資料１－４－１

NOTICEの現況

令和5年1月

事　務　局

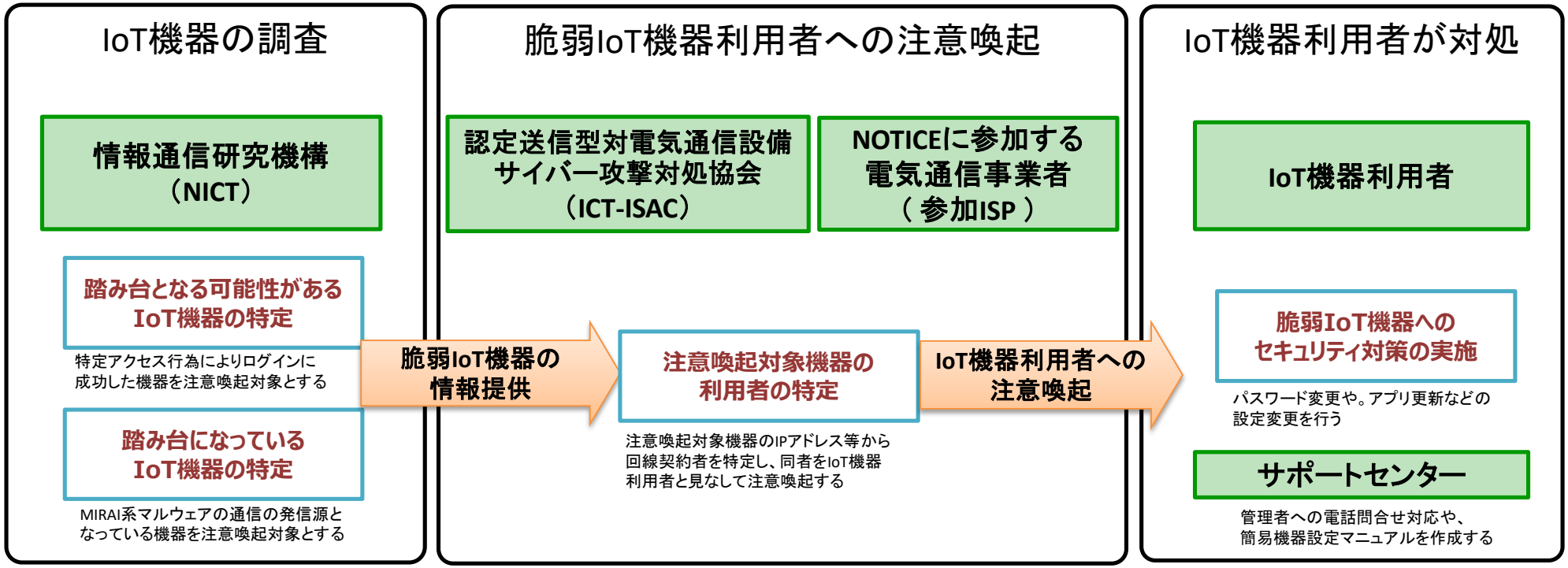
１．NOTICEの枠組み

２．NOTICEの成果

３．NOTICEの課題･今後検討すべき論点

NOTICEの枠組み

- セキュリティ対策の甘いIoT機器の存在が、ボットネットのようなIoT機器等を踏み台とする攻撃が発生する一因となっている
- NICT、ICT-ISAC、ISPによる協調的な対処により、 IoT機器利用者に適切な管理を促す枠組みとして、2019年からNOTICEに着手



＊特定アクセス行為：特定のID・パスワードによりログイン試行する行為。

＊ISPは正当業務行為、緊急避難等の条件に合致する場合に限り、回線契約者を特定する。

＊IoT機器利用者がIoT機器管理者ではない場合は、IoT機器利用者からIoT機器管理者へ連絡するようお願いしている。

NICTによる「IoT機器の調査」

- 参加ISPが管理しているIPアドレスを対象に特定アクセス調査等を実施し、脆弱IoT機器を特定
- 脆弱IoT機器のIPアドレス等を「注意喚起対象IPアドレス」として、ICT-ISACを通じてISPに通知

