資料５－２

総務省におけるサイバーセキュリティ施策の取組状況について

2022年９月

総務省サイバーセキュリティ統括官室

（1）「ICTサイバーセキュリティ総合対策2022」（令和4年8月12日公表）の概要

- 総務省では、2017年から「サイバーセキュリティタスクフォース」（座長：後藤厚宏情報セキュリティ大学院大学学長）において、情報通信分野におけるサイバーセキュリティに係る課題の整理や必要な取組の検討を実施。
- サイバーセキュリティ戦略の策定（2021年9月）、サイバー攻撃リスクの拡大等も踏まえ、パブリックコメントを経て2022年８月12日に、今後重点的に取り組むべき施策として「ICTサイバーセキュリティ総合対策2022」を取りまとめ。

１．情報通信ネットワークの安全性・信頼性の確保

- 2022年度の実証の成果を踏まえ、2023年度も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、制度改正の必要性も含めて検討
- 2年後に実施期限を迎えるNOTICE（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、電気通信事業者を通じて利用者に注意喚起を行う）の取組の拡充及びその検討
- 情報通信分野でのSBOM（ソフトウェア部品表）の導入可能性の検討

２．サイバー攻撃への自律的な対処能力の向上

- 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）の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
- NICTが実施する実践的サイバー防御演習（CYDER）について、未受講の地方公共団体への受講の促進や、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
- 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）」の関連組織セキュリティ担当者等への実施を検討

３．国際連携の推進

- ASEANのセキュリティ人材の育成支援を実施する日ASEANサイバーセキュリティ能力構築センター（AJCCBC）について、プログラム拡充、有志国との第三者連携等の強化を図るとともに、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
- 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を継続的に検討し、国際標準化機関において発信

４．普及啓発の推進

- 中小企業等への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や、地域SECUNITYでのインシデント対応演習の開催支援
- 2022年内に、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」を策定
- 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を検討

（2）サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

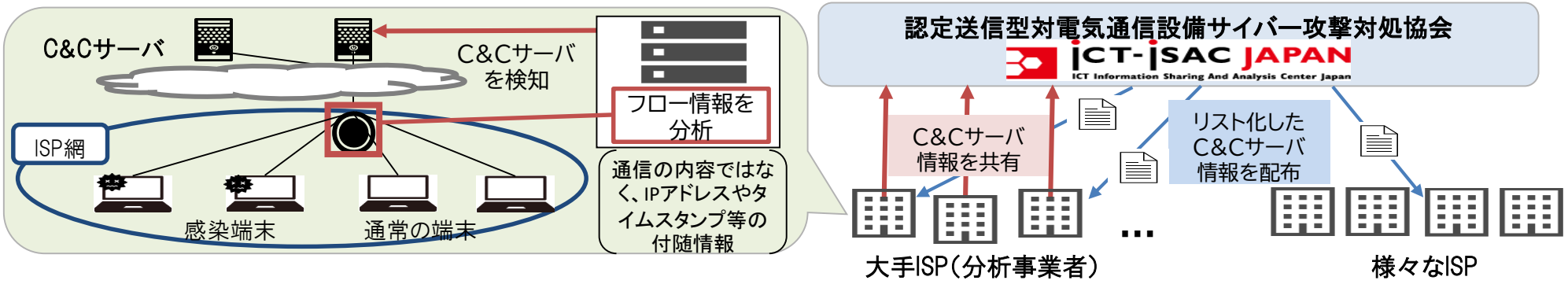
● 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が、より効率的・積極的に対処できるようにするため、①サイバー攻撃の指示を出す管理サーバ（C&Cサーバ）検知技術の実証、②フィッシングサイト等の悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ対策手法の導入に係る実証等を実施。

