3.10.4 ナショナルサイバーオブザベーションセンター

センター長（兼務）　矢野 博之

■概要

NICTは、IoT機器のサイバーセキュリティ対策に貢献するため、国から補助等を受けた場合には、その予算の範囲内で、サイバーセキュリティ戦略（平成30年７月27日閣議決定）等の政府の方針を踏まえ、機構法附則第８条第２項の規定に基づき、機構の有する技術的知見を活用して、パスワード設定等に不備のあるIoT機器の調査及び電気通信事業者への情報提供に関する業務を実施する。

平成30年度は、パスワード設定等に不備のあるIoT機器の調査等に関する業務を行う組織として、ナショナルサイバーオブザベーションセンターを平成31年１月25日に設置するなど実施体制の整備を図るとともに、総務省や関係機関と連携し、適切かつ効果的、効率的な実施に向けた検討を進め、本調査を同年２月20日より開始した。

■主な記事

１．国立研究開発法人情報通信研究機構法の一部改正及び同改正法に基づく実施計画書の認可について

IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化している。平成28年10月には、マルウェア「Mirai」に感染したIoT機器から大規模なDDoS攻撃が行われ、世界各国のサービスへアクセスがしにくくなるという通信障害が発生した。

このようなIoT機器等を悪用したサイバー攻撃の深刻化を踏まえ、NICTの業務に、パスワード設定等に不備のあるIoT機器の調査等を追加（５年間の時限措置）する等を内容とする国立研究開発法人情報通信研究機構法（平成11年法律第162号。以下「法」という。）の改正が行われ、平成30年11月１日に施行された。

法附則第９条に基づく法附則第８条第２項に規定する業務の実施に関する計画（平成31年１月９日に認可申請、以下「実施計画書」という。）は、平成31年１月25日に総務省の情報通信行政・郵政行政審議会（会長：多賀谷 一照 千葉大学名誉教授）に諮問され、同審議会から諮問のとおり認可することが適当とする旨の答申を受け、同日、総務省より認可が行われた。

実施計画書の認可に伴い、NICTは、パスワード設定等に不備のあるIoT機器の調査等に関する業務を行う組織として、ナショナルサイバーオブザベーションセンターを平成31年１月25日に設置した。

本調査業務は、総務省、NICT及びインターネットプロバイダが連携し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」として同年２月１日にプレスリリースが行われ、NICTは２月20日より本調査を開始した。