特定アクセス調査の対象IPアドレス

・調査対象はIPv4グローバルアドレスが付与された機器（構内、宅内の機器は調査対象外）
・国内のIPアドレスの約59%をカバーしている

	日本国内の総IP数（JPNIC管理数）	約1.9億
（未参加ISP、大学等が管理するIPアドレス）	**特定アクセス調査対象IPアドレス**	**約1.12億**

特定アクセスで用いるプロトコル等

開始月	プロトコル	ID/パス
2019.2	Telnet	約100組
2019.7	Telnet/SSH	約100組
2020.10	Telnet/SSH	約600組
2022.6	Telmet/SSH/http/https	約600組

調査手法

調査手法	検知できる脆弱IoT機器	脆弱IoT機器がサイバー攻撃に悪用されるおそれ
特定アクセス	推定可能なIDパスワードを利用している機器	MIRAI系ボットネットに感染してDDoS攻撃に加担するおそれ 攻撃者にログインされ、ルータに格納されたPPPoE認証情報を窃取、悪用されるおそれ
NICTER観測	マルウェアに感染している機器	MIRI系ボットネットの一部としてDDoS攻撃に加担するおそれ
ポートスキャン	悪用される可能性がある機器	DDoS攻撃のリフレクタとして悪用されるリスク（DNS、NTP、SSDPプロトコルが対象） VPN機器の既知の脆弱性を突いて内部ネットワークに侵入されるおそれ

ICT-ISACと参加ISPによる「利用者への注意喚起」

- ICT-ISACは参加ISPに「注意喚起対象アドレス」を配布するとともに、これに基づく注意喚起実施状況を集約して把握
- ICT-ISACは未参加ISPがNOTICEに参加できるよう必要な調整を実施
  - 参加資格の確認、参加手続きの支援、注意喚起実施方法等の指導
- 参加ISPは「注意喚起対象IPアドレス」に基づき、当該IPアドレス利用者を特定して注意喚起を実施

参加ISP数の推移

	参加ISP	注意喚起対象IP
2019年4月	24社	3500万IP
2020年4月	50社	1.08億IP
2021年4月	66社	1.12億IP
2022年4月	70社	1.12億IP
現在	74社	1.12億IP

11月の注意喚起実施状況

特定アクセス調査	Telnet/SSH	http/https
①特定アクセス調査対象	約1.12億	約1.12億
②脆弱IoT機器数（特定アクセス成功件数）	2,226	7,777
③注意喚起対象件数	1,457	3,274

NICTER調査	MIRAI系感染
①NICTER観測対象	（全範囲）
②脆弱IoT機器数（MIRAI系感染疑い件数）	16,793*
③注意喚起対象件数	16,793*

*日次注意喚起の1か月分累計数

参考：ISPがNOTICEに参加するために必要な手続

- NOTICEに参加されているISPには、法令を遵守しながらセキュリティ対策を推進する観点から、以下の手続きをとっていただいています

情報の取り扱いに関するもの

NICTとの覚書締結　（対NICT）

- ✓ NOTICEの調査結果は、不正アクセスにも悪用されかねない機微な情報であることから、情報の適正な取扱いを確保する必要があります。
- ✓ そのため、総務大臣が認可したNICTの実施計画の規定により、参加ISPとNICTとの間で覚書の取り交わしが必要となります。

ICT-ISACとのNDA　（対ICT-ISAC）

- ✓ NOTICEの調査結果については、NICTからICT-ISACを通じてISPに通知しています。
- ✓ ICT-ISACの非会員である場合は、ICT-ISACと秘密保持契約（NDA）の締結が必要となります。

注意喚起の実施に関するもの

技術的条件の設定・認可　（対総務省）

- ✓ NICT法及び電気通信事業法の規定により、利用者の端末設備等がサイバー攻撃(送信型対電気通信設備サイバー攻撃／例:DDoS攻撃)を行うことを禁止すること等の技術的条件を定める必要があります。
- ✓ 技術的条件を定めるに当たっては、申請書を提出し、総務大臣の認可を受ける必要があります。

