IA Japan
迷惑メール対策カンファレンス A-9 パネルディスカッション

電気通信事業法およびNICT法今年の改正

（サイバー攻撃情報の共有関係、パスワード設定に不備のあるIoT機器調査関係）

2018年11月8日

一般社団法人日本インターネットプロバイダー協会
（JAIPA）
会長補佐、行政法律部会長 木村

総務省による説明会の開催

- 「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」についての説明会が今年6月～7月に、総務省地方総合通信局において開催されました。
- 本日はその資料の一部も用いて説明します。

- なお、より詳しい説明をInternet Weekで11/29にS9というセッションで行いますので、そちらもご参照ください。（有料プログラムですいません。）

法案国会提出時の概要（１）

電気通信事業法の一部改正案について

1

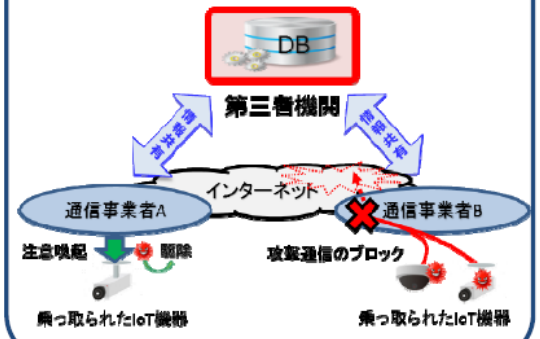
- IoT化に伴うサイバー攻撃の深刻化やネットワークのIP網への移行に対応するため、電気通信事業法の改正を行うもの。

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

法案国会提出時の概要（２）

国立研究開発法人情報通信研究機構法の一部改正案について

2

● 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**）する等を内容とする**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。

