資料44－3

「ICTサイバーセキュリティ総合対策2023」（案）の概要

令和５年６月

サイバーセキュリティタスクフォース事務局

「ICTサイバーセキュリティ総合対策2023」（案）の概要

【サイバーセキュリティに関する政策動向】

- **国家安全保障戦略の策定（2022/12）**
- **経済安全保障推進法に基づく基幹インフラ役務の安定的な提供の確保に係る基本方針の策定（2023/4）**

【サイバーセキュリティ全般を巡る動向】

- **サイバー攻撃リスクの拡大（安全保障を巡る状況の緊迫化等）**
- **情報通信ネットワークへの依存度の更なる高まり**

今やサイバー空間は、あらゆる主体が利用する公共空間となり、サイバー攻撃も政府機関や重要インフラのみならず、あらゆる主体が標的となっていることを踏まえれば、平時から官民を挙げて我が国全体としてサイバーセキュリティを強化していくことが重要。

1．情報通信ネットワークの安全性・信頼性の確保

- 総合的なIoTボットネット対策の推進（NOTICEの延長・拡充、フロー情報の分析によるC&Cサーバの検知に関する実証等）
- 情報通信分野におけるサプライチェーンリスク対策（SBOM（エスボム）導入可能性の検討、スマートフォンアプリ検証等）
- トラストサービスの普及（タイムスタンプの認定制度の必要な見直しの検討、eシールの認定制度創設を含めた検討等）

2．サイバー攻撃への自律的な対処能力の向上

- 今年度から本格運用を開始するCYNEX（サイネックス）（サイバーセキュリティ統合知的・人材育成基盤）の活動強化
- CYNEXを活用した「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（CYXROSS（サイクロス））」の開始
- NICTが実施する実践的サイバー防御演習（CYDER（サイダー））について、重要インフラ事業者への提供拡大やオンライン演習の改良等、演習規模の拡大を検討するとともに、サイバー安全保障分野における人材育成への活用等を推進
- 2025年大阪・関西万博に向けた、サイバー防御演習（CIDLE（シードル））の推進

3．国際連携の推進

- 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）の拡充（プログラムの充実、有志国との連携強化等）
- 大洋州島しょ国向けのセキュリティ人材育成支援プロジェクトの立ち上げを検討

4．普及啓発の推進

- テレワークセキュリティガイドライン・チェックリストの一層の周知と、ガイドライン類の改正を検討
- 地域SECUNITYにおける先進的な取組の横展開の推進等更なる強化支援
- こどもや高齢者に向けたサイバーセキュリティの普及啓発の強化

Ⅱ「ICTサイバーセキュリティ総合対策2023」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）総合的なIoTボットネット対策の推進

➢ サイバー攻撃の大規模化・巧妙化・複雑化を踏まえ、DDoS攻撃のように情報通信ネットワークの機能に支障を生じさせるような大規模サイバー攻撃に対応するため、総合的なIoTボットネット対策を講じていく。

「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分科会※1とりまとめ（案）」に基づく取組

※1：本タスクフォースの下に本年１月に設置し、総合的なボットネット対策の実現に向け、端末（IoT機器）側、ネットワーク側各々について今後取り組むべき対応策について検討を実施

- **端末（IoT機器）側の今後の対応策（NOTICE）**
  - ①脆弱性等のあるIoT機器の調査の延長・拡充
  - ②利用者への注意喚起等の実効性向上
  - ③メーカーやSIer等の幅広い関係者との連携による総合的な対処
  - ④①～③を効果的に実施するためのNOTICEの運営体制の強化
- **ネットワーク側その他の今後の対応策**
  - ①C&Cサーバの検知精度の向上・検知情報の共有・利活用等の推進
  - ②IoTボットネットの全体像の可視化

（２）その他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の推進

➢ 悪性Webサイトの検知技術・共有手法の実装可能性検証及びISPにおけるネットワークセキュリティ技術の導入及び普及促進に関する調査を引き続き実施する。また、広く普及が進むクラウドサービスや5Gサービス等におけるサイバーセキュリティの確保に加え、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。

【主要課題】	【現状（主なもの）】	【今後の主な取組】
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** ● **情報通信分野でのSBOM※2導入可能性の検討** ※2:Software Bill of Materials ● **スマートフォンアプリの挙動の技術的な解析可能性について検証**	● **情報通信分野でのSBOM導入可能性の検討を継続** ● **スマートフォンアプリの挙動の技術的な解析可能性について検証を継続**

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。

（３）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、各種トラストサービスの普及に向けた取組を推進する。

データのやりとりにおけるトラストの確保	● **タイムスタンプに係る認定制度の運用** ● **eシールサービスの状況把握のための調査研究等の実施**	● **タイムスタンプの認定制度について必要に応じた見直しを検討** ● **eシールに関する国による認定制度創設を含めた検討**

Ⅱ「ICTサイバーセキュリティ総合対策2023」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年度から試験運用。55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** ● **CYXROSS**※3**の開始** ※3: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

（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、AI等の中長期的な技術トレンドを視野に入れ、IoT機器を様々な方法で悪用するサイバー攻撃等、変性する脅威に対抗する柔軟な取り組みが求められる。

（３）人材育成の推進

➢ 人材不足に起因したインシデントの発生や被害の拡大が相次ぎ、サイバーセキュリティ人材の育成が喫緊の課題となっていることから、NICTナショナルサイバートレーニングセンターにおいて実施する実践的サイバー防御演習（CYDER）や万博向けサイバー防御講習（CIDLE）等の人材育成の取組を拡充することが求められる。

【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3,000名規模）	● 未受講の地方公共団体への**受講促進** ● **オンライン演習**の**改良と活用推進** ● **重要インフラ事業者**への**提供拡大** ● **サイバー安全保障分野**における人材育成への**活用調整**
万博向けサイバー防御講習（CIDLE）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2020年度まで**東京オリパラ競技大会関連組織を対象とした実践的サイバー演習「サイバーコロッセオ」**を実施した実績等を踏まえ、**大阪・関西万博主催者**（日本国際博覧会協会）及び**関係自治体**（大阪府及び大阪市）から**サイバーセキュリティ人材育成支援の要請あり**	● 大阪・関西万博主催者等からの要請を踏まえ、同主催者等と緊密に連携し、大阪・関西万博の安全な開催に資するよう**「万博向けサイバー防御講習（CIDLE）」を実施**

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2023」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	● G7デジタル技術大臣宣言 、安全で強靱なデジタルインフラの構築に向けたG7アクションプラン 及び2023年５月の日米豪印首脳会合共同声明を踏まえ、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	● G7アクションプランにおいて世界銀行等の国際機関と連携した、発展途上国へのデジタルインフラ支援を確認 ● 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（2023年5月）においてサイバーへの意識向上を目的とした**「サイバー・チャレンジ」や各種共同原則**を歓迎	
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および米国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**（2023年4月時点で1,148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2023」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事業・業種を問わず、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）を整備し、「設定解説資料」を拡充 ● 2022年11月から2023年１月にかけ、**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の実施状況を調査**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改定検討**
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を踏まえ、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**「サイバー攻撃被害に係る情報の共有・公表ガイダンス」**（2023年3月）を**公表**	● 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」について、関係省庁と連携しつつ、所管事業者等に対して、普及啓発を推進

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**（2022年度は2,226件の講座を実施し、約36万人が受講） ● **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利活用に向けた検討**

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。