サービス提供約款の変更　（対加入者）

- ✓ 利用者に対し技術的条件適合性に係る検査を求めることが可能となるため、利用者保護の観点からその旨明確化する約款変更を行う必要があります。
- ✓ NOTICEの調査結果通知を受けた場合は、正当業務行為として利用者を特定し注意喚起を行うため、利用者保護の観点から約款変更を行う必要があります。

サポートセンターによる「IoT機器対策支援」

- 注意喚起を受けたIoT機器利用者は対策を行うことが求められる
  - サポートセンターがIoT機器の機種に応じた対策方法を案内する
- サポートセンターはホームページを通じて各種の情報を提供している
  - NOTICEの活動内容、実施状況
  - お知らせ、FAQ

IoT機器利用者に案内している基本的な対策

- IoT機器のパスワードは初期設定のものを使わず、複雑なものに変更するなど適切な設定を行う
- IoT機器のファームウェアは常に最新のものにする
- 使用していないIoT機器はインターネットに接続しない（又は電源を切る）

令和3年度の活動実績

- コールセンター問合せ対応数　634件
- HP訪問ユニークユーザ数　18,162人
- IoT機器の設定マニュアル数　132件

１．NOTICEの枠組み

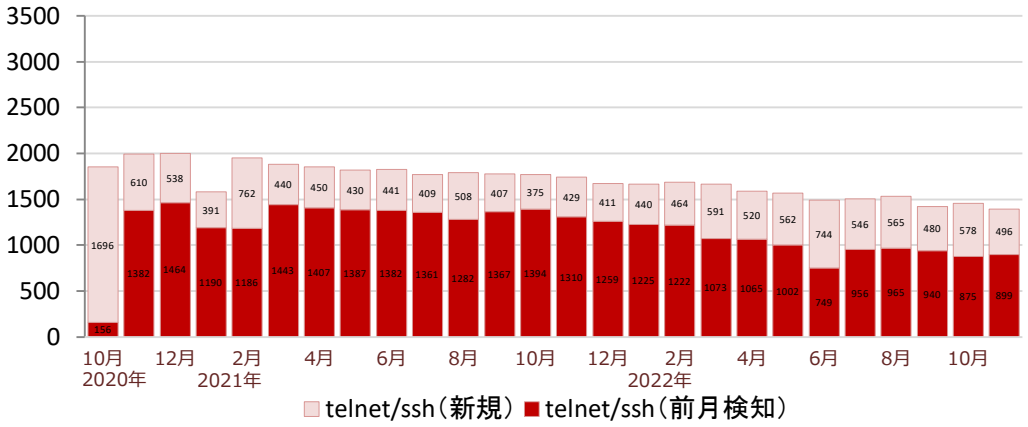
２．NOTICEの成果

３．NOTICEの課題･今後検討すべき論点

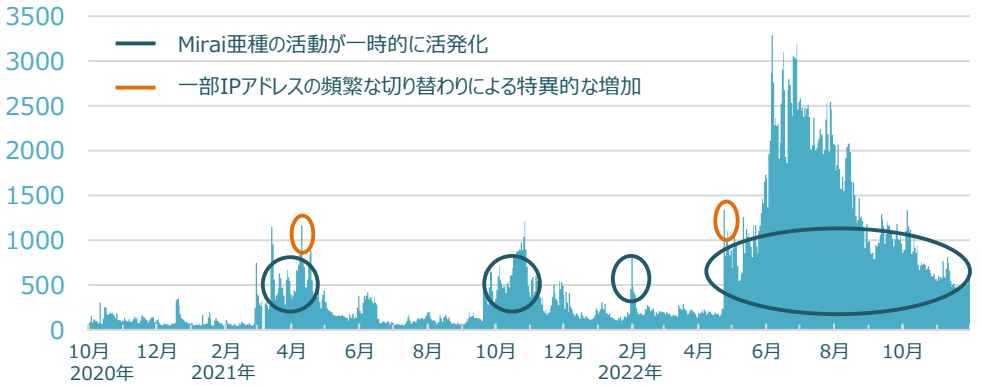
注意喚起対象IPアドレス件数の推移

- 特定アクセス調査により検知される脆弱IoT機器数は継続的に減少傾向にある
  - 2020.12から約30%の削減
- NICTER調査により検知される脆弱IoT機器数はMirai亜種の活動の活発化などにより高い水準に留まっている

