則の実現・浸透を図る必要がある。

このため、2022 年度においては、2021 年 10 月に発行された ITU 勧告 X.1060 の普及展開に関する取組を実施し、本勧告の普及を通して、我が国の取組と整合的なサイバーセキュリティ体制の整備を支援することにより、日本企業が海外に進出しやすい環境の構築を図ることが肝要である。

４．普及啓発の推進

我が国全体としてサイバー攻撃のリスクが高まるとともに、サイバー空間に参加する層が広がる中で、「サイバーセキュリティ戦略」がコンセプトとして掲げている”Cybersecurity for ALL”（誰も取り残さないサイバーセキュリティ）の観点からは、事業者であれば地域や業種、事業規模を問わず、個人であれば世代を問わず、サイバーセキュリティ対策の穴を作らないことが重要である。Ⅰに述べたように、政府としては、特に事業者や地方公共団体に対して、累次にわたりサイバーセキュリティ対策の強化を求める注意喚起を行っているが、引き続き、事業者向け、個人向けそれぞれについて、ターゲットの課題と特性に合わせた普及啓発を推進することが求められる。

（１）事業者向けの普及啓発

事業者向けの普及啓発としては、サイバーセキュリティに関する予算、人材、知見が不足する傾向がある「中小企業等」や、都市部と比べサイバーセキュリティに係る人材育成や情報共有の機会が少ないと考えられる「地域」を主なターゲットとして、テレワークにおけるサイバーセキュリティの確保の推進や、地域におけるセキュリティコミュニティの強化を進める必要がある。

また、サイバー攻撃被害を受けた組織における適切な情報の取扱いに資するため、サイバー攻撃被害に係る情報の共有・公表に関して、実務上の参考となるガイダンスの策定に向けた取組等を引き続き推進することが求められる。

ア．テレワークにおけるサイバーセキュリティの確保

【現状】

「テレワークセキュリティガイドライン[52]」（2004 年に初版を策定）について、テレワークを取り巻く環境やセキュリティ動向の変化に対応するため、2021 年５月に第５版として改定した。また、専任のセキュリティ担当が存在しないような中小企業等においても、最低限のセキュリティを確実に確保してもらうために策定した、「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）[52]」を 2022 年５月に第３版として改定した。

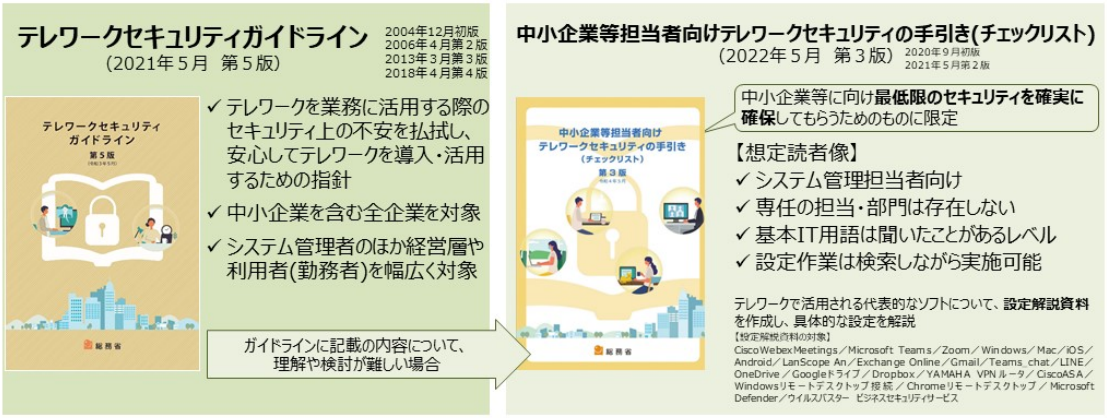
また、2021 年 12 月から 2022 年１月にかけて、今後のテレワーク支援に関する各種政策立案等に活用する目的でテレワークを導入する企業等におけるセキュリティ対策状況の実態を把握するための調査を Web アンケートにより実施し、その結果を公表した[52]。

