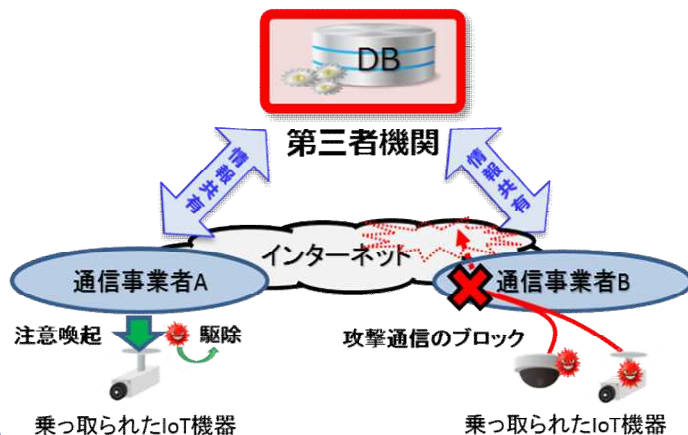


- IoT化に伴うサイバー攻撃の深刻化やネットワークのIP網への移行に対応するため、電気通信事業法の改正を行うもの。

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(0AB-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



- サイバー攻撃を行うマルウェア※感染機器やそれらに指令を出すサーバへの対処を促進するため、**第三者機関**を中心として**通信事業者が必要な情報共有をする**ための制度を整備。

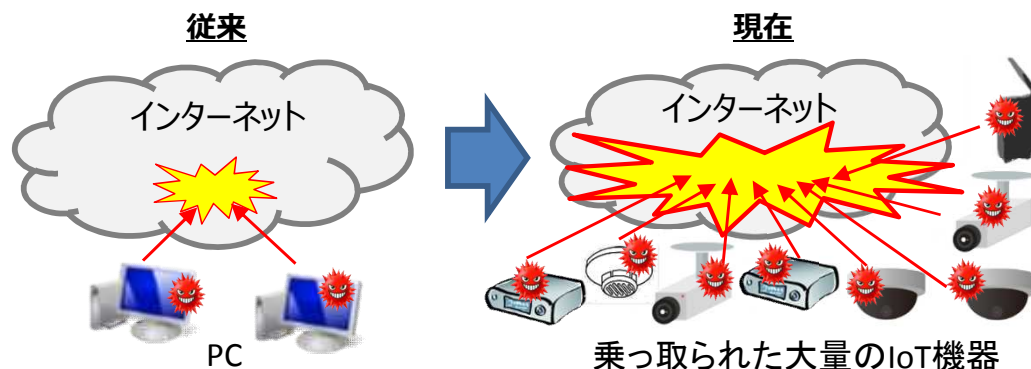
※悪意あるソフトウェアの総称であり、コンピュータに感染することによって、サイバー攻撃などの遠隔操作を自動的に実行するプログラムのこと。

