資料 136－１－２

情報通信審議会 情報通信技術分科会
IPネットワーク設備委員会
第一次報告

―IoTの普及に対応した電気通信設備に係る技術的条件―

情報通信審議会 情報通信技術分科会
ＩＰネットワーク設備委員会
第一次報告　目次

Ⅰ　検討事項

情報通信審議会情報通信技術分科会 IP ネットワーク設備委員会（以下「委員会」という。）では、平成 17 年 11 月より、情報通信審議会諮問第 2020 号「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」（平成 17 年 10 月 31 日諮問）について検討を行ってきている。

本報告は、「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、昨年 12 月から本年７月にかけて開催された委員会（第 34 回～第 41 回）及び技術検討作業班（第 31 回～第 34 回）において検討された結果を第一次報告として取りまとめたものである。

Ⅱ　委員会及び作業班の構成

委員会の構成は、別表１のとおりである。

検討の促進を図るため、委員会の下に、技術検討作業班を設置して検討を行った。技術検討作業班の構成は、別表２のとおりである。

Ⅲ　検討経過

これまで、委員会（第 34 回～第 41 回）、技術検討作業班（第 31 回～第 34 回）を開催して検討を行い、IoT 機器等の電気通信設備の技術的条件、IoT サービスの安全・信頼性を確保するための資格制度等の在り方、IoT 時代における重大事故に関する事故報告等の在り方等について検討を行い、第一次報告を取りまとめた。

(1) 委員会での検討

① 第 34 回委員会（平成 29 年 12 月 19 日）

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課題について、関係事業者からヒアリングを行った。

② 第 35 回委員会（平成 30 年 2 月 8 日）

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課題について、関係事業者からヒアリングを行った。

③ 第 36 回委員会（平成 30 年 3 月 6 日）

「円滑なインターネット利用環境の確保に関する検討会　対応の方向性」を踏まえ、委員会における検討事項の追加を行うとともに、IoT 機器を含む端末設備のセキュリティ対策について関係者からヒアリングを行った。

また、IoT 時代における重大事故に関する事故報告等の在り方について、技術検討作業班において具体的な内容の検討を行うことを決定した。

④　第 37 回委員会（平成 30 年 3 月 30 日）

IoT 機器を含む端末設備のセキュリティ対策について関係者からヒアリングを行った。

⑤　第 38 回委員会（平成 30 年 4 月 27 日）

IoT 機器を含む端末設備のセキュリティ対策について関係者からヒアリングを行うとともに、技術検討作業班において技術的条件の具体的な内容の検討を行うことを決定した。

⑥　第 39 回委員会（平成 30 年 5 月 24 日）

IoT サービスの安全・信頼性を確保するための資格制度等の在り方について関係者からヒアリングを行った。

また、IoT 時代における重大事故に関する事故報告等の在り方について技術検討作業班における検討状況の報告を行うとともに、IP ネットワーク設備委員会第一次報告骨子（案）の検討を行った。

⑦　第 40 回委員会（平成 30 年 6 月 22 日）

技術検討作業班から、技術検討作業班報告について報告を受けるとともに、IP ネットワーク設備委員会第一次報告（案）の検討を行った。また、同報告（案）を意見募集に付すこととした。

⑧　第 41 回委員会（平成 30 年 8 月 21 日～8 月 28 日、メール審議）

意見募集を実施した結果、６件の意見提出があり、提出された意見を踏まえ検討を行い、IP ネットワーク設備委員会第一次報告を取りまとめた。

(2) 技術検討作業班での検討

①　第 31 回技術検討作業班（平成 30 年 3 月 16 日）

IoT 時代における重大事故に関する事故報告等の在り方について関係者からヒアリングを行った。

② 第 32 回技術検討作業班（平成 30 年 4 月 9 日）

IoT 時代における重大事故に関する事故報告等の在り方として、LPWA サービスの事故報告基準及び大規模なインターネット障害発生時の対策について検討を行った。

③ 第 33 回技術検討作業班（平成 30 年 5 月 10 日）

IoT 時代における重大事故に関する事故報告等の在り方として、大規模なインターネット障害発生時の対策のうち電気通信事業者等に推奨する対策について検討を行うとともに、IoT 機器を含む端末設備のセキュリティ対策について検討を行った。

