「ICTサイバーセキュリティ総合対策2022」（案）の概要

2022年〇月

総務省

Ⅰ サイバーセキュリティを巡る最近の動向

【サイバーセキュリティに関する政策動向】

- **サイバーセキュリティ戦略の策定（2021/9）**
  “Cybersecurity for All”をコンセプトに、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を掲げる。また、同戦略に基づく、重要インフラのサイバーセキュリティに係る行動計画の策定に向けた議論が行われている。
- **デジタル庁の設置（2021/9）**
  「デジタル社会の実現に向けた重点計画」では、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」を掲げる。
- **経済安全保障推進法の成立（2022/5）**
  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、経済安全保障推進法が成立・公布。

→情報通信分野を所管する総務省として、これらの政策動向を踏まえたサイバーセキュリティ施策の推進が必要。

【サイバーセキュリティ全般を巡る動向】

- **2020年東京オリパラ競技大会の終了**
  2021年7～9月の大会期間中4.5億回のサイバー攻撃を観測したが、大会運営に影響を及ぼすものは確認されず
  →教訓を踏まえた更なる攻撃対処能力向上が必要。
- **サイバー攻撃リスクの拡大**
  ランサムウェアやフィッシングの報告件数増加、Apache Log4jの脆弱性を狙う攻撃、Emotet感染再拡大、国際社会における安全保障を巡る状況の緊迫化等が発生。
  総務省含む関係省庁では、2022年2月以降、重要インフラ事業者や地方公共団体等への注意喚起を実施
  →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・団体等における、サイバー攻撃脅威の認識及び適切な対策の実施が必要。
- **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を契機に、テレワークやクラウドサービスの利用が拡大する等、デジタル化を支える情報通信ネットワークが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向上
  →情報通信ネットワークの安全性・信頼性の確保が必要。

これらを踏まえ、次の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**
2. **サイバー攻撃への自律的な対処能力の向上**
3. **国際連携の推進**
4. **普及啓発の推進**

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 ①
～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

➢ サイバー攻撃の大規模化・巧妙化・複雑化を踏まえ、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。また、クラウドサービス、5G、スマートシティや放送のサイバーセキュリティの確保に加え、横断的な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。

【主要課題】	【現状（主なもの）】	【今後の主な取組】
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	● **積極的なサイバーセキュリティ対策に関する総合実証の実施** ・ 通信の秘密に係る新たな法的整理を前提とした電気通信事業者におけるフロー情報※1分析によるC＆Cサーバ※2の検知 ※1: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 ※2: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 ・ 自動巡回による悪性Webサイト（フィッシングサイト等）の検知・共有 ・ RPKIやDNSSEC、DMARC※3等のネットワークセキュリティ技術の導入 ※3:BGPハイジャックに対するRPKI（Resource Public-Key Infrastructure）、DNSハイジャックに対するDNSSEC（DNS Security Extensions）、なりすましメールに対するDMARC（Domain-based Message Authentication Reporting and Conformance）が国際標準化されている。 ● **電気通信事業者におけるガバナンス確保の取組** ・ 電気通信事業ガバナンス検討会の議論に基づく「電気通信事業法の一部を改正する法律」の成立	● **R4年度の実証成果を踏まえた、実装に向けた総合実証の継続** ● **通信の秘密に配慮しつつ、電気通信事業者によるより迅速なサイバー攻撃対策を実現するための、制度改正の必要性も含めた検討** ● **「電気通信事業法の一部を改正する法律」について、下位法令の整備**
IoTにおけるサイバーセキュリティの確保	● **NOTICE注意喚起※4の実施** ※4:国立研究開発法人情報通信研究機構(NICT)がパスワード設定等に不備があるIoT機器の調査等を行い、ISPを通じ利用者へ注意喚起する取組。2023年度末に実施期限を迎える。 ● **NICTER注意喚起※5の実施** ※5:NICTが特定したマルウェア感染したIoT機器について、ISPを通じ利用者へ注意喚起する取組	● **NOTICEの取組の拡充及びその検討** ・ 調査対象ポート・プロトコルの拡大 ・ 2年後の実施期限を見据え、更なる対応に係る制度や予算支援の必要性を検討 ● **IoT機器製造事業者との連携**
情報通信分野におけるサプライチェーンリスク対策確保	● **「5Gセキュリティガイドライン第1版」の策定** ● **5Gセキュリティ対策の促進のための政策的措置（税制・免許）の実施**	● **「5Gセキュリティガイドライン第1版」の普及及び政策的措置の継続** ● **情報通信分野でのSBOM※6導入可能性の検討** ※6:Software Bill of Materials