[52] ガイドライン類及び実態調査の結果は、次の URL にて公表している。
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティガイドラインの改定

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示してきた。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年５月**に**全面的に改定**
- ガイドラインを補完するものとして、セキュリティの専任担当がいないような中小企業等においても、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保**してもらうための**チェックリスト**についても策定。

公表URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/



【今後の取組】

テレワークセキュリティガイドライン及び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）について、関係省庁や関連団体・企業等とも連携し、テレワーク実施企業やテレワーク勤務者に一層広く周知していく必要がある。

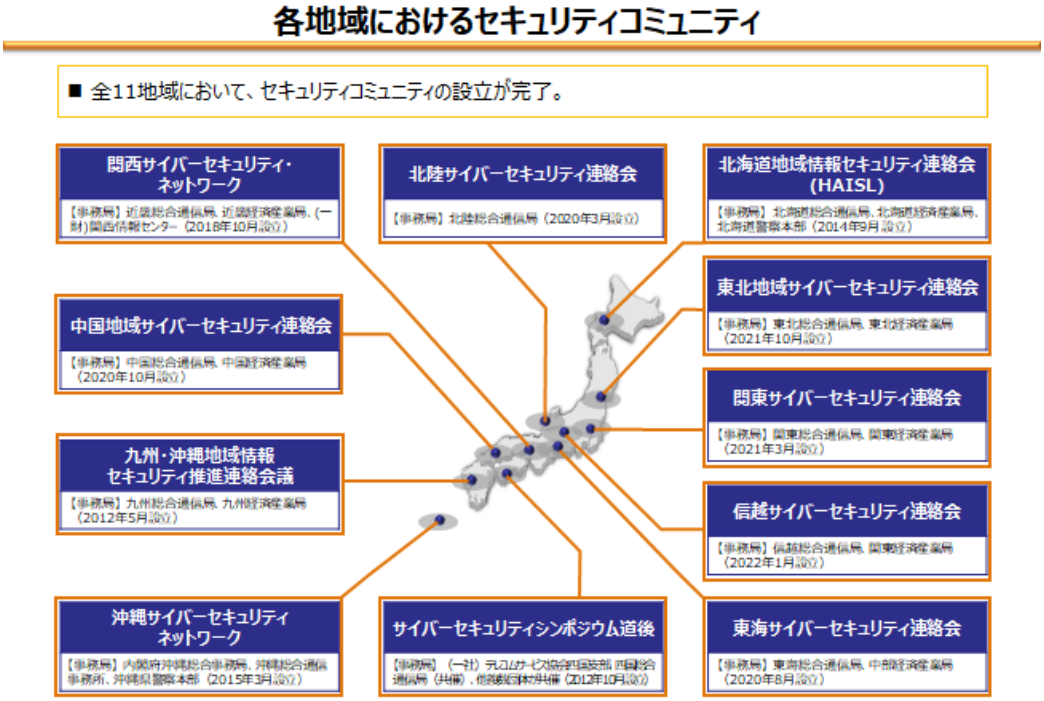
また、コロナ後の対応も見据え、民間企業等におけるテレワークセキュリティの実態を引き続き調査するとともに、当該調査結果やセキュリティ動向等を踏まえつつ、テレワークセキュリティガイドライン等の再改定の検討を引き続き実施することが重要である。

イ．地域セキュリティコミュニティの強化

【現状】

サイバーセキュリティのリスクが地域や企業・団体の規模を問わず高まっているが、地域においては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みが不足しているおそれがあり、地域レベルのコミュニティを設けることで、情報共有等を強化することが重要である。2021 年度末までに、全 11 総合通信局等の管轄地域で「地域 SECUNITY」（地域セキュリティコミュニティ）に当たる組織が設立されており、これらのコミュニティを通じ、セキュリティ意識啓発・対応能力向上の

ためのセミナーやサイバーインシデント対応演習などを実施することで、地域全体としてのサイバーセキュリティの向上を図っている（2021 年度は全 25 回（本省支援分）のイベントに、情報通信関連を中心とする幅広い業種の企業・団体の実務者層や戦略マネジメント層など約 1400 人が参加）。