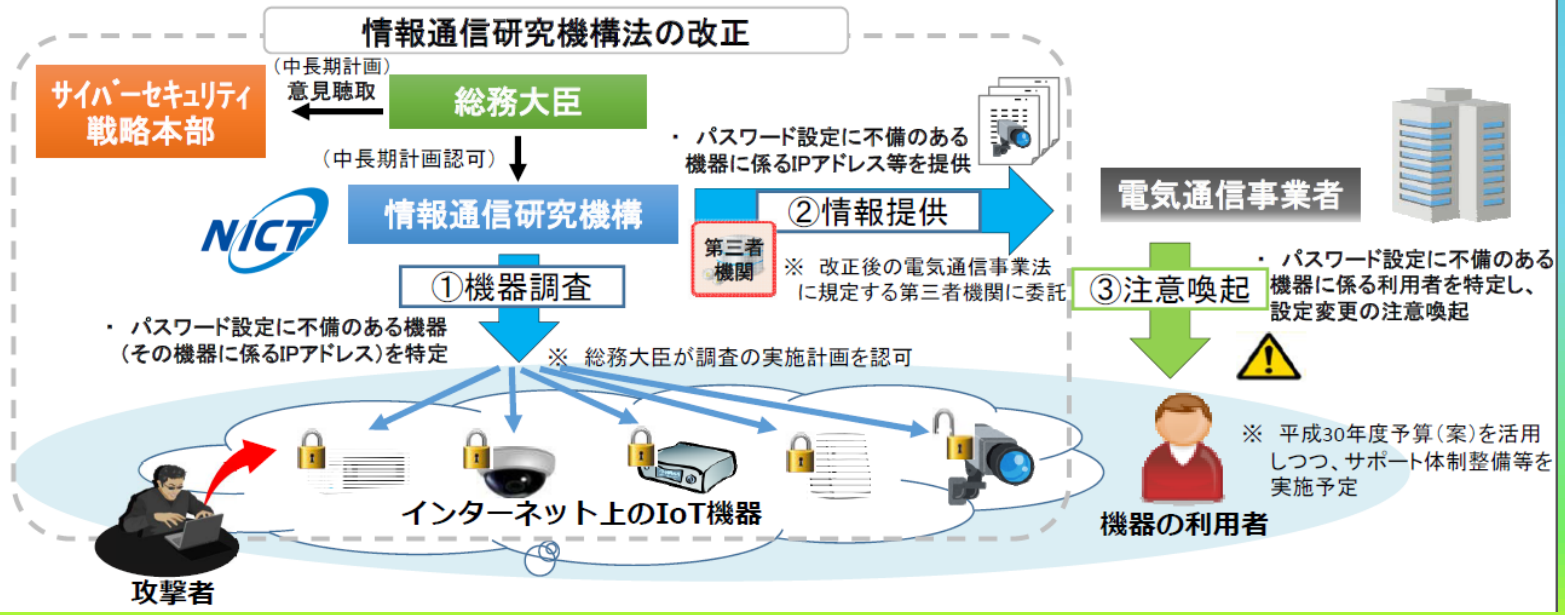
※IoT機器を狙った攻撃は全体の3分の2（2016年）

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）。



サイバー攻撃によるインターネットの障害に関する近年の事例

➢ 近年、国内外において、大規模なサイバー攻撃によりインターネットに障害が生ずる事例が複数発生

国内

2015年12月14日	・一部の電気通信事業者において、DNS サーバがDDoS 攻撃を受け、数時間にわたりDNS サーバへの接続障害が発生
2016年8月29日～9月2日	・一部の電気通信事業者において、権威サーバ（あるドメイン名に対するIPアドレス等の情報を管理しているDNSサーバ）が外部からのDoS攻撃を受け、ホスティングサービスを中心に大きな障害が断続的に発生
2017年9月25日～26日	・一部の電気通信事業者において、レンタルサーバがDoS攻撃を受け、２日間にわたり断続的にサーバに接続できなくなる障害が発生

海外

2016年9月22日	【OVH（フランス）】 ・自社保有サーバに対し、Mirai※に感染したとされる約14万台以上のIoT機器から、最大1.5Tbpsとなる世界最大規模のDDoS攻撃が発生 ・南欧諸国からOVHのサーバを利用するサービスへのアクセスの遅延が発生
2016年10月21日	【Dyn（米国）】 ・Dyn社のDNSサーバに対し、Mirai ※に感染し攻撃に関与した約10万台のIoT機器から1.2Tbpsに及ぶとされるDDoS攻撃が発生 ・世界各国の様々な大手顧客サイト（Twitter、Netflix、Spotify等）に数時間にわたりアクセス障害が断続的に発生
2018年２月28日	【GitHub（米国）】 ・GitHub社のサーバに対し、脆弱なmemcachedサーバを利用して、最大1.35TbpsとされるDDoS攻撃が発生 ・GitHubのウェブサイトへ10分程度にわたりアクセス障害が断続的に発生

※ IoT機器に自動的に感染し、攻撃者からの指示に応じて感染した機器を踏み台としたDDoS攻撃を実施する等の機能を有するマルウェア

過去のオリンピック・パラリンピック時のサイバー攻撃

○　2012年　ロンドン大会

- 大会Webサイト、政府系サイト、その他のサイトに対して、DoS及びDDoS攻撃を確認
- 2億件の悪意のある接続要求をブロック
- 1つのDDoS攻撃につき、1秒あたり11,000件の接続要求を確認

（出典）IPAサイバーセキュリティシンポジウム2014
オリバー・ホーア氏（2012年当時、英国内閣府 上級政策顧問）の講演資料
https://www.ipa.go.jp/about/news/event/securitysympo2014/lecture.html
https://www.ipa.go.jp/files/000039004.pdf

○　2016年　リオデジャネイロ大会

- 開会式の開始前に、オリンピックの公式Webサイトや関連組織に対して540Gbpsに達する大規模なDDoS攻撃が継続的に発生
- IoT機器を踏み台にしたDDoS攻撃を確認

（出典）アーバーネットワークス” DDoS Attacks From IoT Botnets Don’t Have to Mean Game Over”
https://www.arbornetworks.com/blog/asert/ddos-attacks-iot-botnets-dont-mean-game/

IoT機器のセキュリティ上の課題

- IoT機器は、製造業者や利用者が機器のセキュリティ対策を講じる上で制約があり、長期間インターネットに接続されることから、乗っ取られやすく、サイバー攻撃に用いられやすい
- また、IoT機器は数が多く、今後も急増する見込みであるため、乗っ取られる機器数も多くなり、攻撃に用いられるとインターネットの通信に著しい支障が生じるおそれがある