特定アクセス調査に基づく注意喚起対象件数
（Telnet/SSHのみ）



NICTER調査に基づく注意喚起対象件数



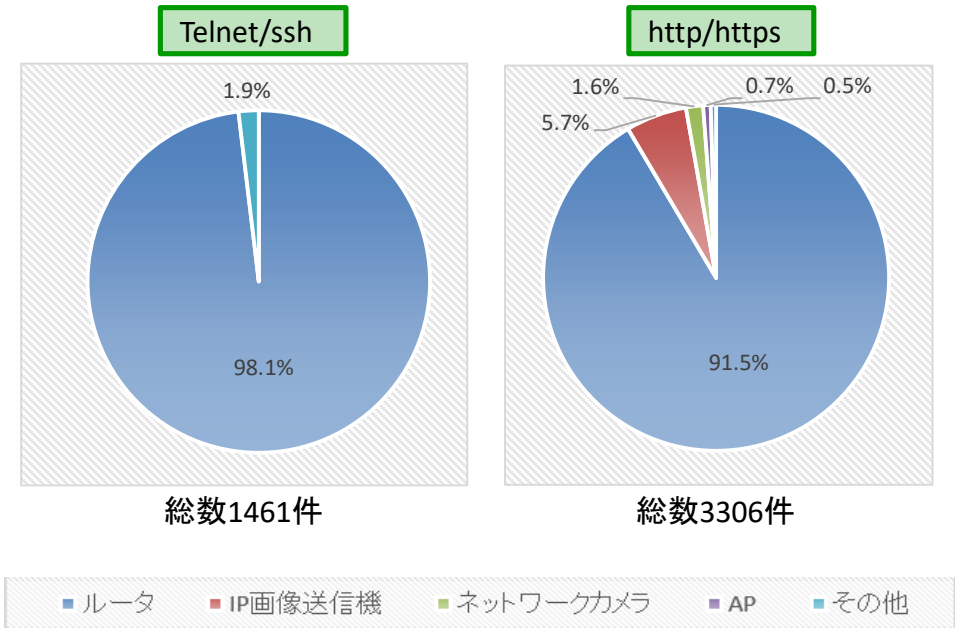
注意喚起の実施件数（2019年4月～2022年10月）

	調査頻度	注意喚起対象累計	期間中平均	注意喚起累計	検知IoT機器機種
特定アクセス調査 (Telnet/SSH)	月次	48,055件	1,092件/月	18,195件	225機種
(http/https)		19,512件	3,252件/月	1,845件	422機種
NICTER調査 (MIRAI系感染)	日次	531,777件	421件/日	13,661件	-

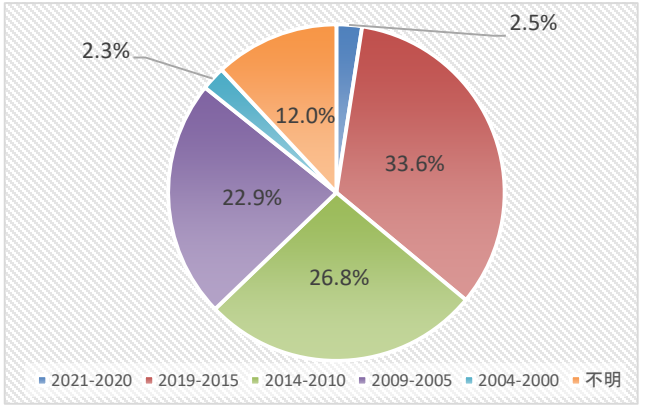
注意喚起対象機器の特徴

- 注意喚起対象機器の大多数はルータで、次いでネットワークカメラ関連機器
- 総務省のIoTセキュリティ基準（端末設備等規則第34条の10）が施行された2020年4月以降後に発売されたIoT機器の検知数は少ない
  - 2014年以前に発売されたIoT機器等が検知数の半数以上(52%)を占めるなど、相当古い機器が多い