【今後の取組】

引き続き、地域 SECUNITY の強化支援を通じてサイバーセキュリティを向上するため、関係機関と連携しつつ、各地域でのセミナーやサイバーインシデント対応演習などの開催を支援することが適当である。また、2021 年度に先行的に一部地域で開催した若年層のサイバーセキュリティ人材育成に向けた CTF（Capture The Flag）など、地域における先進的な取組について、他地域への横展開を図ることが適当である。また、セミナーや演習には情報通信関連以外を含む幅広い業種の企業・団体からの参加が、CTF には大学、高専生などの若年層の参加が期待される。

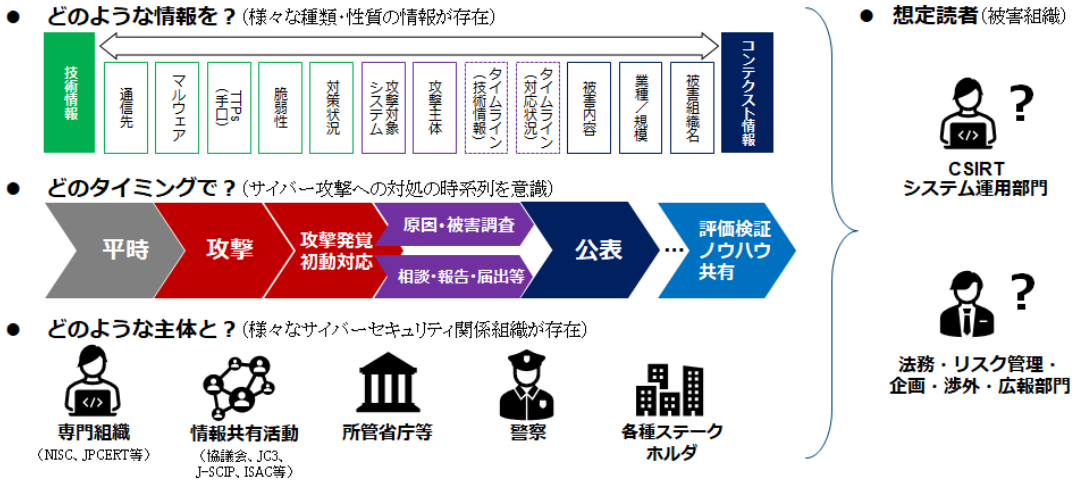
ウ. サイバー攻撃被害に係る情報の共有・公表の適切な推進

【現状】

大手民間企業やそのサプライチェーンを担う中小企業等を対象としたサイバー攻撃が多発している中、攻撃被害を受けた組織が、サイバー攻撃に関する情報を外部専門機関等に共有することは、攻撃者の手口の分析等により発生したサイバー攻撃の全容を解明し、対策強化や第三者における新たな被害の発生を未然に防止することができるため、サイバー攻撃の被害に遭った

組織にとっても社会的全体にとっても非常に有益である。しかし、被害を受けた組織の現場にとっては、自組織のレピュテーションに影響しかねない情報共有等には慎重であるケースも多い。現場からは、被害に係る情報のうち、どのような情報をどのタイミングで、どのような主体と共有すればよいかを検討するに当たっての実務上の参考とすべきものがないため、適切に判断することが難しいとの声も聞かれる。

サイバー攻撃被害情報の円滑な共有や公表に向けては、サイバー攻撃被害組織等の立場にも配慮しつつ、サイバー攻撃被害に係る情報の共有・公表ガイダンスを設けることが必要である。こうした点について、総務省では、2020年度の調査研究事業（JPCERT/CC 実施）において指摘し、関連する基本的論点や方向性を整理・公表しており、本タスクフォースとしても、「総合対策2021」において、公的なガイダンスを作成・発信していく必要性に言及してきたところである。



