

仕様書

IoT 推進部

1. 件名

サイバーセキュリティに関する最新インシデント調査

2. 目的

2020年東京オリンピック・パラリンピック競技大会を迎える我が国にとって、サイバー攻撃の脅威は切実な問題であり、強固なサイバーセキュリティの確保による世界で最も安心・安全な社会基盤の確立が必達の課題である。

上記課題を解決するため、戦略的イノベーション創造プログラム（SIP）の「重要インフラ等におけるサイバーセキュリティの確保」においては、重要インフラサービスの安定運用を担う制御ネットワークおよび制御ネットワークを構成する制御・通信機器（以下「制御・通信機器」という。）のサイバー攻撃対策として、制御・通信機器のセキュリティ確認技術、制御・通信機器および制御ネットワークの動作監視・解析技術と防御技術を研究開発している。その成果を、東京オリンピック・パラリンピック競技大会をターゲットに、実証実験等を通して、通信・放送、エネルギー、交通などのインフラシステムに適用できることを確認する。また、今後普及・拡大が見込まれるIoTシステムのセキュリティ確保に向けて前記技術を拡張するとともに、技術導入を支援する認証制度の設計、分野を超えた運用のための共通プラットフォームの実現、セキュリティ人材育成に取り組む。

一方、本研究の対象となるサイバー攻撃は日々新しい攻撃方法が考案されている状況であり、本研究の成果を有意な形で早期に実用化・事業化するためには、この分野において日々新しく発生する国内外のインシデントを把握し、他の諸技術とのベンチマークも踏まえて計画に反映していく必要がある。

そこで、本事業ではサイバーセキュリティに係る最新のインシデントを調査・分析し、研究開発並びに社会実装計画に反映する、予測を含めた提言をするものである。

3. 内容

(1) サイバーセキュリティの最新インシデントに関する調査等

最新インシデントの傾向から、研究開発の社会実装に向けた課題を整理し、方向性を適時に見直すために以下の調査・分析等を実施する。

①インシデント調査・分析

2019年3月から2020年2月までに国内外で発生したサイバーセキュリティに係るインシデントの攻撃手法を含む状況に関し、半月程度の期間毎に速報レポートをま

とめる。まとめた結果を、半年程度毎に「SIP／重要インフラ等におけるサイバーセキュリティの確保」の研究開発テーマとの関係性について総合的な知見に基づき分析し、予測を含めた提言として、インシデントレポートとしてまとめる。

インシデントレポートには、「SIP／重要インフラ等におけるサイバーセキュリティの確保」のベンチマークについても言及すること。

インシデントレポートにおけるまとめ方としては、重要インフラ等の制御系に対する攻撃、情報通信系に対する攻撃、その他等の分類を行うこと。

半月毎のインシデントレポートについては速報性を重視し、委託期間中のアップデートは可とする。

②定期的な報告の実施

委託期間中においては少なくとも 6 か月に一度報告会を開催し、調査・分析に基づく予測を含めた提言について報告を行うこと。報告会は NEDO が委託する「重要インフラ等におけるサイバーセキュリティの確保」に係るワーキングで行う場合がある。

③シンポジウム等における調査報告資料の公開

シンポジウム(2019年11～12月に東京、2020年1～2月に東京・大阪を予定)において、インシデントレポートの一部を NEDO 協議の上で来場者へ公開すること。

(2) その他

NEDO からの要請があった場合は、協議の上、可能な限り反映する。

4. 調査期間

NEDO が指定する日から 2020 年 3 月 24 日（火）まで

5. 予算額

2,000 万円以内

6. 報告書

提出期限：調査報告書 2020 年 3 月 24 日（火）

提出部数：電子媒体 CD-R（PDF ファイル形式） 1 枚

提出方法：「成果報告書・中間年報の電子ファイル提出の手引き」に従って提出のこと。

<https://www.nedo.go.jp/itaku-gyomu/manual.html>

7. 報告会等の開催

委託期間中又は委託期間終了後に、成果報告会(公開)における報告を依頼することがある。