注意喚起対象機器の機種別の割合（2022年11月）



注意喚起対象機器の発売年（2022年11月）



総数4767件

IoTセキュリティ基準（端末設備等規則第34条の10）

1 アクセス制御機能
2 初期設定のパスワードの変更を促す等の機能
3 ソフトウェア更新機能
4 変更したID/パスワードを維持する機能

NOTICEの成果と期待

- 日本のインターネットに、どのような脆弱IoT機器がどの程度接続されているのかを明らかにできるようになった
  - 参加機関が定期的に脅威情報を共有する機会が得られた
  - 普及しているIoT機器に脆弱性が発見された場合に、それが悪用されればどの程度の影響があるのか等のリスク評価が行えるようになることに期待

- 脆弱IoT機器の利用者へ直接注意喚起ができるようになった
  - 注意喚起のためにISPが利用者を特定してもよい条件が整理がされた
  - サイバー攻撃等のリスクに対処するためにIoT機器管理者の協力が必要になった場合に、迅速に対応できるようになることに期待

- 脆弱IoT機器の利用者に注意喚起を行うことで、脆弱IoT機器を削減する効果が確認された
  - 他方、注意喚起だけでは対策が進まない機器があることもわかってきた
  - 個人利用者と法人利用者では異なる事情があることもわかってきた

NOTICEの副次的な効果

- 関係機関間で問題認識や検知情報の共有等が進んだ結果、当初想定していた利用者への注意喚起以外にも、いくつかの好事例が出ている

ISPによる対策が行われた事例

特定アクセスの予備調査で4000台超の脆弱IoT機器（ルータ）を検知した。これらはISPが配布・管理しているルータであったため、ISPとメーカーの協力を得てパッチを開発・適用し対処を完了できた。

Emotet対策に協力した事例

インターポールから警察庁に日本国内のEmotet感染端末の情報提供があった。警察庁と連携し、NOTICEの枠組みを用いて当該感染端末利用者への注意喚起を行うことができた。

メーカーが脆弱性対策を行った事例

国内で一定規模流通しているIoT機器を対象にNICTが解析を行った。これにより発見した脆弱性をメーカーと共有し、ファームウェアのアップデートを行うことができた。

１．NOTICEの枠組み

２．NOTICEの成果

３．NOTICEの課題･今後検討すべき論点

NOTICEが現在取り組んでいる課題

- 注意喚起の効果が現れない脆弱IoT機器への対策
  - IoT機器管理実態に応じた利用者への注意喚起実施方法の改善
  - IoT機器設置管理に関わる卸売り事業者、Sierとの連携

- 脆弱性が明らかになってから対処を求めるのではなく、
  予め適切な管理が行われるようにするための対策
  - IoT機器メーカーとの連携

- IoT機器の適切な管理の重要性に関する意識啓発
  - NOTICEホームページ等を通じた情報提供の充実

今後検討すべき論点

- 調査対象の拡大・利用者への注意喚起以外の対処方法の在り方
  - ID・パスワードに脆弱性があり、注意喚起対象となるIoT機器は、発売から5年以上経過した古いものが大部分を占めている。
  - 感染の疑いがあるIoT機器（NICTER）の注意喚起件数は、昨年４月以降急増しており現在も高い水準にある。
  - 調査の過程（ポートスキャン）でID・パスワード以外の脆弱性を有するIoT機器が判明するケースもある。
  - メーカーに対してファームウェアの更新依頼を行った事例やISP側の対策強化のきっかけになった事例など、利用者への注意喚起以外の対処により効果的な対策につながった事例もある。

- 参加ISPの拡大・既に参加しているISPのインセンティブの確保に向けた方策
  - NOTICEに参加していないISPのネットワークに接続しているIoT機器等は調査の対象外となっているほか、卸売等の通信サービスの市場構造も踏まえていく必要がある。

- 利用者側におけるIoT機器の適切な管理など、注意喚起の実効性を向上させていくための方策
  - 利用者への注意喚起によって脆弱性のあるIoT機器の数は一定程度減少しているが、注意喚起の効果が現れないケースも存在。注意喚起を受けた利用者におけるIoT機器の管理体制や意識等によっても対応に差が出ている。

- メーカー側の適切なサポートの在り方
  - 利用者がIoT機器に管理機能があることに気づいていないケースも存在。機器マニュアルにリスクとセキュリティ対策方法のわかりやすい説明があると助けになる。
  - サポート期限の明示やサポート期限切れの利用者への告知などが強化されると古いIoT機器の更新が促される。

