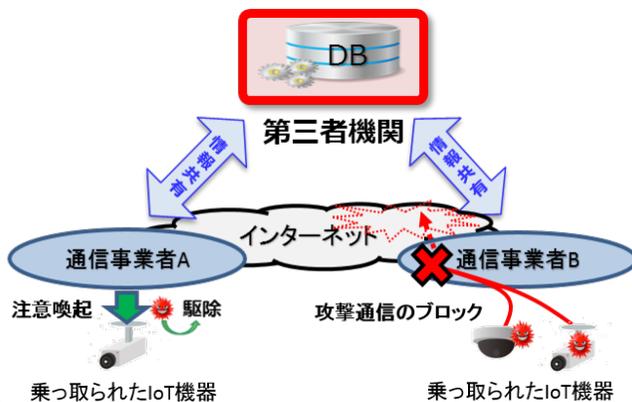


- IoT化に伴うサイバー攻撃の深刻化やネットワークのIP網への移行に対応するため、電気通信事業法の改正を行うもの。

①深刻化するサイバー攻撃への通信事業者の対処の促進

- IoT機器を悪用したサイバー攻撃によるインターネット障害の深刻化
- サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有するための制度を整備し、通信事業者による利用者への注意喚起・攻撃通信のブロック等を促進

第三者機関を通じた情報共有による対処



②電気通信番号に関する制度整備

- モバイル化・IoT化に伴う番号ニーズの増大による番号の逼迫やIP網移行に対応した全ての事業者による番号管理の必要性
- 番号の公平・効率的な使用と電話サービスの円滑な提供のため、使用条件を付して事業者に番号を割り当てるための制度を整備

番号の逼迫状況や効率的な使用

■ 番号の逼迫状況

番号	用途	指定率 (指定数/全番号)	使用率 (使用数/指定数)
070/080/090	携帯電話・PHS	90.4%	70.3%
0120	着信課金	99.2%	55.3%

※ その他、固定電話(OAB-J番号)の市外局番は、全国(582地域)のうち138地域で指定率が80%以上(平均使用率が18.6%)

■ 番号ポータビリティ(電話番号の持ち運び)

固定電話は現在、NTT東西から他事業者への片方向のみ。今後、携帯電話と同様、双方向番号ポータビリティを実現

③電気通信業務等の休廃止に係る利用者保護

- IP網移行や通信設備の更改等を背景として利用者への影響が大きい業務等の終了が予定
- 事業者が業務の休廃止に伴い行う利用者周知について、行政が予め確認するための制度を整備

例：廃止予定のINSサービスの用途



- 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