【今後の取組】

かかる現状を踏まえ、総務省を含む関係省庁等では、2022 年４月、サイバーセキュリティ協議会運営委員会の下に、有識者からなる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」検討会を設置し、ガイダンス文書の検討を開始した。総務省は、同検討会の事務局として、技術情報等、組織特定に至らない情報の共有の在り方の整理を含め、サイバー攻撃被害を受けた組織において実務上の参考となるガイダンスを年内に策定すべく進めることが適当である。

エ．サイバーセキュリティ対策に係る情報開示の促進

【現状】

総務省では、民間企業によるサイバーセキュリティ対策の情報開示の重要

性について、認識を促進するため、2019 年６月に、民間企業の実際の開示事例等を盛り込んだ「サイバーセキュリティ対策情報開示の手引き[53]」を公表した。その後、手引きを踏まえ、企業のサイバーセキュリティ対策情報の開示状況を調査・公表したほか、それを踏まえて一定の企業を表彰する取組（サイバー・インデックス・アワーズ[54]）が登場している。

【今後の取組】

引き続き、サイバーセキュリティを巡る状況変化を踏まえながら、企業のサイバーセキュリティ対策情報の開示状況の調査・公表等の取組への必要な支援を行うことなどにより、適切な情報開示を促すことが重要である。

オ．サイバーセキュリティに関する功績の表彰を通じたモチベーション向上策

【現状】

総務省では、2017 年度より、サイバーセキュリティ対応の現場において優れた功績を挙げ、今後も更なる活躍が期待される個人又は団体を自薦又は他薦により募集し、その中から実績等を踏まえ、「サイバーセキュリティに関する総務大臣奨励賞」として毎年表彰している[55]。

【今後の取組】

情報共有、事案対処、人材育成、研究、国際標準化、普及啓発、コミュニティ形成等のサイバーセキュリティに係る様々な現場で活躍する現役世代は、我が国のサイバー強靱性の基盤である。こうした個人や団体を顕彰していくことで、現場のサイバーセキュリティ人材のモチベーションの向上を更に図るべく、「サイバーセキュリティに関する総務大臣奨励賞」について、一層の充実を図る必要がある。

（２）個人向けの普及啓発

サイバー空間と実空間の一体化の進展により、あらゆる主体がサイバー空間に参画する流れがある一方、サイバー攻撃の巧妙化・複雑化も増しているため、デジタル化の動きと呼応し「誰一人取り残さない」サイバーセキュリティの確保に向け、こどもや高齢者等に向けた普及啓発を通じて、社会全体のサイバーセキュリティ能力の向上に貢献することが求められる。

---

[53] https://www.soumu.go.jp/main_content/000630516.pdf

[54] 日本経済新聞社が主催する国際会議「サイバー・イニシアチブ東京」において、日本 IT 団体連盟の調査に基づいて、サイバーセキュリティで優れた成果を上げる企業や取り組みを表彰するもの。

[55] 2022 年の表彰者は以下のとおり報道発表を行っている（2022 年２月 28 日）。
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00130.html

また、利用者が安全に情報通信サービスを利用するためには、利用者一人ひとりがサイバーセキュリティ上の脅威を認識し、それを回避するための適切な対策を把握し、実践することが重要である。このため、利用者層に応じた普及啓発施策に取り組んでいく必要がある。