従来のインターネットに接続される機器とIoT機器の特徴の比較

PC等の従来機器	センサーや家電等のIoT機器
● 機器の演算処理能力が比較的高く、アンチウィルスソフトやファイアウォール等のセキュリティソフトの導入による高度な対策が可能	● 機器の演算処理能力が比較的低く、アンチウィルスソフトやファイアウォール等のセキュリティソフトの導入による高度な対策は困難
● 機器のライフサイクルが短く、脆弱性を有する機器も一定期間後にセキュリティ強度の高い新たな機器に置き換わる見込み	● 機器のライフサイクルが長く、10年以上の長期にわたって利用されるものも多いため、脆弱性を有したままネットワークに接続され続けるおそれ
● 画面等を通じた、人的管理が容易	● 画面等がないものが多く、人的管理が困難
● ネットワークに接続される機器数は多いが、IoT機器と比べ今後の増加数は少ない見込み※ ※ PCは、2015年の約20億個をピークに微減傾向となる見込み。（IHS Technology調べ）	● ネットワークに接続される機器数が膨大であり、今後も急増する見込み※ ※ 家庭、医療、産業用等で用いられるIoT機器は2020年に約200億個となる見込み。（IHS Technology調べ）

円滑なインターネット利用環境の確保に関する検討会について

1. 趣旨

近年、増加するIoT機器を悪用したサイバー攻撃等によるインターネット障害が発生している。更に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が懸念される。このため、電気通信事業においてインターネットの障害を防ぐための方策について検討を行う。

2. 検討事項

（１）電気通信事業者によるサイバー攻撃等によるインターネットの障害の防止措置
（２）電気通信事業者等によるインターネットの障害に関する情報共有の在り方
（３）IoT機器を含む脆弱な端末設備への対策　　等

3. 構成員

（敬称略、五十音順）

	遠藤　信博	日本電気株式会社　代表取締役会長
（座長代理）	佐伯　仁志	東京大学大学院法学政治学研究科　教授
（座長）	佐々木良一	東京電機大学未来科学部　教授
	宍戸　常寿	東京大学大学院法学政治学研究科　教授
	長田　三紀	全国地域婦人団体連絡協議会　事務局長
	藤本　正代	富士ゼロックス（株）パートナー、情報セキュリティ大学院大学　客員教授
	森　　亮二	英知法律事務所　弁護士
	吉岡　克成	横浜国立大学大学院環境情報研究院／先端科学高等研究院　准教授