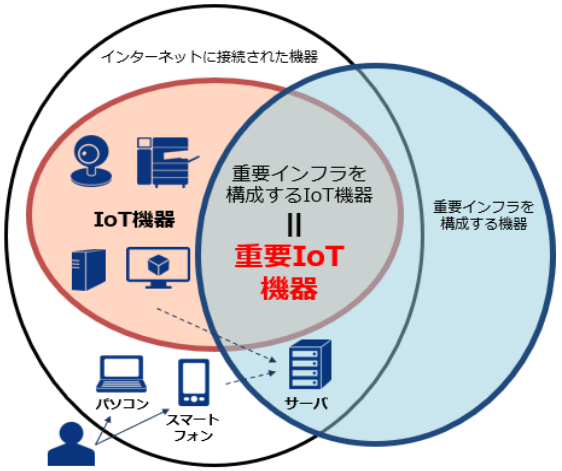
- 上記課題等に効果的に対応していくための今後のNOTICEの枠組みと運営の在り方
  - NOTICEの取組により、脆弱性を有するIoT機器の全体的な傾向を把握し、対処につなげる枠組みができたことは大きな成果であり、上記課題に対処しつつ、この枠組みを更に効果的に活用していくことが必要。

参考情報

参考：重要IoT機器調査

- 2017年と2020年の２度にわたり、CENSYSを用いた調査を実施し、脆弱IoT機器を複数確認
- 脆弱IoT機器の管理体制が十分でない事例がいくつか確認された
  - 問題が認識されても即応可能な運用体制がないことがあることが分かった

重要IoT機器



例：水道監視システムのIoT機器

年度	調査対象	脆弱性検出	利用者特定	注意喚起実施	対策済
2017	約1.5億IP*	150件	77件	36件	-
2020		924件	359件	224件	187件

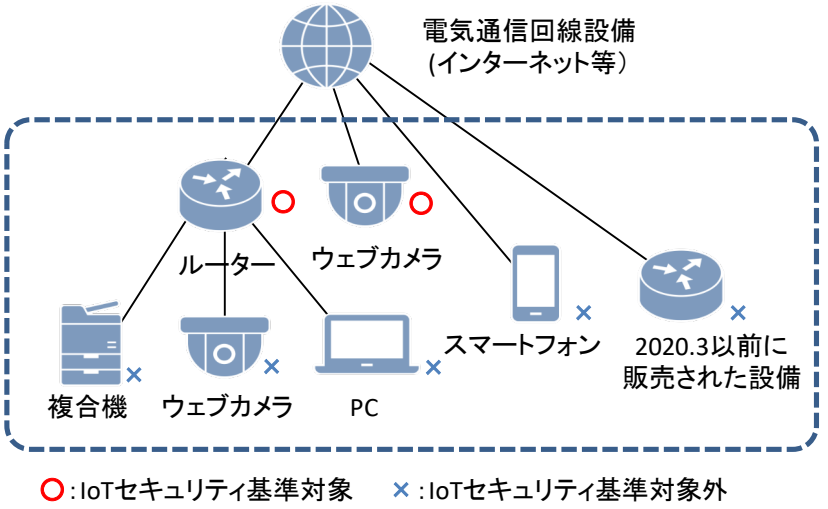
*日本が保有する総IP数の2億から一般的なWebサイト、到達性のないもの、海外で利用されている可能性があるものなどを除外

ISPが利用者からの接続の請求を拒否できる場合１

１　電気通信事業者（ISP）は、利用者から端末設備をその電気通信回線設備に接続すべき旨の請求を受けたときは、その接続が総務省令で定める技術基準※（技術的条件を含む。）に適合しない場合その他総務省令で定める場合を除き、その請求を拒むことができません。

※IoTセキュリティ基準（端末設備等規則第34条の10）の概要

IoT機器は次の条件に適合するか同等以上のものであること
1 設定変更するためのアクセス制御機能
2 初期設定のパスワードの変更を促す等の機能
3 ソフトウェア更新機能
4 電力供給が停止しても変更したID/パスワードを維持する機能