IoT 時代における重大事故に関する事故報告等の在り方について、検討状況を委員会に報告することとした。

また、IoT 機器を含む端末設備のセキュリティ対策について詳細の検討を行うため、アドホック会合を開催することとした。

④ 技術検討作業班アドホック会合（平成 30 年 5 月 18 日）

IoT 機器を含む端末設備のセキュリティ対策について検討を行った。

⑤ 第 34 回技術検討作業班（平成 30 年 6 月 7 日）

技術検討作業班及びアドホック会合におけるこれまでの検討結果を取りまとめた技術検討作業班報告（案）について検討を行い、技術検討作業班報告を委員会に報告することとした。

Ⅳ　検討結果

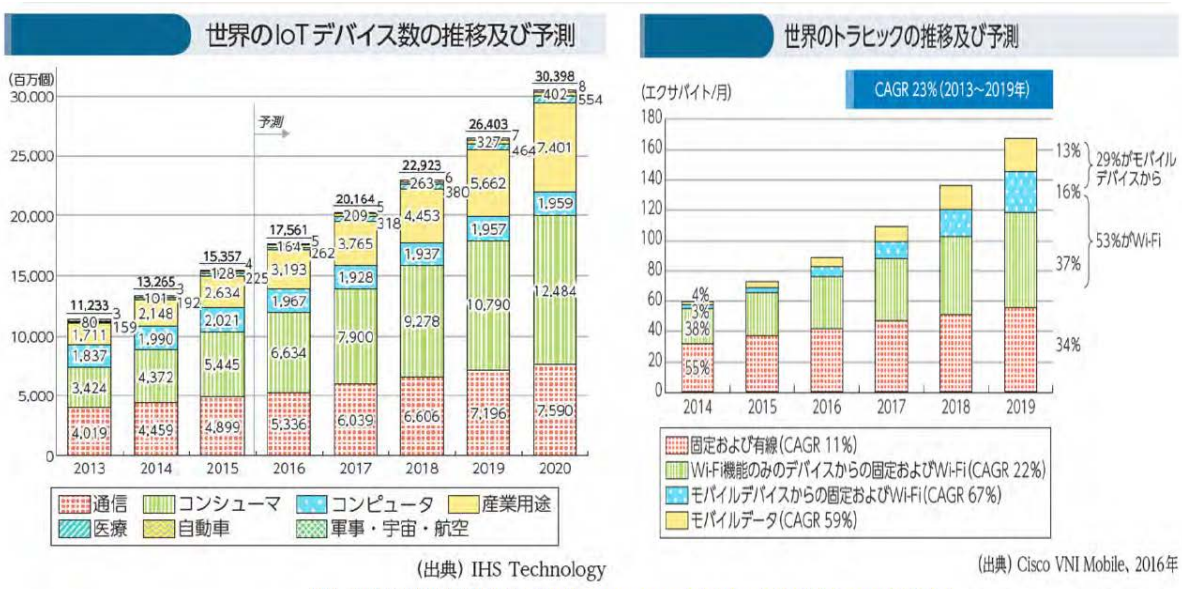
第１章　IoT の普及に対応した電気通信設備に関する検討課題

1.1　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等の利用が進む中、様々な分野において IoT（Internet of Things）の普及が進んでおり、IoT サービスが国民生活に深く浸透しつつある。

民間調査会社の推定によれば、図 1.1 のとおり 2015 年時点で IoT デバイスの数は約 154 億個、2020 年までには約２倍の約 304 億個まで増大すると予測されている。

このように、膨大な機器がネットワークに接続されることにより、データ通信のトラヒックは飛躍的に増大することが予想される。機器メーカの調査によれば、その中でも特にモバイルデバイスからのトラヒックが大きく伸びていくことが見込まれている。



出典：平成28年度情報通信白書　http://www.soumu.go.jp/johotsusintokei/whitepaper/h28.html

図 1.1　世界の IoT デバイス数とトラヒックの推移及び予測

また、IoT サービスの導入が本格化しつつある中で、それを支える通信ネットワークについても、技術革新により高機能化が進むとともに、設備構成の複雑化や利用形態の多様化が急速に進展している。