⇩

「対応の方向性」を公表（平成30年2月20日）

「対応の方向性」の概要等

1. 電気通信事業者による攻撃通信の発生の防止

・マルウェア感染の疑われる利用者に対する注意喚起、指令サーバとの通信遮断、未知のマルウェア感染端末等を検知。

※事業者が、利用者の同意なく、注意喚起、検知等のために利用者の通信に係るIPアドレスやタイムスタンプ等を利用することは、通信の秘密の窃用に該当し得る。

→ 通信の秘密に配慮した実施方法等を整理し、民間のガイドラインに反映。

2. 情報共有、分析基盤の構築

・1. の対策の実効性を高めるため、第三者機関が指令サーバ等に関する情報を集約し、分析・検証した上で電気通信事業者との間で情報共有。

※本取組においては、第三者機関が、通信の秘密を集約、分析・検証、共有することとなる。

→ 第三者機関が通信の秘密に該当する情報を扱うことから、裏付けとなる法制度を整備。

3. IoT機器を含む脆弱な端末設備への対策の検討

・DDoS攻撃等の発生源となりうる脆弱なIoT機器について、基本的なセキュリティ対策を実施。

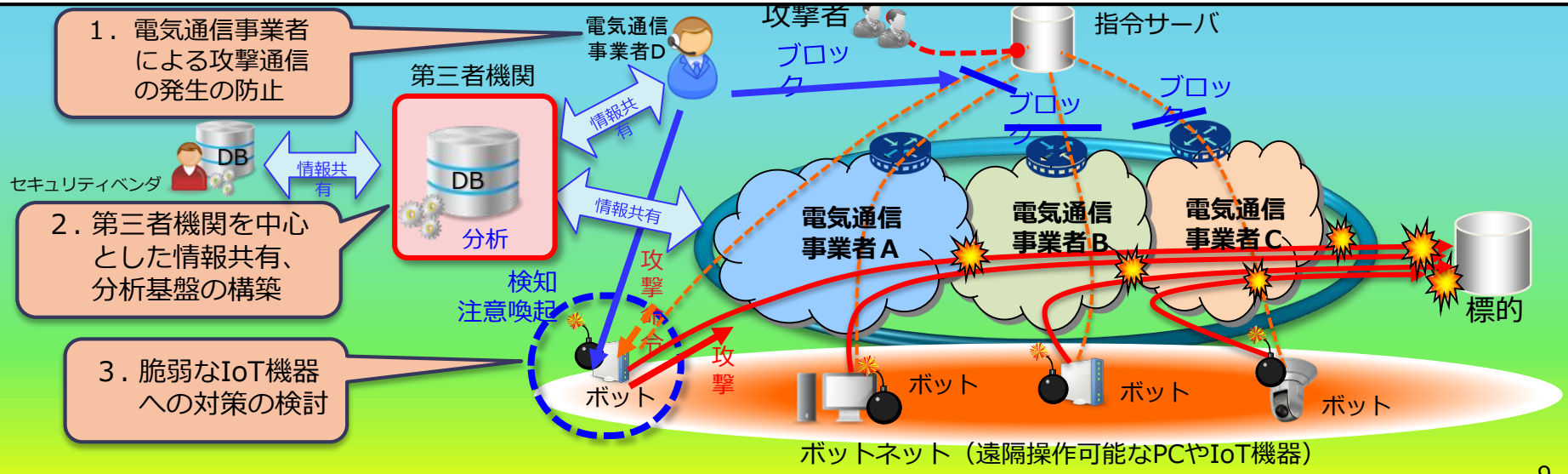
※事業者のネットワークに接続される端末設備の技術基準には、現時点ではサイバー攻撃等によるインターネットの障害に関する規定はない。

→ ネットワークの安全・信頼性を確保するための端末のセキュリティ対策について、国際動向等を踏まえ、情報通信審議会で検討。

4. 昨年8月に発生した大規模なインターネット障害の検証を踏まえた対策の検討

・事業者においてインターネットの経路情報を適切に制御する技術的対策を実施するともに、事業者間でインターネット障害に関する情報を共有。

→ 情報通信ネットワーク安全・信頼性基準（ガイドライン）の改訂や、事業者から総務省へのインターネット障害の報告の在り方について検討。



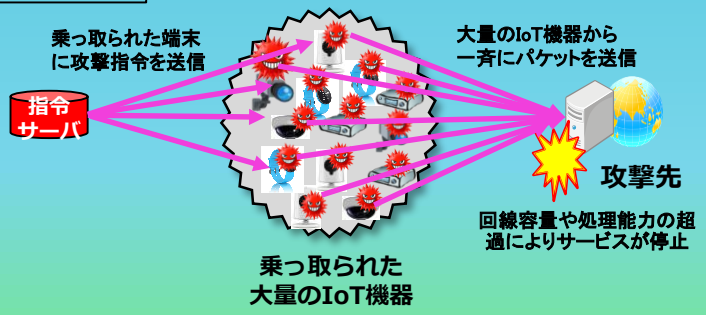
送信型対電気通信設備サイバー攻撃の範囲

送信型対電気通信設備サイバー攻撃

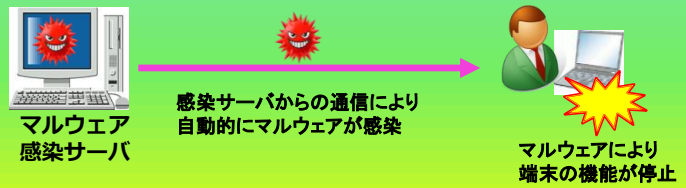
- 「送信型対電気通信設備サイバー攻撃」とは、以下を満たすものをいう。
  - ① **サイバー攻撃**（通常の通信によるトラフィック集中等は含まない。）**のうち、**
  - ② **電気通信設備**（電気通信事業者の電気通信設備及び利用者の端末）**を攻撃の対象とし、**
  - ③ **その機能に障害を与える通信の送信により行われるもの**（受信者の行為が介在することにより障害が発生する場合は該当しない）
- また、上記の通信の送信を行う指令を与える通信の送信（C&Cサーバからの攻撃指令等）も含まれる。