令和5年度要求額 18.0億円 （令和3年度補正予算 18.0億円）

① フロー情報分析によるC&Cサーバ検知技術の実証

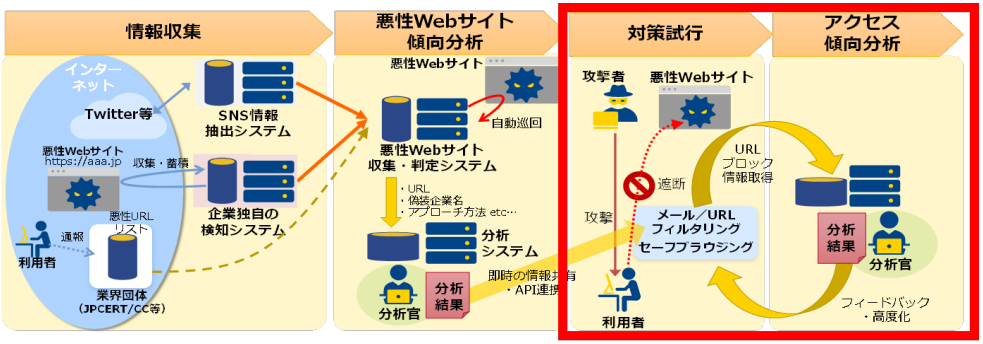
※C&Cサーバ：ボットネットを構成する各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

インターネット利用者のトラヒックのうちフロー情報を大規模かつ統計的・相関的に分析し、C&Cサーバを検知する手法の有効性や、C&Cサーバの検知・共有に当たっての技術・運用面の課題を整理。



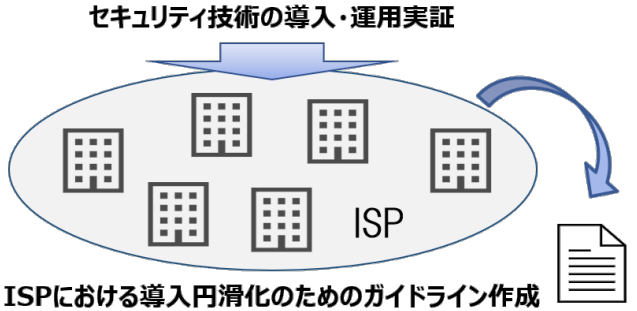
② 悪性Webサイトの検知技術・共有手法の実証

悪性Webサイト（フィッシングサイト等）の情報を収集・分析し、検知する手法の有効性を実証するとともに、検知結果を活用し継続的な対策を講じるための必要事項を整理。



③ ネットワークセキュリティ対策技術の導入実証

ISPにおけるセキュリティ対策を強化するため、ネットワークセキュリティ対策技術の円滑な導入、実装及び運用に係る技術的な諸課題を整理。



（2）ナショナルサイバートレーニングセンターの強化

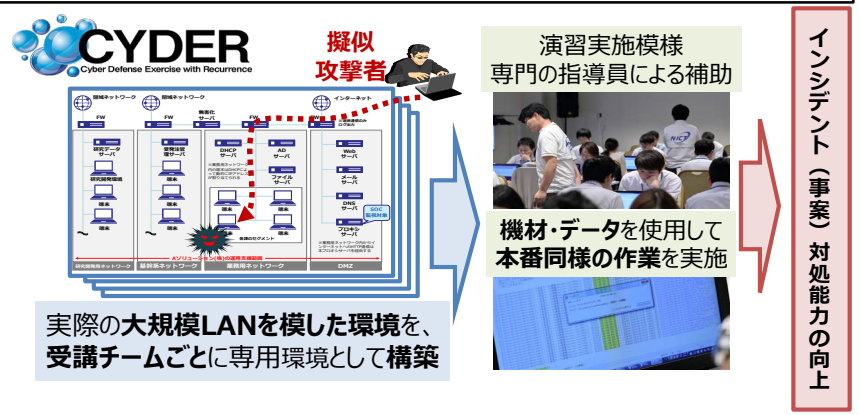
● 巧妙化・複雑化するサイバー攻撃に対し、国立研究開発法人情報通信研究機構（NICT）に設置した「ナショナルサイバートレーニングセンター」において、実践的な対処能力を持つセキュリティ人材等を育成し、我が国のサイバーセキュリティを強化。