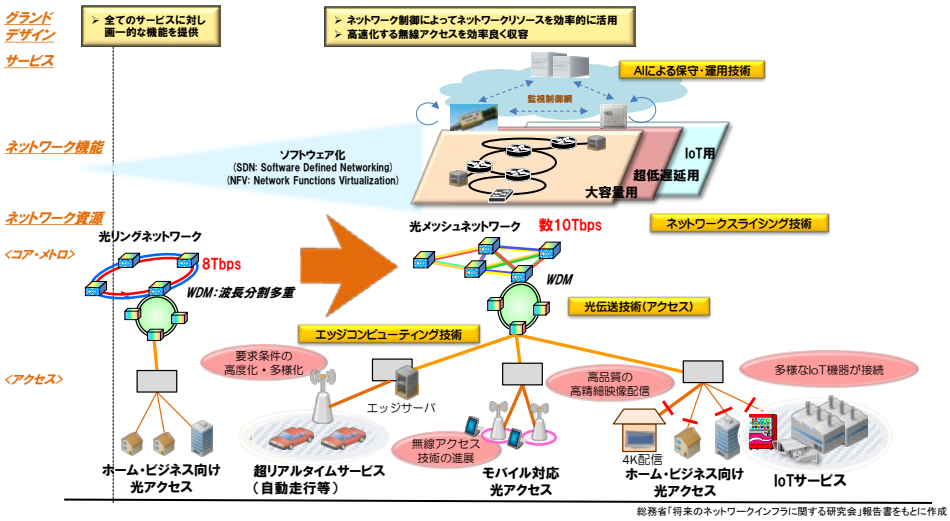


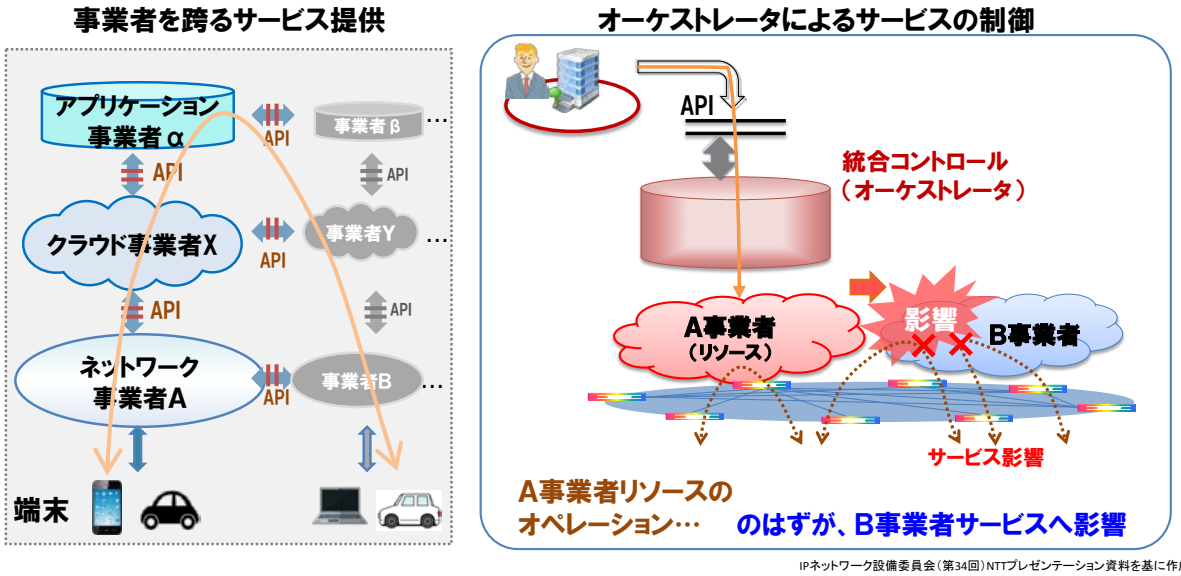
図 1.2　ネットワークの高機能化に伴う設備構成の複雑化及び利用形態の多様化

具体的には、ネットワーク機能のソフトウェア化の進展により、図 1.3 のとおり一つのサービスが様々な事業者が関わることによって提供されるケースが増加しており、今後、多種多様な IoT サービスの普及に伴い、事業者ごとの機能や責任の分界点がより複雑化していくことが想定される。

また、仮想化されたネットワークを活用して複数の事業者が様々な IoT サービスを提供する際には、ネットワーク制御を統合的に行うオーケストレータにより、それぞれの事業者が簡単に自らのサービスリソースを制御できるようになることが想定されるが、その一方で誤った制御をしてしまうと、同じ物理的なリソースを利用している他の事業者のサービスにまで影響を与えてしまう可能性も懸念されている。