該当する例

例①：DDoS攻撃



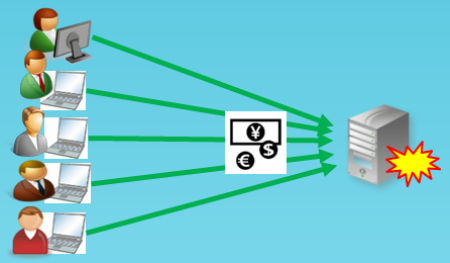
例②：マルウェア感染による機能障害



該当しない例

例①：販売サイトへのアクセス等
によるトラフィック集中

サイバー攻撃には該当しないため、
該当しない

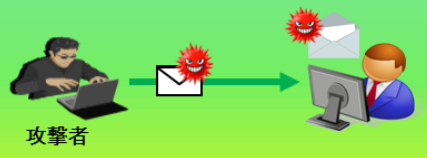


例②：不正アクセス

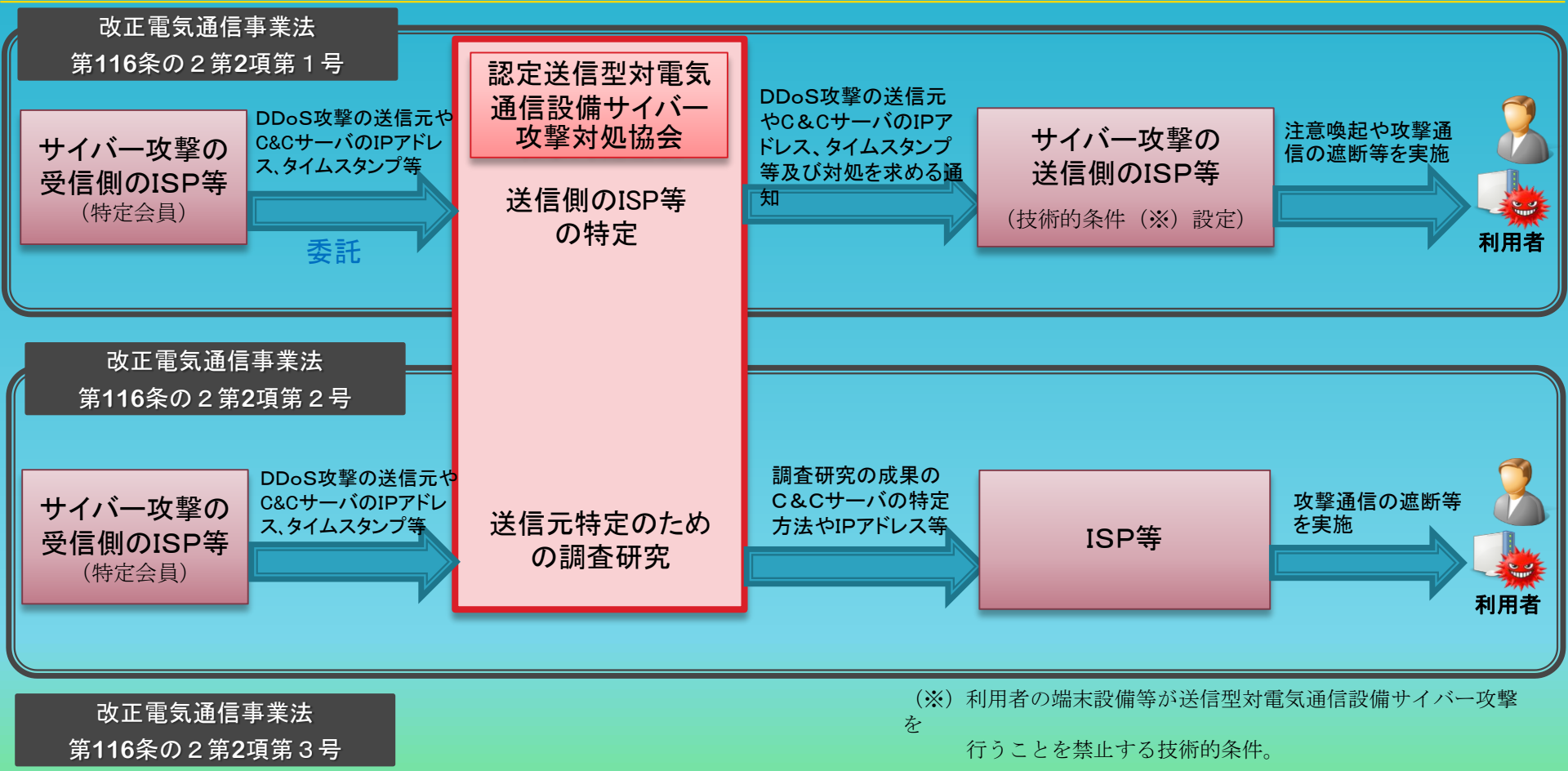
電気通信設備の機能に障害を与えな
いため、該当しない

例③：標的型メール

受信者の行為が介在することにより
障害が発生するため、該当しない



認定送信型対電気通信設備サイバー攻撃対処協会の業務



（※）利用者の端末設備等が送信型対電気通信設備サイバー攻撃を
行うことを禁止する技術的条件。

- 送信型対電気通信設備サイバー攻撃に対処する電気通信事業者を支援。

その他の業務

