IoTの普及に対応した電気通信設備の技術基準等に関する制度整備

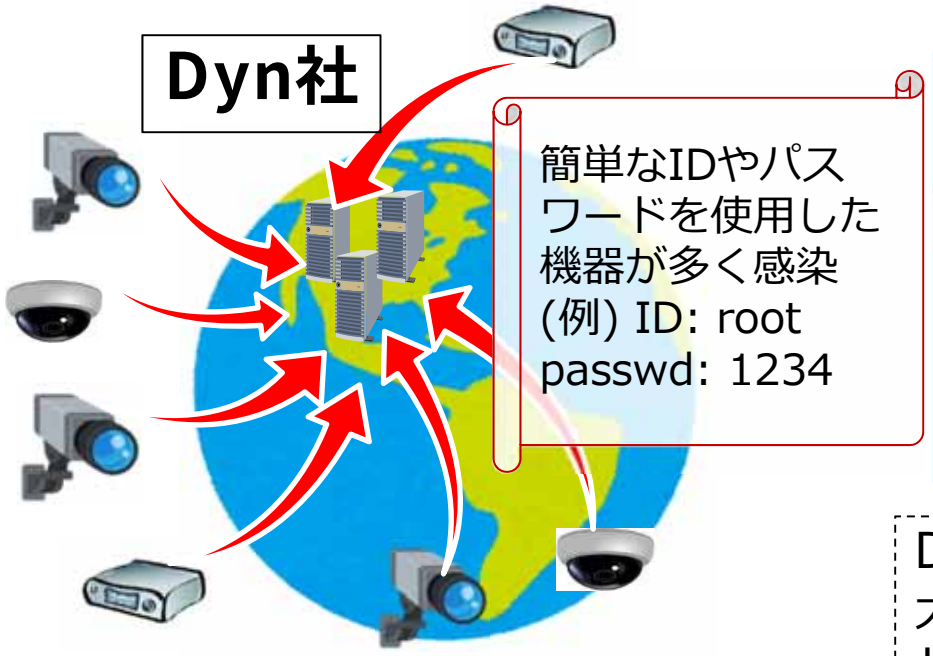
令和元（2019）年10月17日

総務省総合通信基盤局電気通信事業部
電気通信技術システム課
石原　浩樹

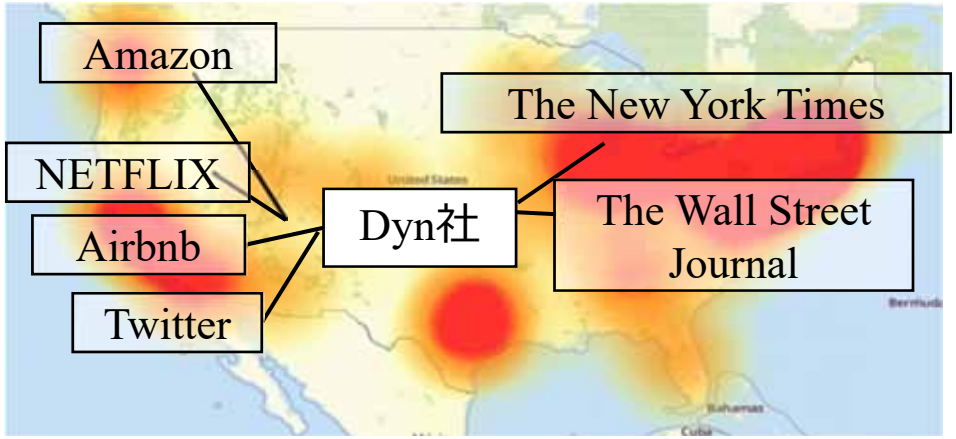
はじめに

IoT機器を踏み台とした大規模DDoS攻撃

- 2016年10月21日、米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が２回発生。その結果、多数の企業のサービスにアクセスしにくくなる等の障害が発生。
- 「Mirai」というマルウェアに感染した10万台を超えるIoT機器から、大量の通信（最大1.2Tbps)が発生したことが原因。