このような状況においては、ひとたびネットワーク等に障害が発生すれば、その影響が他の事業者に波及したり、責任の所在があいまいとなるケースが増える可能性があり、国民生活や社会経済活動に大きな影響を及ぼすことが想定される。

今後普及していく様々な IoT サービスを誰もが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ためには、このようなネットワークの高度化や利用形態の多様化の状況を的確に捉えて、将来の IoT サービスの普及に柔軟に対応しつつ、同時にネットワークの安全・信頼性を確実に確保するための対策について、早急に検討することが必要となっている。



IPネットワーク設備委員会（第34回）NTTプレゼンテーション資料を基に作成

図 1.3　ネットワーク機能のソフトウェア化の進展によるサービス形態の複雑化

1.2　IoT の普及に対応するための検討課題

1.1 で述べたように、今後、多種多様な IoT サービスが急速に普及していくことが予想される中、将来にわたり誰もが 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が重要である。このため、委員会において、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に対応するために必要な電気通信設備に係る技術的条件を検討することとしたものである。

具体的には、「IoT の普及に対応した電気通信設備に係る技術的条件」として、以下のとおり検討を行うこととした。

①　IoT に対応した電気通信設備の技術的条件

新たな IoT 用無線通信サービスの導入や通信設備のソフトウェア化等の進展により、ネットワーク設備や端末設備の利用が多様化する中、現行の技術基準や情報通信ネットワーク安全・信頼性基準等の有効性を検証し、必要に応じて見直すこととする。

②　IoT サービスの安全・信頼性を確保するための資格制度等の在り方

IoT 時代のネットワーク設備や端末設備の多様化を踏まえ、電気通信主任技術者や工事担任者に求められるスキルや役割等を検証し、資格制度等の在り方について検討を行う。

③　IoT 時代における重大事故に関する事故報告等の在り方

今後、IoT サービスが多様化し、従来の設備故障以外の原因による事故が増加していくことが想定される中、IoT 時代における重大事故に関する事故報告の在り方について検討を行う。

④　その他

新たな技術を活用した通信インフラの維持方策や、端末機器の基準認証の在り方など IoT 時代に対応するための課題を整理し、必要な検討を行う。

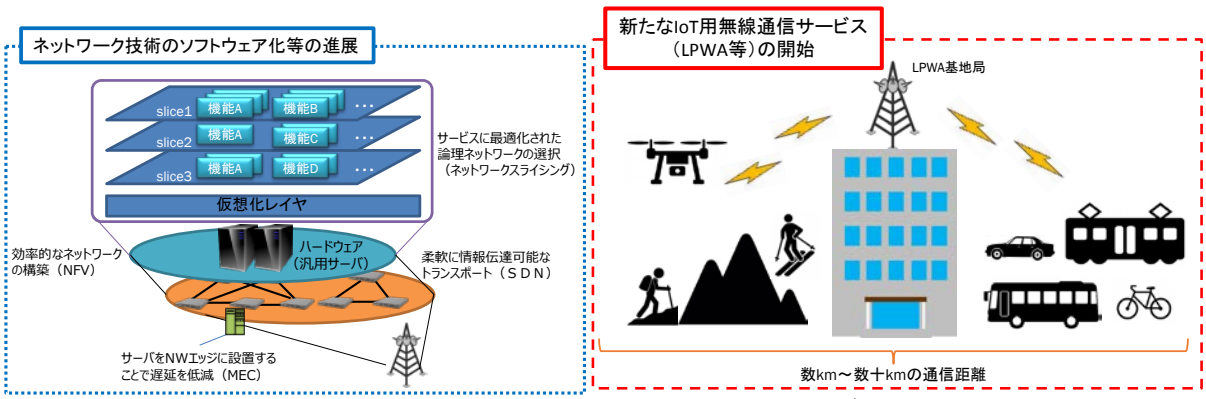


図 1.4 IoT 時代におけるネットワーク設備やサービスの多様化

1.3　サイバー攻撃等によるインターネット障害対策に係る検討課題の追加

近年サイバー攻撃等によりインターネットに重大な支障が発生する事例が増加していることを踏まえて総務省が開催した、「円滑なインターネット利用環境の確保に関する検討会」において、2018 年２月、電気通信事業におけるこれらの障害への対処を促進するための「対応の方向性」が取りまとめられた。