- NICTから委託を受けて、パスワード設定に不備のある機器に係るIPアドレス、タイムスタンプ等を当該機器利用者のISPに通知（改正NICT法附則第8条第2項のNICTの業務の受託）。

国立研究開発法人情報通信研究機構によるIoT機器調査に係る制度の概要

- 本年５月23日に公布された改正国立研究開発法人情報通信研究機構法において、国立研究開発法人情報通信研究機構（NICT）に、平成35年度までの時限措置として以下の業務を追加（改正国立研究開発法人情報通信研究機構法は本年11月頃に施行を予定）。

（ア）インターネット上で外部からアクセス可能であり、かつパスワード設定等に不備のある電気通信設備を特定するための調査を行うこと

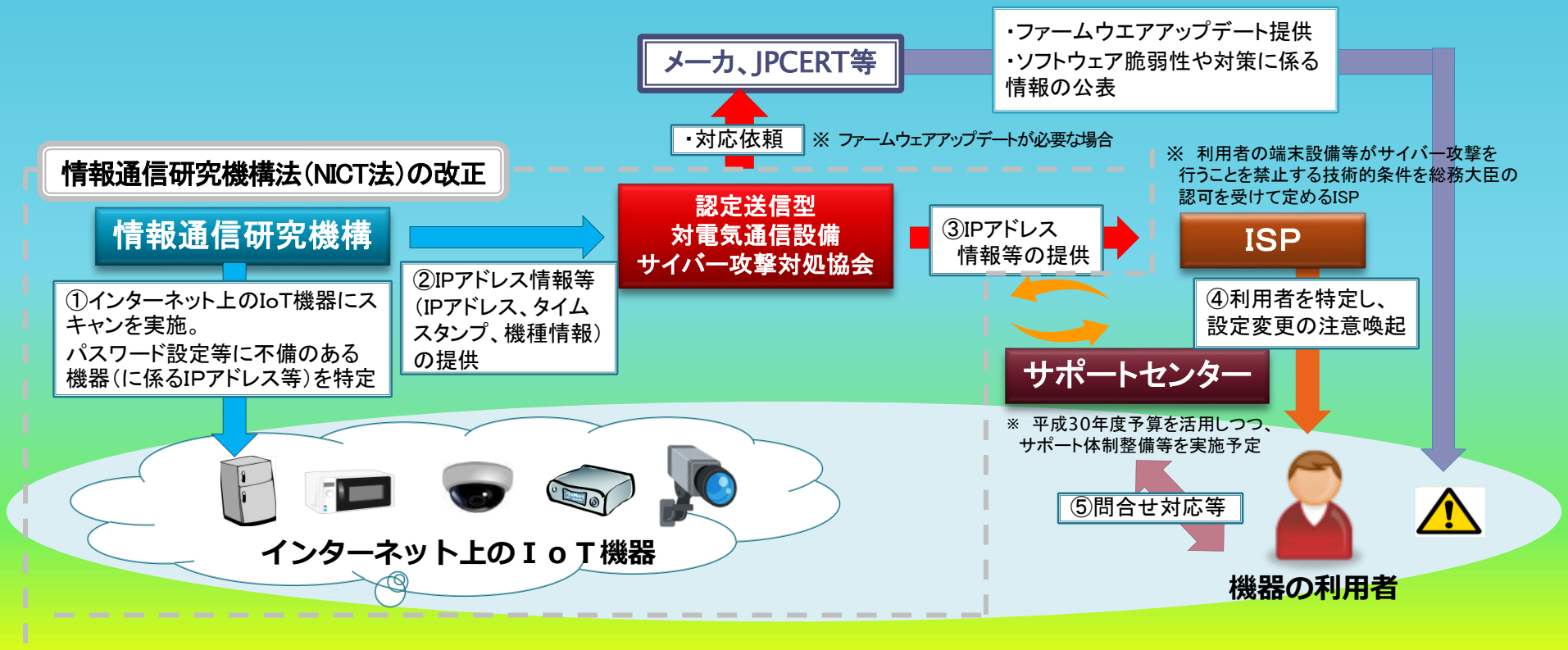
※　NICTは、総務省令で定める基準（電気通信事業者が技術的条件で定める基準を勘案し、不正アクセス行為から防御するため必要な基準）を満たさないID・パスワードを機器に入力。