ア. 無線 LAN におけるサイバーセキュリティの確保

【現状】

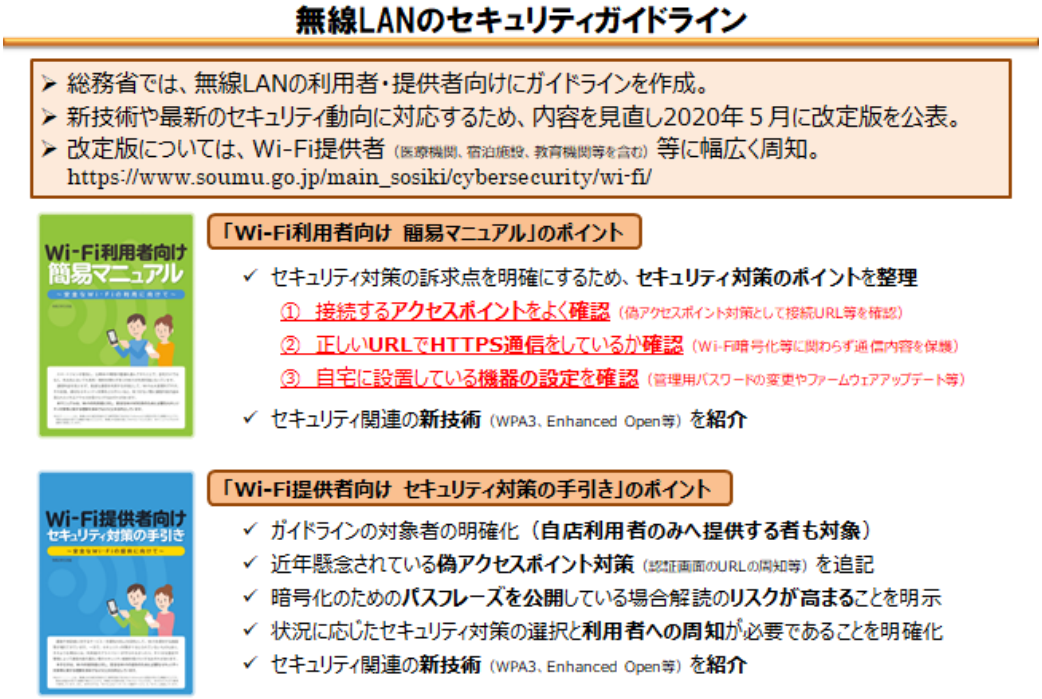
無線 LAN の利用者・提供者向けのセキュリティに関するガイドラインとして、2015 年に策定した「Wi-Fi 利用者向け簡易マニュアル[56]」及び「Wi-Fi 提供者向けセキュリティ対策の手引き[56]」について、新たな無線 LAN 規格の登場等を踏まえ、2020 年５月に改定し、総務省 Web サイトを通じて周知を行った。

また、2021 年 12 月から 2022 年１月にかけて、無線 LAN の利用者におけるセキュリティ意識や、無線 LAN の提供者におけるセキュリティ対策状況等を把握するため、利用者意識調査と提供者状況調査を実施し、その結果を公表した[56]。

さらに、無線 LAN の利用者のセキュリティ対策に関する周知啓発の一環として、オンライン動画講座を 2022 年２月 1 日から同年３月 25 日にかけて開講した。これは、有識者が無線 LAN 利用時のリスクや適切なセキュリティ対策等を動画全 12 回により紹介するもので、2204 名が受講登録を行った。また、若年層を含む利用者への周知を目的として、20 秒程度の動画コンテンツを作成し、SNS を通じて、2022 年２月１日から同年３月 25 日にかけて、238 万インプレッション（3.1 万クリック）の動画配信（広告）を行った[57]。

[56] ガイドライン類及び実態調査の結果は、次の URL にて公表している。
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

[57] 動画コンテンツについては註 56 の URL にて公表している。



【今後の取組】

総務省においては、無線 LAN のセキュリティ対策に関して、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いるところ、適切なセキュリティ対策を講じることによってプライバシー性の高い情報が保護されることを含め、この内容についてオンラインメディア等を活用して継続的な周知を実施する必要がある。

また、利用者に対するセキュリティ実態調査や提供者に対するセキュリティに配慮したサービスの提供状況調査等を行い、セキュリティ対策や対策意識の浸透状況を確認するとともに、必要に応じて各種ガイドラインの改定について検討を進めることが適当である。

イ．国民のためのサイバーセキュリティサイトを通じた普及啓発

【現状】

インターネットと情報セキュリティの知識の習得に役立ち、利用方法に応じた情報セキュリティ対策を講じるための基本となる情報を提供するために従前より運用している「国民のための情報セキュリティサイト」を、より情報の鮮度を保てるような更新を可能とするとともに、最新のセキュリティ動向を踏まえて最低限の内容更新を行うべく改修を実施し、新たに「国民のためのサイバーセキュリティサイト」と改称して 2022 年５月に公開した[58]。