システムダウンの状況



Dyn社のDNSサービスを使用した数多くの大手インターネットサービスやニュースサイトに影響。

情報セキュリティの10大脅威（組織）

	2016年	2017年	2018年	2019年
1位	標的型攻撃による情報流出	標的型攻撃による情報流出	標的型攻撃による被害	標的型攻撃による被害
2位	内部不正による情報漏えいとそれに伴う業務停止	ランサムウェアによる被害	ランサムウェアによる被害	ビジネスメール詐欺による被害
3位	ウェブサービスからの個人情報の窃取	ウェブサービスからの個人情報の窃取	ビジネスメール詐欺による被害	ランサムウェアによる被害
4位	サービス妨害攻撃によるサービスの停止	サービス妨害攻撃によるサービスの停止	脆弱性対策情報の公開に伴う悪用増加	サプライチェーンの弱点を悪用した攻撃の高まり
5位	ウェブサイトの改ざん	内部不正による情報漏洩とそれに伴う業務停止	脅威に対応するためのセキュリティ人材の不足	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ウェブサイトの改ざん	ウェブサービスからの個人情報の窃取	サービス妨害攻撃によるサービスの停止
7位	ランサムウェアを使った詐欺・恐喝	ウェブサービスへの不正ログイン	**IoT機器の脆弱性の顕在化**	インターネットサービスからの個人情報の窃取
8位	インターネットバンキングやクレジットカード情報の不正利用	**IoT機器の脆弱性の顕在化**	内部不正による情報漏洩	**IoT機器の脆弱性の顕在化**
9位	ウェブサービスへの不正ログイン	攻撃のビジネス化（アンダーグラウンドサービス）	サービス妨害攻撃によるサービスの停止	脆弱性対策情報の公開に伴う悪用増加
10位	過失による情報漏えい	インターネットバンキングやクレジットカード情報の不正利用	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい

情報処理推進機構（IPA）ホームページ（https://www.ipa.go.jp/security/vuln/index.html）より引用し作成

情報セキュリティの10大脅威（個人）

	2016年	2017年	2018年	2019年
1位	インターネットバンキングやクレジットカード情報の不正利用	インターネットバンキングやクレジットカード情報等の不正利用	インターネットバンキングやクレジットカード情報等の不正利用	クレジットカード情報の不正利用
2位	ランサムウェアを使った詐欺・恐喝	ランサムウェアによる被害	ランサムウェアによる被害	フィッシングによる個人情報等の詐取
3位	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ	スマートフォンやスマートフォンアプリを狙った攻撃	ネット上の誹謗・中傷	不正アプリによるスマートフォン利用者への被害
4位	巧妙・悪質化するワンクリック請求	ウェブサービスへの不正ログイン	スマートフォンやスマートフォンアプリを狙った攻撃	メール等を使った脅迫・詐欺の手口による金銭要求
5位	ウェブサービスへの不正ログイン	ワンクリック請求等の不当請求	ウェブサービスへの不正ログイン	ネット上の誹謗・中傷・デマ
6位	匿名によるネット上の誹謗・中傷	ウェブサービスからの個人情報の窃取	ウェブサービスからの個人情報の窃取	偽警告によるインターネット詐欺
7位	ウェブサービスからの個人情報の窃取	ネット上の誹謗・中傷	情報モラル欠如に伴う犯罪の低年齢化	インターネットバンキングの不正利用
8位	情報モラル不足に伴う犯罪の低年齢化	情報モラル欠如に伴う犯罪の低年齢化	ワンクリック請求等の不当請求	インターネットサービスへの不正ログイン
9位	職業倫理欠如による不適切な情報公開	インターネット上のサービスを悪用した攻撃	**IoT機器の不適切な管理**	ランサムウェアによる被害
10位	インターネットの広告機能を悪用した攻撃	**IoT機器の不適切な管理**	偽警告によるインターネット詐欺	**IoT 機器の不適切な管理**

情報処理推進機構（IPA）ホームページ（https://www.ipa.go.jp/security/vuln/index.html）より引用し作成

情報通信審議会における検討

IoTの普及に対応した電気通信設備に係る技術的条件の検討

検討の背景

○　近年、インターネットから操作可能な家電やスマートメーターの利用等、**IoTサービスが広く社会に普及**しつつあり、国民生活や企業の社会経済活動に対する影響力は、より一層大きくなっていくものと思料。

○　IoTサービスの普及に伴い、通信ネットワークについても**設備構成の複雑化や利用形態の多様化が急速に進展**。

○　このような中、今後導入される様々な**IoTサービスを安心して安定的に利用できるネットワーク環境を確保する**ことを目的として、現行の電気通信設備の技術基準や関連制度について検証を行い、**IoTの普及に伴うネットワークの高度化や利用形態の多様化を踏まえた電気通信設備に係る技術的条件**について検討。