上記のほか、**「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」**、**「スマートシティにおけるサイバーセキュリティの確保」**、**「ICT-ISACを通じた情報共有」**、**「放送設備におけるサイバーセキュリティ対策」**及び**「Beyond 5G・6Gに向けたサイバーセキュリティの検討」**を引き続き推進。

（2）トラストサービスの普及

➢ 既に整備した国によるタイムスタンプに係る認定制度等を引き続き適切かつ確実に運用・普及啓発するとともに、政府におけるデータ戦略、特に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、eデリバリー等データ流通の信頼性確保に係る検討を行う。

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 ②
～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

➢ 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、サイバー攻撃への自律的な対処能力を高めるため、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を構築する。

【主要課題】	【現状（主なもの）】	【今後の主な取組】
CYNEX等の推進	● NICTにおいて、サイバーセキュリティに係る技術・ノウハウ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となるCYNEXを構築し、2022年から試験運用。37組織が産学官コミュニティに参画**	● **2023年度の本格運用**に向けた継続的な構築・運用及び**産学官コミュニティの形成** ● **共用コンテンツの拡充**

（2）研究開発の推進

➢ 安全保障の観点を含む我が国をとりまく現下の課題認識に基づき、サイバーセキュリティに係る実践的な研究開発を推進する。その際、Beyond 5Gや耐量子計算機暗号等の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。

（3）人材育成の推進

➢ 我が国のサイバーセキュリティ人材が質的にも量的にも不足しており、NICTの「ナショナルサイバートレーニングセンター」を通じた人材育成の取組（CYDER、SecHack365）や、地域においてセキュリティ人材を自立的に育成するエコシステムの確立に向けた実証等の取組を引き続き実施し、深化させる。

【主要課題】	【現状（主なもの）】	【今後の主な取組】
実践的サイバー防御演習（CYDER）の実施	● 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**（年間100回、計3000名規模）	● **未受講の地方公共団体への受講の促進** ● 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**オンライン演習の演習効果向上のための改善**を実施
大規模イベント向け実践的サイバー演習の実施	● 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、東京オリパラ競技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」について、2020年度での終了後、**本演習内容をCYDERのプログラムに準上級コースとして組み込み、レガシーとして継続的に活用**	● 2025年日本国際博覧会側からの要望を踏まえつつ、**「サイバーコロッセオfor万博（仮）」として、関連組織のセキュリティ担当者等を対象に高度な攻撃にも対処可能な人材の育成を実施できるよう検討。**

上記のほか、**「SecHack365の実施」**及び**「地域人材エコシステムの形成」**を引き続き推進。

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 ③
～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り、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ことから、各国政府・民間レベルでの情報共有や国際標準化活動に積極的に関与する。また、世界全体のサイバーセキュリティのリスクを低減させる等の観点から開発途上国に対する能力構築支援を行うとともに、国内企業のサイバーセキュリティ分野の国際競争力向上を図る取組も推進する。