２　端末設備に異常がある場合等において、技術基準に適合するかどうかの検査の結果、適合しなかった場合

ISPは、端末設備に異常がある場合その他電気通信役務の円滑な提供に支障がある場合等において、利用者に対し、その端末設備の接続が総務省令で定める技術基準（技術的条件を含む。）に適合するかどうかの検査を求めることができます。これを拒否した場合、又は検査の結果、適合せず、その後の改善がなされなかった場合に、接続の請求を拒むことができます。

ISPが利用者からの接続の請求を拒否できる場合２

３　ISPが定めるサービス約款のサービス停止規程に該当する場合

参考例：

（FTTHサービスの利用停止）
当社は、基本契約者又は利用契約者が次のいずれかに該当する場合は、6ヶ月以内で当社が定める期間、そのFTTHサービスの利用を停止することがあります。
(1)（利用に係る基本契約者又は利用契約者の義務）の規定に違反したとき。

（利用に係る基本契約者又は利用契約者の義務）
基本契約者又は利用契約者は、次のことを守っていただきます。利用契約者の行為が禁止行為のいずれかに該当すると判断した場合は、義務に違反したものとみなします。
（守るべきこと）
(1) 違法に、又は公序良俗に反する態様で、FTTHサービスを利用しないこと。
（禁止行為）
(1) 当社若しくは他人の電気通信設備等の利用若しくは運営に支障を与える行為又はそのおそれのある行為
(2) 他人に無断で広告、宣伝若しくは勧誘の文書等を送信又は記載する行為
(3) 他人が嫌悪感を抱く、又はそのおそれのある文書等を送信、記載若しくは掲載する行為

参考:電気事業通信法の端末設備の接続に関する参照条文 19

電気事業通信法

（端末設備の接続の技術基準）

第五十二条　電気通信事業者は、利用者から端末設備（電気通信回線設備の一端に接続される電気通信設備であつて、一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む。）又は同一の建物内であるものをいう。以下同じ。）をその電気通信回線設備（その損壊又は故障等による利用者の利益に及ぼす影響が軽微なものとして総務省令で定めるものを除く。第六十九条第一項及び第二項並びに第七十条第一項において同じ。）に接続すべき旨の請求を受けたときは、その接続が総務省令で定める技術基準（当該電気通信事業者又は当該電気通信事業者とその電気通信設備を接続する他の電気通信事業者であつて総務省令で定めるものが総務大臣の認可を受けて定める技術的条件を含む。次項並びに第六十九条第一項及び第二項において同じ。）に適合しない場合その他総務省令で定める場合を除き、その請求を拒むことができない。

2　前項の総務省令で定める技術基準は、これにより次の事項が確保されるものとして定められなければならない。

一　電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること。

二　電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること。

三　電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界が明確であるようにすること。

（端末設備の接続の検査）

第六十九条　利用者は、適合表示端末機器を接続する場合その他総務省令で定める場合を除き、電気通信事業者の電気通信回線設備に端末設備を接続したときは、当該電気通信事業者の検査を受け、その接続が第五十二条第一項の総務省令で定める技術基準に適合していると認められた後でなければ、これを使用してはならない。これを変更したときも、同様とする。

2　電気通信回線設備を設置する電気通信事業者は、端末設備に異常がある場合その他電気通信役務の円滑な提供に支障がある場合において必要と認めるときは、利用者に対し、その端末設備の接続が第五十二条第一項の総務省令で定める技術基準に適合するかどうかの検査を受けるべきことを求めることができる。

3　前項の規定は、第五十二条第一項の規定により認可を受けた同項の総務省令で定める電気通信事業者について準用する。この場合において、前項中「総務省令で定める技術基準」とあるのは、「規定により認可を受けた技術的条件」と読み替えるものとする。

4　（略）

参考:電気事業通信法の端末設備の接続に関する参照条文 20

電気通信事業法施行規則

（利用者からの端末設備の接続請求を拒める場合）

第三十一条　法第五十二条第一項の総務省令で定める場合は、利用者から、端末設備であつて電波を使用するもの（別に告示で定めるものを除く。）及び公衆電話機その他利用者による接続が著しく不適当なものの接続の請求を受けた場合とする。

端末設備等規則

（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。