（イ）パスワード設定等に不備のある電気通信設備のIPアドレス・タイムスタンプ等の情報を、該当する電気通信事業者に対して提供し、対処（注意喚起等）を求める通知を行うこと

※　認定送信型対電気通信設備サイバー攻撃対処協会に委託することができる。

- （上記（イ）の通知を受けた電気通信事業者は、IPアドレス情報等をもとに利用者を特定し、当該利用者に対して注意喚起を行う。）

※　総務省予算を活用して利用者からの個別の問合せ対応を行うなど、電気通信事業者における注意喚起のサポート体制を整備予定。



ユーザへの注意喚起イメージ

注意喚起

機器の利用者

問合せ対応

ISP

（1）NICTから提供されたIPアドレス、タイムスタンプと通信履歴を照合し、**利用者を特定**

（2）特定した利用者にメールにて**注意喚起**

【注意喚起のメール案】

…

このたび、お客様がご利用の〇〇サービスに接続されたIoT機器について、脆弱と思われるID・パスワードが設定された状態で運用されていることを確認しました。つきましては、ID・パスワード変更を実施して頂きますようお願いいたします。

確認日：※年※月※日
IoT機器：△△

◆ IoTセキュリティ対策サイト
http://www.〇〇〇.co.jp

◆ IoT機器△△の設定変更方法
http://www.×××.co.jp

■お問い合わせ■
※※※※
電話番号：※※
メールアドレス：※※
受付時間：※※～※※

サポートセンター

※　平成30年度予算を活用しつつ、サポート体制を整備予定

（1）設定変更案内の作成

（2）問合せ対応

※ NICTの調査を受けた注意喚起は、平成35年度までを想定

NICTから事前調査の発表　11月7日

ENGLISH TOP　アクセス　お問い合わせ　Google カスタム検索

NICT 国立研究開発法人 情報通信研究機構

NICTについて　研究紹介　研究成果　オープン イノベーション　公募・調達　広報・出版　採用情報

Home 〉 お知らせ&イベント 〉 お知らせ 〉 日本国内でインターネットに接続されたIoT機器等に関する事前調査の実施について

印刷

日本国内でインターネットに接続されたIoT機器等に関する事前調査の実施について

2018年11月7日

国立研究開発法人情報通信研究機構

ツイート　いいね！ 183

国立研究開発法人情報通信研究機構（NICT）は、パスワード設定等に不備のあるIoT機器の調査等をNICTの業務に追加（５年間の時限措置）する「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が今月1日に施行されたことを受け、同調査等の業務の実施（今年度内に開始予定）に向けた検討、準備を進めてまいります。

今後の具体的な検討にあたっては、日本国内でインターネットに接続されたIoT機器等につき、当該接続状況などの全体的な傾向、概数等を把握する必要があることから、ポート開放状況の把握など、現状に関して、事前の準備のための調査を実施することといたします。

○事前調査の概要

・日本国内のIPv4アドレスを対象に、22/TCP(SSH)、23/TCP(Telnet)、80/TCP(HTTP)などの

https://www.nict.go.jp/about/location.html

お知らせ

2018年
2017年
2016年
2015年
2014年
2013年
2012年
2011年
2009年

省令でパスワードの基準が決まる。

総務省　10月19日公表

電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律の施行に伴う国立研究開発法人情報通信研究機構法附則第八条第四項第一号に規定する総務省令で定める基準及び第九条に規定する業務の実施に関する計画に関する省令案に係る意見募集の結果及び情報通信行政・郵政行政審議会からの答申