[58] https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

【今後の取組】

近年、スマートフォンやタブレット等の新たな情報端末の普及でインターネット利用の増加やテレワークの普及による情報セキュリティを取り巻く状況に変化があるため、これに対応し、かつ国民のニーズに沿った形でサイバーセキュリティに関する情報を発信していく必要がある。「国民のためのサイバーセキュリティサイト」について、現在のセキュリティ状況を踏まえ、各内容を適時更新しつつ、改めて全体的な構成についても見直しを検討し、本サイトを通じてサイバーセキュリティに関する情報の周知・啓発をしていくことが引き続き重要である。

ウ. こどもや高齢者等に向けた普及啓発

【現状】

総務省では、誰もが安心・安全にインターネットを利用して、デジタルの恩恵を享受できるように、様々な取組を実施している。

こども向けの取組としては、「e-ネットキャラバン」として、インターネットの安全な利用に係る普及啓発を目的に、児童・生徒、保護者・教職員等

に対する学校等の現場での無料の出前講座を、情報通信分野等の企業・団体と総務省・文部科学省が協力して全国で開催している（実施主体は一般財団法人マルチメディア振興センター（FMMC）。2021 年度は、2559 件の講座を実施し、約 40 万人が受講）。

また、高齢者向けの取組としては、現在、総務省で実施している「デジタル活用支援推進事業」（民間企業や地方公共団体等と連携し、デジタル活用に不安のある高齢者等向けに、オンライン行政手続等のスマートフォンの利用方法に対する助言・相談等を行う取組）について、総務省・内閣官房で連携し、サイバーセキュリティの普及啓発の観点からの検討を進めた。

【今後の取組】

スマートフォンの保有割合やインターネットの利用割合が全世代で上昇しており[59]、これに伴い、サイバーセキュリティ上のリスクも高まっていることから、こども、高齢者といった特に注力すべきターゲットに向けて、以下のとおり、普及啓発を強化する必要がある。

まず、こども向けの「e-ネットキャラバン」、高齢者向けの「デジタル活用支援推進事業」の実施において、“Cybersecurity for ALL”の観点を考慮し、サイバーセキュリティ戦略本部における「サイバーセキュリティ意識・行動強化プログラム」の見直しも踏まえつつ、「e-ネットキャラバン」については、サイバーセキュリティの普及啓発に資する取組内容の充実を検討し、「デジタル活用支援推進事業」については、サイバーセキュリティに関する講座の追加に向けて検討する。

また、フィッシングの急拡大を踏まえ、電気通信事業者における対策（DMARC 対応等）を推進するほか、利用者向けには、メールや SMS の送信元やリンク先 URL をよく確認することの重要性を周知するなど、普及啓発の強化を検討する。その際、利用者には真偽の判別がつきづらい、送信元を偽装するなりすまし送信メールが 2020 年６月以降大幅に増加している[60]点についても十分に留意して普及啓発を進めることが必要である。

[59] 令和 3 年通信利用動向調査の結果（2022 年 5 月 27 日 総務省）
https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000158.html
[60] 詳細はサイバーセキュリティタスクフォース資料 36－3－2 フィッシングの現状（2021 年版）（フィッシング対策協議会）のとおり。
https://www.soumu.go.jp/main_content/000801033.pdf

Ⅲ　今後の進め方

「ICT サイバーセキュリティ総合対策 2022」は、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大等の動向や国際情勢の変化を踏まえて、社会全体のデジタル改革・DX の推進や経済安全保障の観点からもサイバーセキュリティの確保が主要課題であるとの認識の下で、当該課題への対処のために講じるべき施策を取りまとめたものである。総務省においては、「サイバーセキュリティ戦略」を初めとする政府方針に基づき、関係省庁と連携しつつ、今後、本提言を踏まえて「自由、公正、かつ安全なサイバー空間」の実現を下支えする情報通信ネットワークのサイバーセキュリティの確保等を図る観点から、各施策を具体的に推進していくことが求められる。なお、施策の推進に際しては、サイバー空間を取り巻く環境等が常に変化し続けていることを踏まえて、そうした変化に柔軟に対応しつつ、取り組んでいくことが必要である。