令和5年度要求額 13.0億円（令和4年度予算額 11.9億円）

①CYDER（実践的サイバー防御演習）

国の行政機関、地方公共団体、独立行政法人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実践的サイバー防御演習（CYDER）を実施。

※オンライン受講環境を令和３年度より本格稼働。



②SecHack365（若手セキュリティイノベータの育成）

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得る最先端のセキュリティ人材を育成。

③万博向け演習プログラムの提供

2025年日本国際博覧会（大阪・関西万博）開催に向けて、万博関連組織の情報システム担当者等を対象に、CYDERを基にした人材育成の演習プログラムを提供。

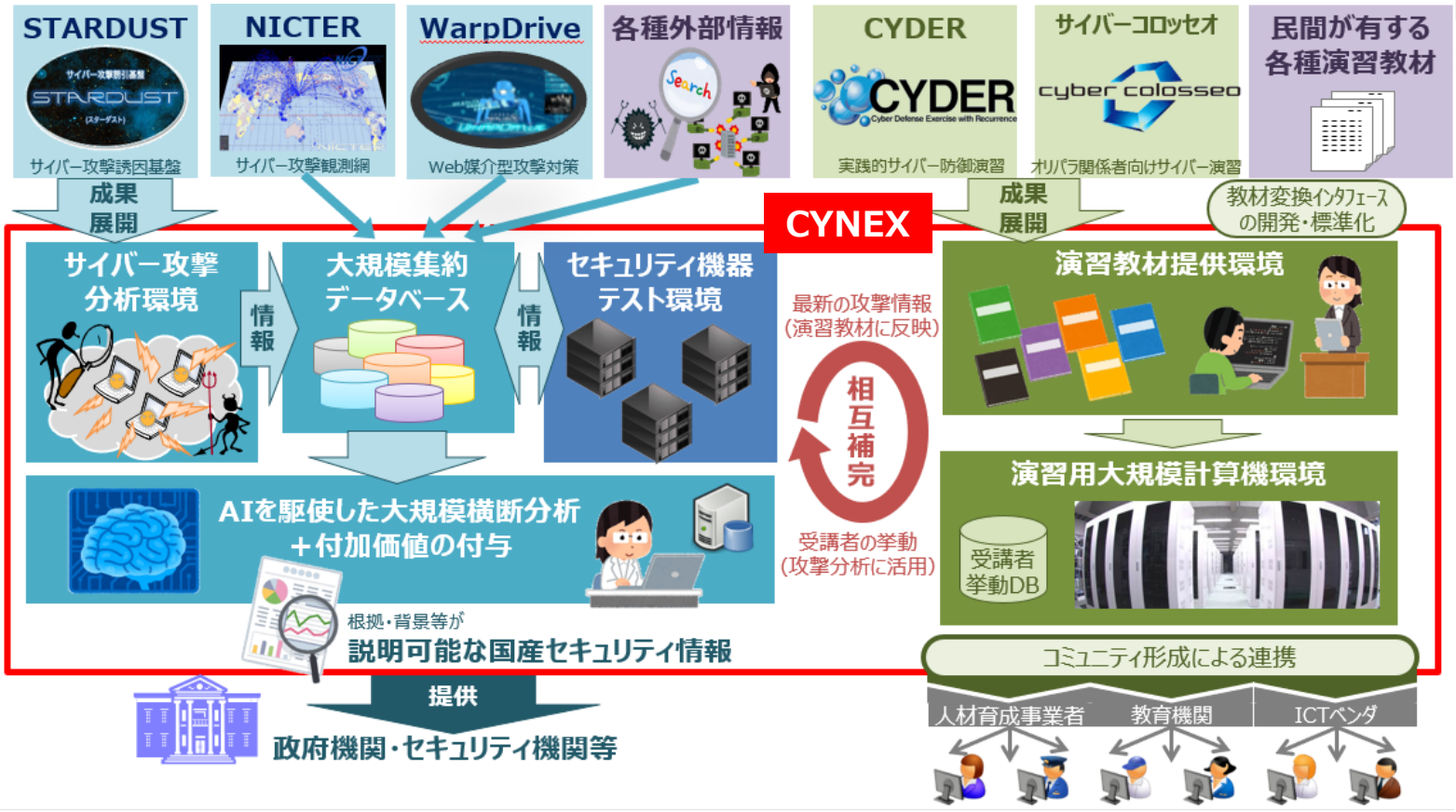
サイバー攻撃に対処可能な万博関連組織の人材育成

万博向け演習プログラムの提供

（2）サイバーセキュリティ統合知的・人材育成基盤の構築

● サイバーセキュリティ情報を国内において収集・蓄積・分析・提供するとともに、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（CYNEX）を国立研究開発法人情報通信研究機構（NICT）に構築し、産学の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力を強化。

令和5年度要求額 8.5億円（令和4年度予算額 7.0億円）



次のとおり活用可能な基盤をNICTに構築。

- **国産セキュリティ情報の収集・蓄積・分析・提供**
  幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。
- **セキュリティ機器テスト環境**
  国産のセキュリティ機器・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。
- **高度解析人材の育成**
  収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。
- **人材育成のための基盤提供**
  NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自立的な人材育成を推進。

（3）KDDI・通信事故の概要

長時間にわたり全国の利用者に影響

