

- IoT機器などを悪用したサイバー攻撃の深刻化を踏まえ、国立研究開発法人情報通信研究機構(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)する等を含む国立研究開発法人情報通信研究機構法の改正を行うもの。

サイバー脅威の深刻化

- 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。

※IoT機器を狙った攻撃は全体の3分の2(2016年)

対策の必要性

- パスワード設定等に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

- NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進(下図)。

情報通信研究機構法の改正

(中長期目標・計画)

意見聴取

総務大臣

サイバーセキュリティ
戦略本部

(中長期目標・計画認可)

情報通信研究機構

- パスワード設定等に不備のある機器に係るIPアドレス等を提供

②情報提供

電気通信事業者

①機器調査

第三者
機関

※ 改正後の電気通信事業法に規定する第三者機関に委託

③注意喚起

- パスワード設定等に不備のある機器に係る利用者を特定し、設定変更の注意喚起

- パスワード設定等に不備のある機器(その機器に係るIPアドレス)を特定

※ 総務大臣が調査の実施計画を認可

インターネット上のIoT機器

機器の利用者

攻撃者



※ 平成30年度予算を活用しつつ、サポート体制整備等を実施予定