【主要課題】	【現状（主なもの）】	【今後の主な取組】
有志国との二国間連携の強化	● G7各国を中心に**総務省のサイバーセキュリティ政策の積極的な発信や意見交換**を実施	● 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との関係強化等を踏まえ、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、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二国間・多国間の関係性構築を推進**
多国間会合を通じた有志国との連携の強化	● OECDの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 ● 日ASEANサイバーセキュリティ政策会議等の**多国間の枠組みに積極的に参画** ● 日米豪印首脳会合（2022年5月）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」**公表	
ISACを通じた民間分野での国際連携の促進	● **一般社団法人ICT-ISAC及び米国IT-ISACによる定期会合の開催を通じた連携の強化** ● **ISP向け日ASEAN情報セキュリティワークショップの開催**	● 情報共有自動化等に向けた**日米ISAC間連携の継続** ● EUをはじめとする**他の国・地域のISAC関連組織との連携促進** ● **ASEAN地域における民間レベルでの脅威情報共有基盤を活用したワークショップの検討**等
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	● **2018年にバンコクに設立した日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）**において、CYDER等を通じて、ASEANのセキュリティ人材の育成支援を実施**（2022年4月時点で787名が参加）	● **オンライン・オンサイトで受講可能なプログラム拡充** ● **有志国との第三者連携や国内企業との連携の強化** ● **研修等への参加者のすそ野拡大** ● **ASEAN以外のインド太平洋地域における能力構築支援の検討**
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	● **2021年10月に、日本発のノウハウである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** ● **「IoTセキュリティガイドライン」の国際標準への反映における貢献**（ISO/IEC 27400として発行）	● **5Gセキュリティ等の我が国の取組について、国際標準化等の可能性について継続的に検討** ● **「自由、公正かつ安全なサイバー空間」の理念に整合しない動きに対して、必要な連携を強化**
国内企業のASEAN地域等に向けた国際展開支援	● **ASEAN地域を中心に、国内企業のサイバーセキュリティ製品等の海外展開を支援するための実証を実施**	● **我が国における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**

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 ④
～4 普及啓発の推進～

➢ "Cybersecurity for ALL" の観点から、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よう、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。

（1）事業者向けの普及啓発

【主要課題】	【現状（主なもの）】	【今後の主な取組】
テレワークにおけるサイバーセキュリティの確保	● **「テレワークセキュリティガイドライン」**（2021年５月改定、第５版）**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）」**（2022年５月改定、第３版）を整備 ● 2021年12月から2022年１月にかけ、**テレワーク導入企業等におけるセキュリティ対策状況の実態調査アンケートを実施**し、結果を公表	● **左記ガイドライン及び中小企業向け手引き（チェックリスト）の一層の周知** ● **実態調査結果を踏まえたガイドライン類の再改定の検討**
地域セキュリティコミュニティの強化	● **「地域SECUNITY」**（地域セキュリティコミュニティ）**を全国11の地域ブロックに形成し、**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の開催等による**普及啓発の取組を支援**	● 地域の取組への支援を継続するとともに、**先進的な取組について、他地域への横展開を推進**
サイバー攻撃被害に係る情報の共有・公表の適切な推進	● 2020年度の総務省調査研究の成果として、サイバー攻撃被害を受けた組織の立場にも配慮した、**サイバー攻撃被害情報の円滑な共有・公表に向けた基本的論点や方向性を整理・公表**	● サイバーセキュリティ協議会運営委員会下に2022年4月に設置した検討会において、**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**

上記のほか、**「サイバーセキュリティ対策に係る情報開示の促進」**及び**「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」**を引き続き推進。

（2）個人向けの普及啓発

こどもや高齢者等に向けた普及啓発	● 情報通信分野の企業等と総務省・文科省が協力し、**インターネットの安全な利用に係る無料の出前講座を「e-ネットキャラバン」として学校等で開催**（2021年度は2,559件の講座を実施し、約40万人が受講） ● **デジタル活用に不安のある高齢者等向けに、「デジタル活用支援推進事業」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検討**	● **「e-ネットキャラバン」について、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** ● **「デジタル活用支援推進事業」について、サイバーセキュリティに関する講座の追加に向けた検討** ● **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のほか、利用者向けの普及啓発の強化を検討（送信元を偽装するなりすまし送信メールへの留意等）**

上記のほか、**「無線LANにおけるサイバーセキュリティの確保」**及び**「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」**を引き続き推進。