資料38－2

「ICTサイバーセキュリティ総合対策2022（仮）」の骨子（案）

令和４年５月

サイバーセキュリティタスクフォース事務局

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

➢ 過去４回のサイバーセキュリティタスクフォースにおいて、2021年７月の「ICTサイバーセキュリティ総合対策2021」の策定・公表以降のサイバー攻撃を巡る最近の動向や総務省のサイバーセキュリティ政策に係る取組等について御議論いただいてきたところ。

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

- 「ICTサイバーセキュリティ総合対策2022（仮）」については、本タスクフォースでの御議論や昨今のサイバーセキュリティの動向を踏まえ、**第35～37回タスクフォースにおける論点に沿った構成に再編（→次頁）し、各施策の現状及び今後取組むべき事項を記載**することとしてはどうか。
- また、「ICTサイバーセキュリティ総合対策2021」では別添資料としていた、施策の進捗状況をまとめた**「プログレスレポート」の内容は**、一覧性を重視し**本文に盛り込む**こととしてはどうか。

「ICTサイバーセキュリティ総合対策2022（仮）」の構成案

Ⅰ サイバーセキュリティを巡る最近の動向

Ⅱ 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

（１）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
（２）情報通信分野におけるサプライチェーンリスク対策
（３）IoTにおけるサイバーのセキュリティの確保
（４）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
（５）スマートシティのサイバーセキュリティの確保
（６）ICT-ISACを通じた情報共有
（７）放送設備におけるサイバーセキュリティの確保
（８）Beyond 5G・6Gに向けたサイバーセキュリティの検討

2 トラストサービスの普及

Ⅲ サイバー攻撃への自律的な対処能力の向上

1 CYNEX等の推進

2 研究開発の推進

3 人材育成の推進

（１）実践的サイバー防御演習（CYDER）の実施
（２）大規模イベント向け実践的サイバー演習の実施
（３）SecHack365の実施
（４）地域人材エコシステムの形成

Ⅳ 国際連携の推進

（１）二国間連携
（２）多国間連携
（３）ISAC間連携
（４）能力構築支援
（５）国際標準化
（６）国際展開支援

Ⅴ 普及啓発の推進

1 事業者向けの普及啓発

（１）テレワークにおけるサイバーセキュリティの確保
（２）地域セキュリティコミュニティの強化
（３）サイバー攻撃被害に係る情報の共有・公表の適切な推進
（４）サイバーセキュリティ対策に係る情報開示の促進
（５）サイバーセキュリティに関する功績の表彰

2 個人向けの普及啓発

（１）無線LANにおけるサイバーセキュリティの確保
（２）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
（３）こどもや高齢者等に向けた普及啓発

Ⅰ サイバーセキュリティを巡る最近の動向

➢ 2021年７月の「ICT サイバーセキュリティ総合対策2021」の策定以降の状況変化として以下のような点を盛り込むこととしてはどうか。

- **政府内におけるサイバーセキュリティに関する動向**
  - 「サイバーセキュリティ戦略」の閣議決定（2021年9月）
    ”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柱として策定されており、総務省として同戦略を踏まえた取組の推進が求められる。また、同戦略に基づき、重要インフラ行動計画の改定に向けた議論が進んでいる。
  - デジタル庁の設置（2021年９月）
    「デジタル社会の実現に向けた重点計画」（2021年12月閣議決定）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。
- **サイバーセキュリティ全般を巡る動向**
  - 2020年東京オリンピック・パラリンピック競技大会の終了
    大会運営に支障を生じるようなサイバー攻撃は確認されなかったが、本大会の教訓を踏まえ、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ることが重要。
  - 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報告件数の増加、NICTER観測のサイバー攻撃関連通信数の増加傾向、Emotet再拡大、ロシアによるウクライナ侵略などの国際社会における安全保障を巡る状況の緊迫化等、サイバー攻撃リスクは拡大している。政府としても、2022年２月23日、３月１日、同月24日、４月25日に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。こうした動向を踏まえ、政府機関や重要インフラ事業者をはじめとする企業・団体等においては、サイバー攻撃の脅威に対する認識をより一層深めるとともに、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を背景としたテレワークの利用の拡大・定着など、デジタル活用がますます進展し、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とともに、国際社会における安全保障を巡る状況の緊迫化に伴い、国家間の競争・衝突の場となる中、情報通信ネットワークは、国民生活や経済活動の基盤としてその重要性が高まっていると考えられる。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 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

➢ 情報通信ネットワークの安全性や信頼性を強化し、利用者の安心を確保するため、電気通信事業者等による積極的なサイバーセキュリティ対策、情報通信分野におけるサプライチェーンリスク対策、IoT、クラウドサービス、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の確保等を推進することとしてはどうか。