また、「ICT サイバーセキュリティ総合対策 2022」の推進に当たっては、社会全体のデジタル改革・DX 推進の主体となる多様なステークホルダーの理解と連携の下で効果的に進めていくことが必要である。こうした観点から、関係するステークホルダーとの間で、本提言及び提言の目的・狙い、ビジョンの共有を図り、取組の強化を図っていくべきである。

付録１　「サイバーセキュリティタスクフォース」開催要綱

「サイバーセキュリティタスクフォース」開催要綱

１　目的

サイバー空間は、あらゆる主体が利用する公共空間として、今後の経済社会の持続的な発展の基盤であるとともに、自由主義、民主主義、文化発展を支える基盤である。これを支える情報通信ネットワークのサイバーセキュリティを確保し、国民一人ひとりが安心してサイバー空間を利用できるようにすることは、いわば不可欠の前提としてますます重要になっている。

そこで、2020年東京オリンピック・パラリンピック競技大会における成果や「サイバーセキュリティ戦略」（2021年９月28日閣議決定）を踏まえつつ、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大などの動向に対応したサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、本タスクフォースを開催する。

２　名称

本タスクフォースは、「サイバーセキュリティタスクフォース」と称する。

３　主な検討・推進事項

（１）サイバーセキュリティに係る動向把握
（２）サイバーセキュリティを支える基盤・制度の在り方
（３）サイバーセキュリティを担う人材育成や普及啓発の在り方
（４）サイバーセキュリティ確保に向けた国際連携の在り方

４　構成及び運営

（１）本タスクフォースは、総務省サイバーセキュリティ統括官のタスクフォースとして開催する。
（２）本タスクフォースの構成員は、別添のとおりとする。
（３）本タスクフォースには、座長及び座長代理を置く。
（４）座長は、構成員による互選とし、座長代理は座長が指名する。
（５）座長は、本タスクフォースを招集し、主宰する。また、座長代理は、座長を補佐し、座長不在のときは、座長に代わって本タスクフォースを招集し、主宰する。
（６）本タスクフォースの構成員は、やむを得ない事情により出席できない場合において、代理の者を指名し、出席させることができる。

（７）座長は、必要に応じ、臨時構成員を指名又はオブザーバを招聘することができる。
（８）座長は、必要に応じ、外部の関係者の出席を求め、意見を聞くことができる。
（９）座長は、検討を促進するため、必要に応じ、分科会を開催することができる。
（１０）分科会の主査は、座長が指名する。
（１１）その他、タスクフォースの運営に必要な事項は、座長が定める。

５　議事・資料等の扱い

（１）本タスクフォースは、原則として公開とする。ただし、座長が必要と認める場合については、非公開とする。
（２）タスクフォースで使用した資料については、原則として、総務省のウェブサイトに掲載し、公開する。ただし、公開することにより、当事者又は第三者の利益を害するおそれがある場合若しくは座長が必要と認める場合については、非公開とする。
（３）本タスクフォースの議事要旨は、原則として公開とする。ただし、座長が必要と認める場合については、非公開とする。

６　スケジュール

本タスクフォースは、平成29年１月から開催する。

７　その他

本タスクフォースの事務局は、サイバーセキュリティ統括官室が行う。

（別添）

「サイバーセキュリティタスクフォース」構成員名簿

（敬称略、五十音順）

鵜飼（うかい） 裕司（ゆうじ）	株式会社 FFRI セキュリティ 代表取締役社長
宇佐美（うさみ） 理（おさむ）	日本テレビ放送網株式会社 ICT 戦略本部 専任部長
岡村（おかむら） 久道（ひさみち）	英知法律事務所 弁護士、京都大学大学院医学研究科講師
後藤（ごとう） 厚宏（あつひろ）	情報セキュリティ大学院大学 学長
小山（こやま） 覚（さとる）	NTT コミュニケーションズ株式会社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（しのだ） 佳奈（かな）	株式会社 BLUE 代表取締役
園田（そのだ） 道夫（みちお）	国立研究開発法人情報通信研究機構（NICT） サイバーセキュリティ研究所 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（つじ） 伸弘（のぶひろ）	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（とがわ） 望（のぞむ）	早稲田大学理工学術院 教授
徳田（とくだ） 英幸（ひでゆき）	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（なかお）　康二（こうじ）　ICT-ISAC　顧問、
国立研究開発法人情報通信研究機構（NICT）
サイバーセキュリティ研究所　主管研究員