現 状

インターネットの障害の深刻化

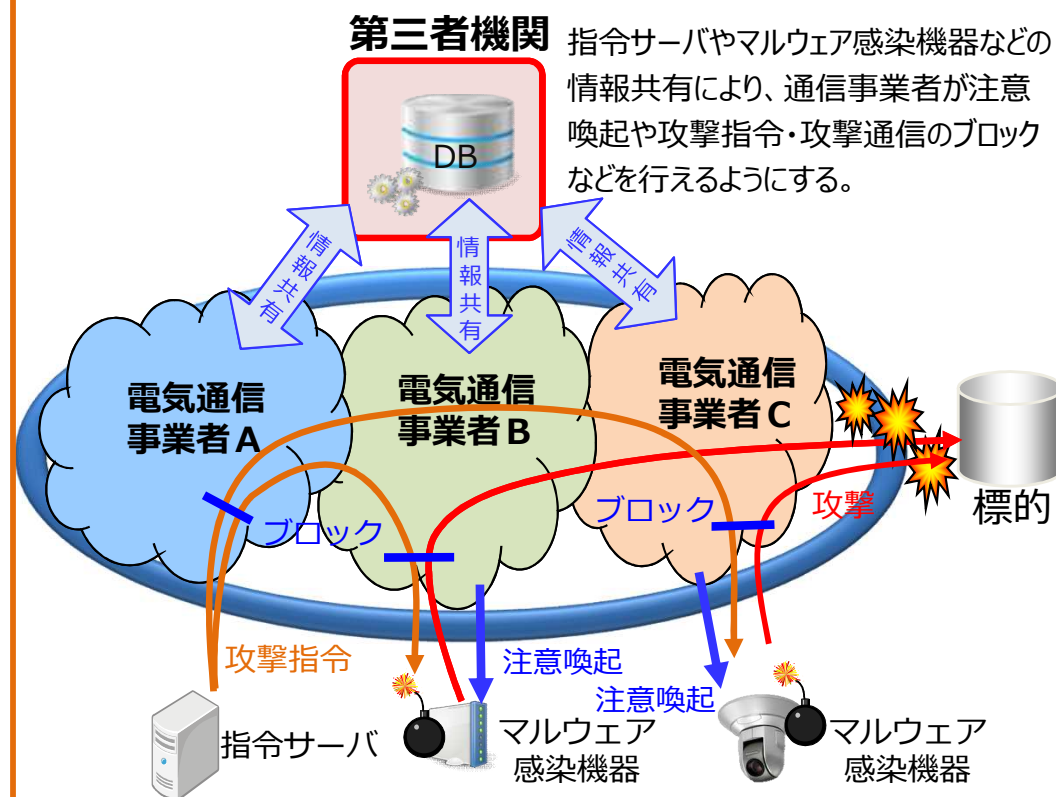
- サイバー攻撃によるインターネットの障害が発生し、国民生活や社会経済活動に影響
- 増加するIoT機器※を悪用したサイバー攻撃によりインターネットに重大な障害が発生
- 2020年の東京オリンピック・パラリンピック競技大会に際して、日本に対する大規模なサイバー攻撃の発生の懸念

※インターネットに接続される家庭用機器や業務用センサーなどの機器



制度整備(イメージ)

第三者機関を中心とした情報共有基盤の構築



- 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

(中長期計画)
意見聴取

サイバーセキュリティ
戦略本部

総務大臣

(中長期計画認可)



情報通信研究機構

①機器調査

- ・パスワード設定に不備のある機器(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

- ・パスワード設定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

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

電気通信事業者

③注意喚起

- ・パスワード設定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



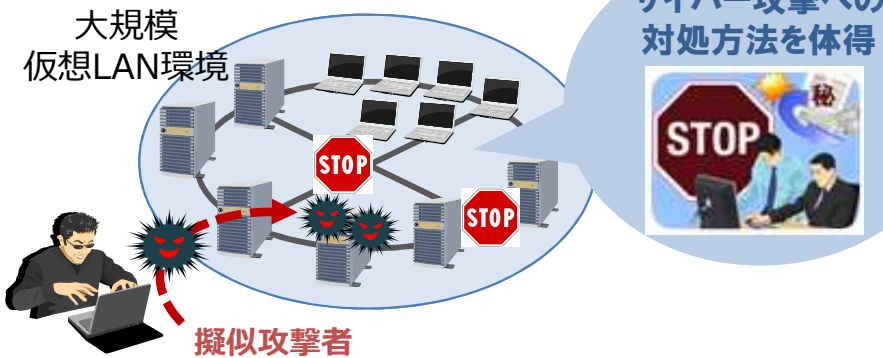
※ 平成30年度予算(案)を活用しつつ、サポート体制整備等を実施予定

インターネット上のIoT機器

機器の利用者

- 総務省は、行政機関等のセキュリティ運用者(情報システム担当者等)を対象とした体験型の実践的なサイバー防御演習(CYDER)を行う情報通信研究機構(NICT)を支援。
- 受講者は、組織の情報システム担当職員として、チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴ってサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験。
- 平成29年度については、全国で100回開催され、計3,009名が受講。

演習のイメージ



CYDER演習風景

- NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用し、行政機関等の実際のネットワークを模した大規模仮想LAN環境を構築。
- NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した最新の演習シナリオを用意。

平成30年度の実施計画

コース	受講対象組織	開催地	開催回数
Aコース(初級)	(全組織共通)	47都道府県	60回
B-1コース(中級)	地方公共団体向け	全国11地域	20回
B-2コース(中級)	国の行政機関等向け	東京	10回
B-3コース(中級)	重要インフラ事業者向け	東京	10回