- **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**
  - 令和３年度補正予算で実施する、①C＆Cサーバの検知技術、②悪性Webサイト（フィッシングサイト等）検知技術・共有手法及び③ネットワークセキュリティ対策技術（RPKI等）の実証については、その結果を踏まえつつ、技術精度向上や事業者における自走化等を図る観点から2023年度も継続する。また、RPKIやDNSSEC、DMARC等の効果的な脆弱性対策手法の普及方策等を検討する。
  - 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する。
  - 電気通信事業ガバナンス検討会における議論を踏まえ、現在国会審議中の「電気通信事業法の一部を改正する法律案」のうち、①大規模な事業者が取得する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、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について、法案が成立した場合には、必要な制度整備を行う。
- **情報通信分野におけるサプライチェーンリスク対策**
  - 5Gネットワークのセキュリティに関する技術的検証の取組の成果の一部として、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、国内の5Gネットワークのセキュリティの確保を進める。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。
  - 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も重要となる中、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。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。

II 情報通信ネットワークの安全性・信頼性の確保②

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（続き）

- **IoTにおけるサイバーセキュリティの確保**
  - NOTICEについては、調査ポートの拡大等の調査の詳細化・高度化やISPから利用者への注意喚起効果の改善を図る。２年後に実施期限を迎えるNOTICEの在り方を含め、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も含め検討する。
  - IoTにおけるサイバーセキュリティの確保を推進していく上で、機器メーカとの連携の強化を図る。
- **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**
  - 2021年９月に改定した「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」の普及促進を図るとともに、2022年中に「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）」を策定・公表する。
- **スマートシティのサイバーセキュリティの確保**
  - 2021年６月に改定した「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海外の政府機関との意見交換の取組を行う。
- **ICT-ISACを通じた情報共有**
  - 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、関係者による取組を促進する。
- **放送設備におけるサイバーセキュリティの確保**
  - 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、更なるサイバーセキュリティ対策の必要性を検討する。
- **Beyond 5G・6Gに向けたサイバーセキュリティの検討**
  - 5Gセキュリティに関する既存施策を着実に実施するとともに、Beyond 5G・6G を念頭に、サイバー空間に関する将来動向を主体的に把握し、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や、サイバー空間のガバナンスやルールの形成に積極的に関与していくため、関係する国際的な議論の状況の調査及び国内における議論の活性化に資する取組を実施する。

トラストサービスの普及

- 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ことを踏まえ、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、引き続き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としてはどうか。

Ⅲ 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）、研究開発、人材育成の推進

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について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べく、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を進めることとしてはどうか。

- **情報収集・分析**
  - 取得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、早期の本格稼働に向けて、システム基盤構築・運営環境整備をサイバーセキュリティタスクフォースに報告しつつ引き続き進める。
  - 産学官の関係性を深め、コミュニティの形成を積極的に推進し、これらの組織がより深い関係性と信頼を築けるよう運営する。
  - 国内のマルウェア感染状況について、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。
- **人材育成**
  - 演習の実施に必要なデータセット、計算機リソース等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、産学官の連携により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踏まえつつ、自立的な人材育成に向けた取組を進める。

研究開発の推進

➢ Beyond 5G等の中長期的な技術トレンドを視野に入れつつ、以下のように、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いた実践的な研究開発を推進することとしてはどうか。

- **NICTにおける研究開発**
  - 巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術などの研究開発を引き続き実施する。
  - 耐量子計算機暗号等を含む新たな暗号・認証技術や高機能暗号技術の研究開発を実施し、成果普及を図る。
- **大学や民間企業における研究開発の支援等**
  - 暗号技術に関し、主に安全性評価の観点から、2022年度末目途に予定されているCRYPTREC暗号リストの10年に一度の全面改定に向けた検討を進めるとともに、耐量子計算機暗号、軽量暗号や高機能暗号のガイドライン作成を行う。

Ⅲ サイバー攻撃への自律的な対処能力の向上②

CYNEX（サイバーセキュリティ統合知的・人材育成基盤）、研究開発、人材育成の推進

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。そのため、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）を積極的に推進するとともに、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引き続き行うこととしてはどうか。

- **実践的サイバー防御演習（CYDER）の実施**
  - 未受講の地方公共団体がサイバーセキュリティ上の穴とならないよう、出前講習やサテライト講習といった形態も活用して受講を促進するとともに、地理的・時間的要因等によりCYDERが受講できない者への対応として、2021年度から追加実施しているオンライン演習は今後も積極的に進める。

- **大規模イベント向け実践的サイバー演習の実施**
  - 大阪・関西万博事務局の要望を踏まえ、東京オリパラ時の「サイバーコロッセオ」の経験を活用して、「サイバーコロッセオfor万博（仮）」を実施し、関連組織のセキュリティ担当者を対象に高度な攻撃にも対処できる人材育成を行う。