名和（なわ）　利男（としお）　サイバーディフェンス研究所 専務理事/上級分析官

林（はやし）　紘一郎（こういちろう）　情報セキュリティ大学院大学 元学長・名誉教授

藤本（ふじもと）　正代（まさよ）　情報セキュリティ大学院大学 教授、
GLOCOM 客員研究員

吉岡（よしおか）　克成（かつなり）　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（わかえ）　雅子（まさこ）　株式会社読売新聞東京本社　編集委員

※ その他、議題に応じて、座長は臨時構成員を指名

付録２　これまでのサイバーセキュリティタスクフォースにおける検討状況

回　次	議 事 内 容
第34回 （R3.10.14）	✓ 「ICTサイバーセキュリティ総合対策2021」に基づく取組 ✓ 令和4年度総務省サイバーセキュリティ関連予算概算要求について ✓ IoTセキュリティに関連する近年の研究内容の紹介 ✓ 東京2020オリンピック・パラリンピック大会期間中のサイバー攻撃の動向（非公開）
第35回 （R4.1.14）	✓ 総務省におけるこれまでの取組及び最近のサイバーセキュリティの動向 ✓ 令和3年度補正予算及び令和4年度予算案における総務省サイバーセキュリティ関係事項について ✓ 今後検討いただきたい論点（案）
第36回 （R4.3.24）	✓ 開催要綱の改正について ✓ サイバーセキュリティを巡る最近の動向について ✓ 人材育成及び普及啓発等に係る課題について ✓ サイバーセキュリティ統合知的・人材育成基盤（CYNEX）に係る課題について
第37回 （R4.4.22）	✓ サイバーセキュリティを巡る最近の動向について ✓ 情報通信ネットワークの安全性・信頼性の確保に係るサイバーセキュリティ対策の現状と課題について ✓ 国際連携の現状と課題について
第38回 （R4.5.20）	✓ サイバーセキュリティを巡る最近の動向について ✓ 「ICTサイバーセキュリティ総合対策2022（仮）」の骨子案について
第39回 （R4.6.10）	✓ 「ICTサイバーセキュリティ総合対策2022」（案）について

付録３ 本文に記載した総務省作成ガイドラインの一覧

ガイドライン名	URL
5G セキュリティガイドライン第１版(2022 年４月)	https://www.soumu.go.jp/main_content/000812253.pdf
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（第３版）（2021 年９月）	https://www.soumu.go.jp/main_content/000771515.pdf
スマートシティセキュリティガイドライン（第 2.0 版）（2021 年６月）	https://www.soumu.go.jp/main_content/000757799.pdf
e シールに係る指針（2021 年６月）	https://www.soumu.go.jp/main_content/000756907.pdf
IoT セキュリティガイドライン ver1.0（2016 年７月）	https://www.soumu.go.jp/main_content/000428393.pdf
テレワークセキュリティガイドライン（第５版）（2021 年５月）	https://www.soumu.go.jp/main_content/000752925.pdf
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）（第３版）(2022 年５月）	https://www.soumu.go.jp/main_content/000816096.pdf
サイバーセキュリティ対策情報開示の手引き（2019 年６月）	https://www.soumu.go.jp/main_content/000630516.pdf
Wi-Fi 利用者向け簡易マニュアル（令和２年５月版）	https://www.soumu.go.jp/main_content/000690266.pdf
Wi-Fi 提供者向けセキュリティ対策の手引き（令和２年５月版）	https://www.soumu.go.jp/main_content/000690267.pdf