２．業務の概要

本業務は、NICTにおいて、インターネットに接続された電気通信設備のうち、パスワード設定等に不備のある設備を特定し、電気通信事業者に対して当該設備に係

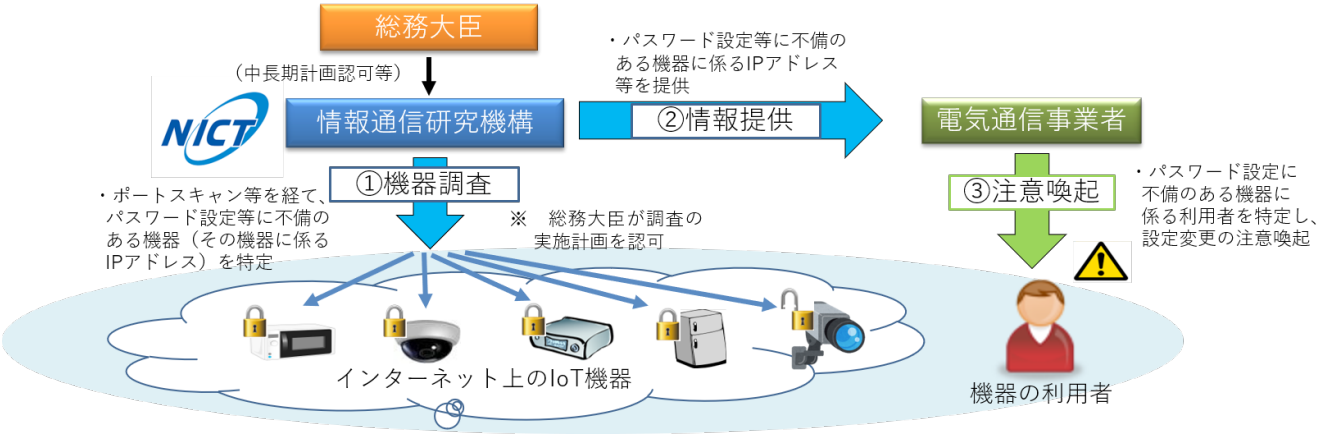

図1　IoT機器調査及び利用者への注意喚起の取組について

るIPアドレス情報等の提供を行うものである（図１）。

具体的には、①特定アクセス行為等による調査、②通信履歴等の電磁的記録の作成、③電気通信事業者への通知を行う。

本業務の概要（図２）及び実施の流れは下記のとおり。

■実施の流れ

１．特定アクセス行為等による調査

（1）ポートスキャン調査

日本国内の約２億のグローバルIPアドレス（IPv４）を対象として、それぞれのIPアドレスに係る機器への接続要求を行い、セッションを確立できるか確認。

（2）特定アクセス行為による調査

ID・パスワードによる認証要求があったものについて、ID・パスワードを入力し、特定アクセス行為を行うことができるかの可否を確認。調査はプログラム及びシステムを開発・構築して実施。

２．通信履歴等の電磁的記録の作成

１．による調査において、特定アクセス行為を行うことができた機器について、当該機器への通信の送信元IPアドレス、送信先IPアドレス、通信日時（タイムスタンプ）等の情報を内容とする通信履歴等の電磁的記録を作成。

３．電気通信事業者への通知

当該通信履歴の送信先IPアドレスに係る電気通信事業者に対して、２．で作成した記録を証拠として、送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を実施。

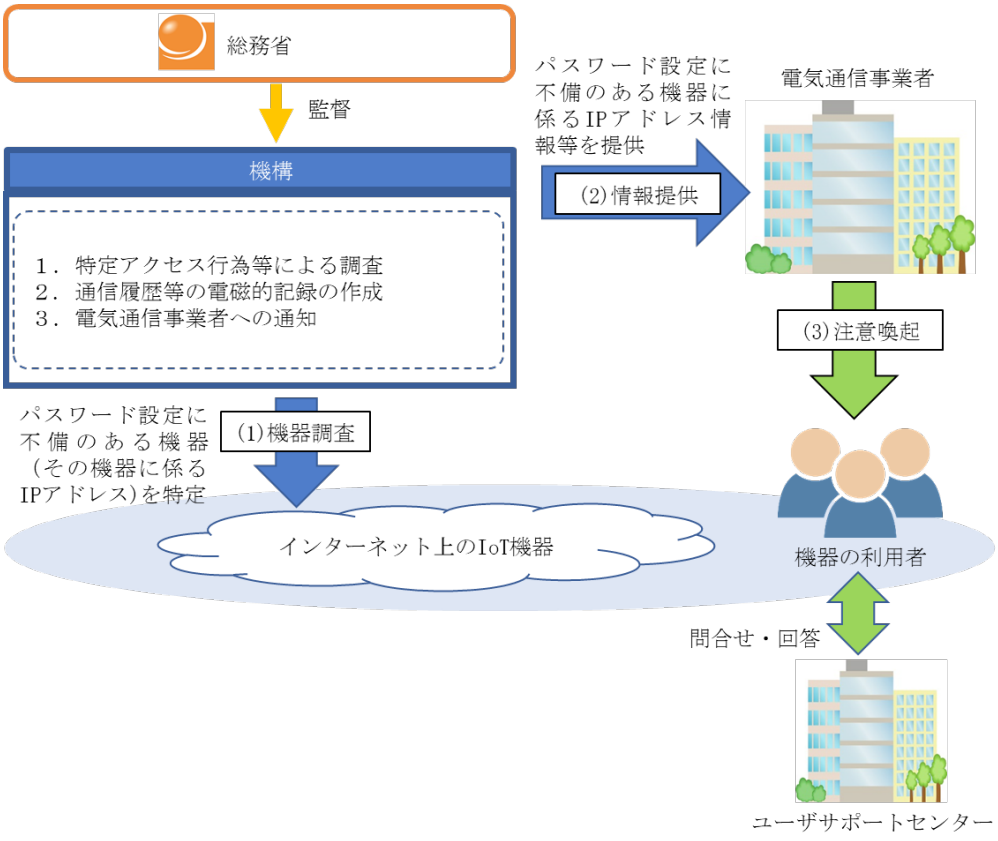

図2　業務の概要