識別符号（ID・パスワード）の基準に関する規定について

2

改正法の概要

○ NICTが特定アクセス行為において入力する識別符号（ID・パスワード）は、「不正アクセス行為から防御するため必要な基準として**総務省令で定める基準**を満たさないものに限る」とされている。（改正法附則第８条第４項第１号）

※ 当該基準は電気通信事業者が総務大臣の認可を受けた技術的条件を勘案して定めるとされている。

省令案の概要

○ 総務省令で定める基準として、以下の①及び②のいずれにも該当する暗証符号（パスワード）を規定。（省令案第１条）

① ８文字以上であること。

② これまで送信型対電気通信設備サイバー攻撃※のために用いられたもの、同一の文字のみ又は連続した文字のみを用いたものその他の容易に推測されるもの以外のものであること。

※「送信型対電気通信設備サイバー攻撃」とは、以下を満たすものをいう。（改正電気通信事業法第116条の２第１項第１号）

① サイバー攻撃（通常の通信によるトラフィック集中等は含まない。）のうち、② 電気通信設備（電気通信事業者の電気通信設備及び利用者の端末）を攻撃の対象とし、③ その機能に障害を与える通信の送信により行われるもの（受信者の行為が介在することにより障害が発生する場合は該当しない）

【該当するパスワードの例】

これまで送信型対電気通信設備サイバー攻撃のために用いられたもの	同一の文字のみ又は連続した文字のみを用いたもの
password 、admin1234 、supervisor、smcadmin	aaaaaaaa、11111111、abcdefgh、12345678

○ 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）
附　則
（業務の特例）
第八条
4
一　特定アクセス行為　機構の端末設備又は自営電気通信設備を送信元とし、アクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先とする電気通信の送信を行う行為であって、当該アクセス制御機能を有する特定電子計算機である電気通信設備に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号（当該識別符号について電気通信事業法第五十二条第一項又は第七十条第一項第一号の規定により認可を受けた技術的条件において定めている基準を勘案して**不正アクセス行為から防御するため必要な基準として総務省令で定める基準を満たさないものに限る**。）を入力して当該電気通信設備を作動させ、当該アクセス制御機能により制限されている当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備の特定利用をし得る状態にさせる行為をいう。

これに基づき、ISPも同内容の「技術的条件」を定め、利用者に適用

通信の秘密の整理

- インターネットの安定的な運用に関する協議会
- **「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」**を策定
- 2006年から活動
- 構成団体は
  - 一般社団法人日本インターネットプロバイダー協会（JAIPA)
  - 一般社団法人電気通信事業者協会（TCA)
  - 一般社団法人テレコムサービス協会
  - 一般社団法人日本ケーブルテレビ連盟
  - 一般社団法人ICT-ISAC

ガイドラインはJAIPAのホームページで公開
https://www.jaipa.or.jp/other/intuse/

いわゆる「通信の秘密」ガイドラインの変遷

- 2007年　初版
  「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン 」として作成。関係者限りで限定公開
- 2011年　第2版　　一般にも公開
- 2014年　第3版
  電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会の第一次とりまとめ（2014年4月）を受けて改正
- 2015年　第4版
  同研究会の第二次とりまとめ（2015年9月公表）を受けて改正
- 2018年　第5版（予定）　同研究会の第三次とりまとめ（2018年9月公表）を受けて改正

第4版において、ガイドラインの名称が「大量通信等への対処」から「サイバー攻撃等への対処」に変更。

民間版「通信の秘密」ガイドラインの位置付け

- 業界の自主基準としての位置づけ
  - 法令上の位置づけがあるガイドラインではなく民間における法令の解釈指針
  - 事業者に対処を強制したり、活動を規制するものではない
  - 総務省はオブザーバとして協議会に参加
- 同様な事例が生じた際に、ISPがその都度解釈に関して総務省に問合せる手間を省略するためのもの
  - ガイドラインに沿って対応すれば免責されるなどの効果はないが、裁判所が法的判断の参考として参照することを期待
- インターネット上で新たに発生する問題に対応するため、定期的な見直しを実施