- **SecHack365の実施**
  - 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。

- **地域人材エコシステムの形成**
  - 地域において、民間による雇用の受け皿創出とともに、就業の場の確保と就業につながる研修を一体的に行い、モデル事業対象地域における人材エコシステムの確立を図るとともに、その成果を他地域にも横展開して活用できるよう進める。

Ⅳ 国際連携の推進

➢ 各国政府・民間レベルでのサイバーセキュリティ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るとともに、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発展途上国に対する能力構築支援を行うほか、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としてはどうか。

① 二国間連携

- 総務省主催のICT政策対話等の経験を踏まえ、引き続き、情報の自由な流通という理念を共有する国を中心に、連携強化を図る。

② 多国間連携

- 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との関係強化を踏まえ、引き続き、情報の自由な流通という理念を共有する国を中心に、連携強化を図る。

③ ISAC間連携

- ICT-ISACと米国IT-ISAC間でより効果的な情報共有の在り方を引き続き模索するとともに、EUをはじめとする他の国・地域のISAC関連組織との連携を促進する。
- 日ASEAN情報セキュリティワークショップの経験を踏まえ、民間の脅威情報共有基盤を活用したASEAN地域のISP向けワークショップの在り方について検討を進める。

④ 能力構築支援

- 2018年設立の日ASEANサイバーセキュリティ能力構築センター(AJCCBC)におけるCYDER 等を引き続き実施する。
- 「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（サイバーセキュリティ戦略本部決定）」の方針に則り、AJCCBCが実施する研修参加者のすそ野拡大や、ASEAN以外のインド太平洋地域における能力に係る構築支援について検討を進める。

⑤ 国際標準化

- 「IoTセキュリティガイドライン」の国際標準化に向けた活動に引き続き貢献していくほか、「自由、公正かつ安全なサイバー空間」という我が国の基本的理念に必ずしも整合的でない動きに積極的な対処ができるよう連携体制の強化に取り組む。

⑥ 国際展開支援

- ASEAN諸国を中心とした海外展開支援に係る調査等を踏まえ、「ICT国際競争力強化パッケージ支援事業」等の取組を通じ、我が国の成功事例の海外展開や製品・サービスの海外プロモーションを推進する。

Ⅴ 普及啓発の推進①

事業者向けの普及啓発

- ”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、中小企業等のテレワークにおけるサイバーセキュリティの確保を推進するとともに、地域におけるセキュリティコミュニティの強化を進めてはどうか。
- 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・公表の適切な推進に向けた取組等を引き続き進めてはどうか。

- **テレワークにおけるサイバーセキュリティの確保**
  - 2021年5月に改定した「テレワークセキュリティガイドライン」及び2022年5月に改定した「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）」について、関係省庁や関連団体・企業等とも連携してテレワーク勤務者や実施企業に広く周知するとともに、民間企業等におけるテレワークセキュリティの実態調査を踏まえた再改定についても引き続き検討する。
- **地域セキュリティコミュニティの強化**
  - 関係機関と連携しつつ、各地域でのセミナーやインシデント対応演習等の開催を支援することにより、「地域SECUNITY」（地域セキュリティコミュニティ）の強化を行う。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等の、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。
- **サイバー攻撃被害に係る情報の共有・公表の適切な推進**
  - 2022年４月にサイバーセキュリティ協議会運営委員会の下に設置された「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。
- **サイバーセキュリティ対策に係る情報開示の促進**
  - 2019年６月に公表した「サイバーセキュリティ対策情報開示の手引き」に基づき、引き続き、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。
- **サイバーセキュリティに関する功績の表彰**
  - 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ている個人・団体を表彰する「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。

Ⅴ 普及啓発の推進②

個人向けの普及啓発

➢ あらゆる主体がサイバー空間に参画することとなる中で、無線LANにおけるサイバーセキュリティの確保、新たに公開する「国民のためのサイバーセキュリティサイト」を通じた周知啓発、インターネットの安全・安心な利用に向けたこどもや高齢者等に向けた普及啓発を通じて、社会全体ののサイバーセキュリティ能力の向上に貢献することとしてはどうか。

- **無線LANにおけるサイバーセキュリティの確保**
  - これまでに実施したオンライン動画講座等の経験を踏まえ、オンラインメディア等を活用し、「Wi-Fi利用者向け簡易マニュアル」及び「Wi-Fi提供者向けセキュリティ対策の手引き」の継続的な周知を実施する。
  - 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。

- **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**
  - 「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を更新して2022年５月に改称・公開する「国民のためのサイバーセキュリティサイト」について、サイバーセキュリティを取り巻く状況変化や国民のニーズを勘案しつつ全体的な更新を検討しながら、平行して本サイトを通じた周知・啓発を継続する。

- **こどもや高齢者等に向けた普及啓発**
  - “Cybersecurity for ALL”の観点から、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、児童・生徒等に対する学校等での無料の出前講座を全国で開催する「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「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対応の推進等）のほか、利用者向けの普及啓発の強化を検討する。