検討事項

「ネットワークのIP化に対応した電気通信設備に係る技術的条件」のうち「IoTの普及に対応した電気通信設備に係る技術的条件」について

検討体制

IPネットワーク設備委員会（主査：相田 仁 東京大学大学院工学系研究科教授）において検討

IoTの普及に対応した電気通信設備に関する検討課題

１．IoTに対応した電気通信設備の技術的条件

① LPWAサービス用電気通信設備の技術基準の適用

クラウド上の通信機能を活用してLPWAサービスを提供する場合の技術基準の適用の考え方等を整理

② IoT機器を含む端末設備のセキュリティ対策

DDoS攻撃の原因となるIoT機器がマルウェアに大量感染する事態を防止すること等を目的として、IoT機器を含む端末設備の接続の技術基準に**最低限のセキュリティ対策を追加**することについて検討

２．IoT時代における重大事故に関する事故報告等の在り方

① LPWAサービスの事故報告基準

LPWAサービスの通信頻度等を考慮し、LPWAサービスに係る事故報告基準(影響利用者数及び継続時間)について検討

② 大規模なインターネット障害発生時の対策

大規模障害発生時の情報共有を効果的に実施するため、電気通信事業者と総務省との情報共有の在り方を整理するとともに、事業者における技術的対策についても検討

IoT機器を含む端末設備のセキュリティ対策

端末設備の接続の技術基準に追加すべきセキュリティ対策の内容

- 次の条件を満たす端末設備に対して①～③の機能が必要。
- ただし、PCやスマートフォン等については、当該セキュリティ要件の規定の対象外とするが、利用者においてアンチウィルスソフトを導入する等の適切な対策を行うことが求められる。

条　件

・ インターネットプロトコル（IP）を使用する端末設備

・ 電気通信回線設備を介して接続することにより当該設備に備えられた電気通信の送受信に係る機能を操作可能なもの

必要な機能

① アクセス制御機能

② アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能

③ ファームウェアの更新機能（又はそれらと同等以上の機能）

平成30年9月20日に一部答申

端末設備等規則への反映

端末設備等規則への反映

- 情報通信審議会からの答申後、本年1月に情報通信行政・郵政行政審議会に諮問　→　答申
- 情報通信行政・郵政行政審議会の答申を受け、端末設備等規則を改正

端末設備等規則第34条の10として追加

（インターネットプロトコルを使用する専用通信回線設備等端末）

第三十四条の十　専用通信回線設備等端末（デジタルデータ伝送用設備に接続されるものに限る。以下この条において同じ。）であつて、 デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもののうち、電気通信回線設備を介して接続する ことにより当該専用通信回線設備等端末に備えられた電気通信の機能（送受信に係るものに限る。以下この条において同じ。）に係る設定を変更できるものは、次の各号の条件に適合するもの又はこれと同等以上のものでなければならない。ただし、次の各号の条件に係る 機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末については、この限りでない。

一　当該専用通信回線設備等端末に備えられた電気通信の機能に係る設定を変更するためのアクセス制御機能（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有すること。

二　前号のアクセス制御機能に係る識別符号（不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。）であつて、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの（二以上の符号の組合せによる場 合は、少なくとも一の符号に係るもの。）の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用 通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること。

三　当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること。

四　当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること。

電気通信事業法に基づく端末機器の基準認証に関するガイドライン

- **策定の目的**

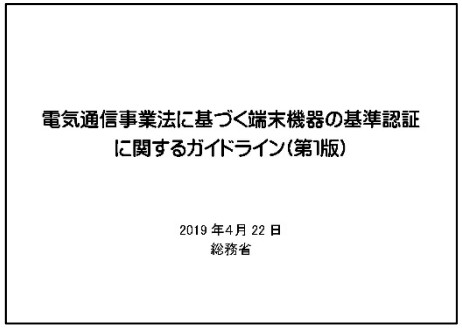
端末設備等規則の規定等に係る端末機器の基準認証に関する運用について明確化を図る

- **主な内容**
  - 第1章：IoT機器のセキュリティ基準関連（端末設備等規則第34条の10）

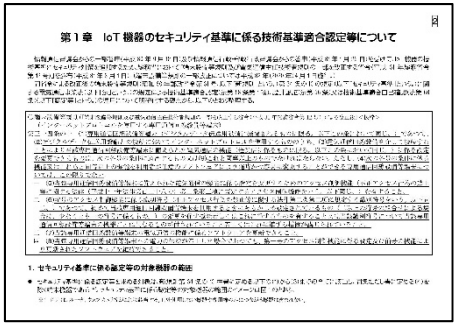
①対象となる機器の範囲、②セキュリティ基準の内容と解説、③セキュリティ基準に係る技術基準適合認定等の審査方法、④通信モジュール等の扱い