影響時間	7月2日（土）1:35　～　7月4日（月）15:00　（61時間25分）
影響エリア	全国
事故の原因	メンテナンス作業におけるルーターの経路誤設定

＜影響数＞

音声（VoLTE）	約2,316 万人
データ（4G/5G）	775万人以上
合計	のべ 3,091万人以上

※影響規模は通常時（通信障害の１週間前の同時間帯）と通信障害時の差分（呼数や位置登録数）をもとに推計し算出

（3）KDDIの通信事故に対する総務省の対応

1. 本年８月３日の行政指導に基づき、**11月10日までに状況の報告、以降、定期的に報告させる**。
2. 同時に、総務省の電気通信事故検証会議において、有識者の専門的視点から原因分析や再発防止策を検証。**他の携帯電話事業者に対して同様の事故を発生させないよう緊急点検を要請**する。
3. 事故検証会議において、**KDDI、沖縄セルラーに対する追加的な再発防止策が提言された場合には、その実施状況についても報告すべきことを、指導文書に明記**。

事故発生（7月2日(土)）

※ 発生状況や事故原因、再発防止策等　について30日以内に報告
※ 報告書を受領した旨報道発表（28日）

重大事故の報告（7月28日(木)）

行政指導（8月3日（水））

電気通信事故検証会議（第1回 8月8日(月)）
※ 以降、計3回程度の開催を想定

検証結果

検証結果も踏まえた再発防止策について
その実施状況を報告させる

検証結果

※ 専門家による事故発生当時の対応や再発防止策の検証を行い、他事業者に共有

他事業者へ緊急点検の要請

行政指導に基づく実施状況の報告
（11月10日までに状況の報告、以降、定期的に報告）

※　このほか、非常時における緊急通報等の事業者間ローミングに関する検討会を本年９月に立ち上げる予定。

（3）NTT西日本・通信事故の概要

１　発生日時
令和４年８月２５日（木）
８時５７分～９時４５分（４８分）（つながらない状態）
９時４５分～１４時４４分（最大４時間５９分）（つながりにくい状態）

２　障害が発生したサービス
ＮＴＴ西日本のインターネットサービス
（フレッツ光ネクスト、フレッツ光ライト、フレッツ光クロス）

３　影響を受けた利用者数
つながらない状態：最大６３万回線
つながりにくい状態：最大２１１万回線

４　影響エリア
つながらない状態：兵庫県、京都府、奈良県、滋賀県、和歌山県、愛知県、
静岡県、岐阜県、三重県、石川県、富山県、福井県
つながりにくい状態：ＮＴＴ西日本全域

５　発生原因
伝送装置（ルータ間を接続する通信設備）の故障、
及び故障復旧に向けた対応に伴う影響