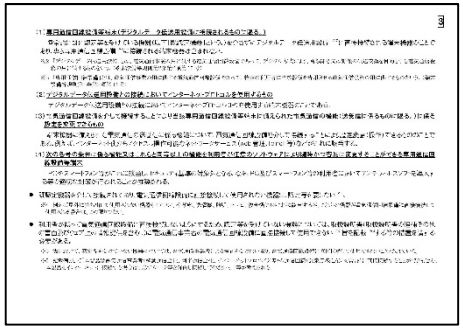
  - 第2章：電波を使用する端末機器関連（端末設備等規則第9条）

対象となる機器の範囲と審査方法


電気通信事業法に基づく端末機器の基準認証
に関するガイドライン(第1版)

2019 年4月 22 日
総務省


第１章　IoT 機器のセキュリティ基準に係る技術基準適合認定等について



電気通信事業法に基づく端末機器の基準認証に関するガイドライン

- **セキュリティ基準をかみ砕くと…**

  - **対象機器の例**

    Webカメラ

    電気通信事業者回線に直接接続される（可能性のある）ルータ

  - **対象機器が実装すべき機能・要件**

    ① 電気通信に関する設定を変更する際にIDやパスワード等の入力を求める機能

    ② 端末の出荷時に設定されている電気通信に関する設定を変更する際に必要なIDやパスワード等について、初回起動時にこれらを変更するよう促す機能

    ③ 電気通信の機能を制御等するソフトウェアを更新できる機能

    ④ 端末の電源を落としても上記①の機能及び③で更新されたソフトウェアが確実に維持されていること

  - **本制度（関係省令、ガイドライン）の施行時期**

    令和2年4月1日

● 適合表示端末機器を組み込んだ端末機器について

- 既に端末接続の技術基準に係る認定等を受けた表示がなされている端末機器（例：通信モジュール）を組み込んだ製品がセキュリティ基準の対象機器である場合には、**当該製品を対象としてセキュリティ基準を含む端末設備の接続の技術基準に係る認定等を受ける**ことになる

- 施行日前後の認定については、下図のとおり。

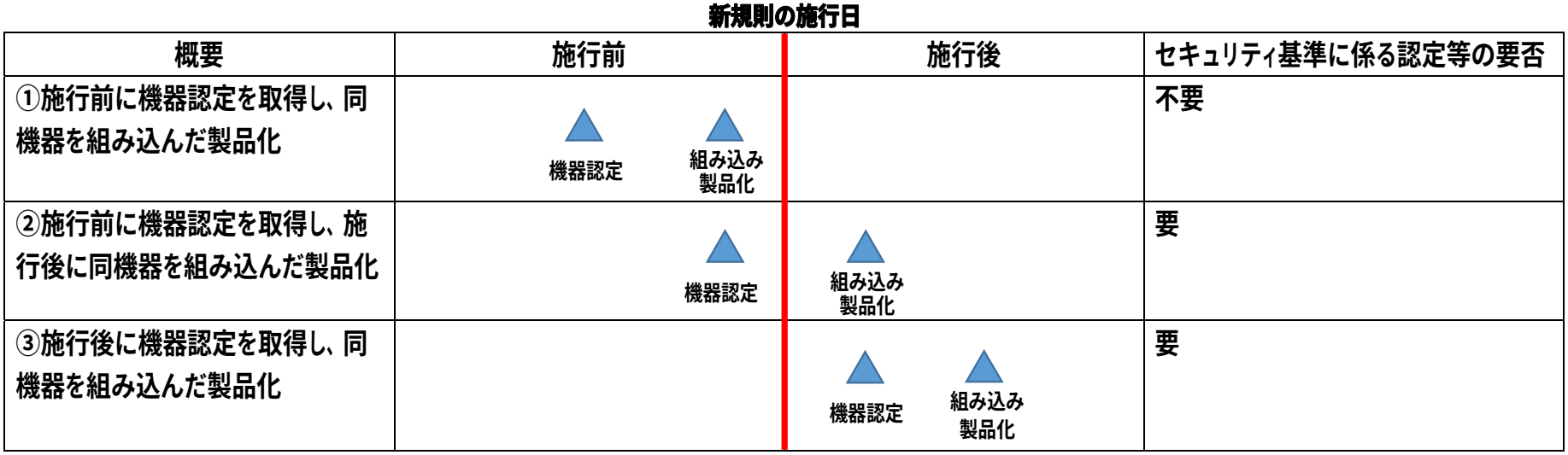


図　端末設備等規則の改正前後における認定等の対象機器の扱い