委員会では、その内容を踏まえて以下のとおり検討課題の追加を行った。

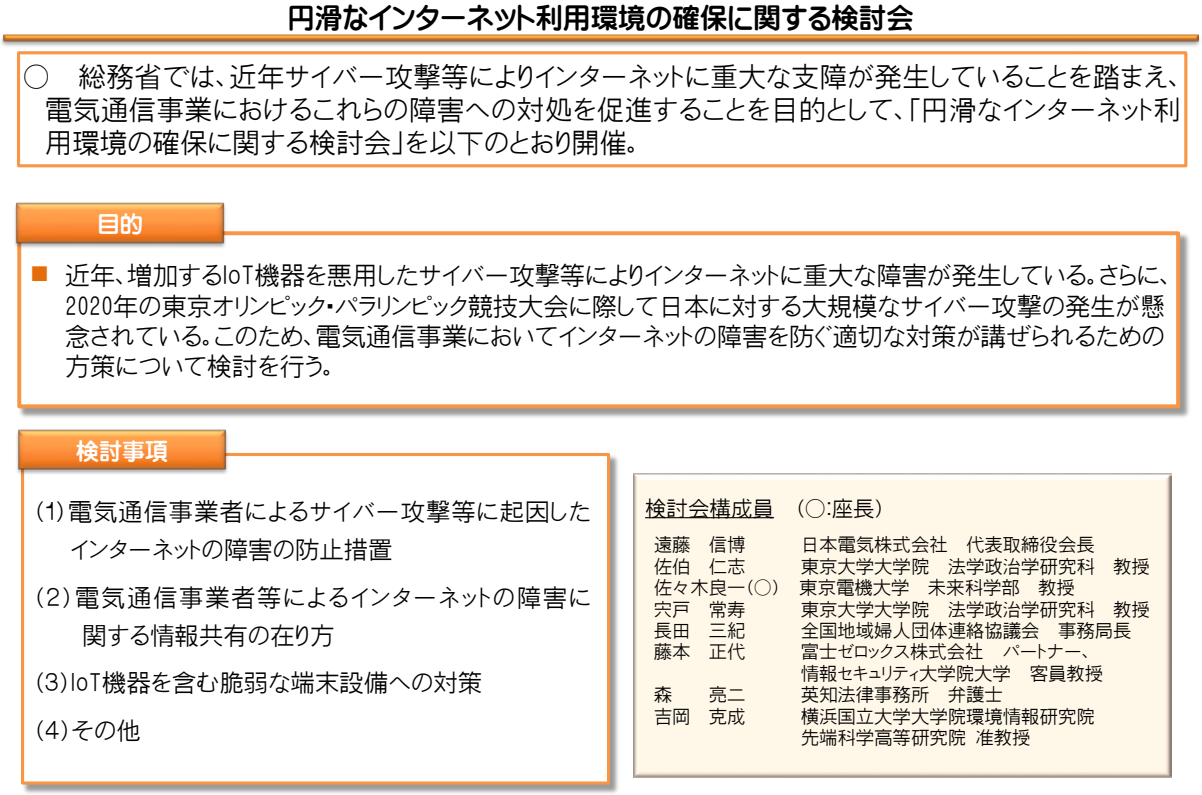


図 1.5　円滑なインターネット利用環境の確保に関する検討会概要

「円滑なインターネット利用環境の確保に関する検討会」により取りまとめられた「対応の方向性」の概要は図 1.6 及び図 1.7 のとおりである。

このうち、「IoT 機器を含む脆弱な端末設備のセキュリティ対策」については、IoT 機器等の端末設備において、基本的なセキュリティ対策を実施すべきとして、具体的な検討にあたっては、国際競争力確保等の観点も踏まえ、IoT サービスや機器の普及の阻害とならないよう、諸外国の検討状況等を踏まえた上で関係者から広く意見聴取し、検討することとされた。

また、「大規模なインターネット障害発生時の対策」については、インターネットの経路情報の送受信を適切に制御する経路フィルターの設定を推奨、インターネット障害に関する情報共有体制の整備といった対策を実施すべきとして、具体的な検討にあたっては、ガイドライン等においてルータの設定について規定するとともに、電気通信事業者から総務省への迅速な障害報告の在り方を含めた情報共有体制を検討する

こととされた。

これら２点の検討課題については、IoT 機器等の端末設備の技術基準や IP ネットワークの事故報告制度の在り方に関する検討を要するものであり、1.2 で述べた委員会の検討課題に密接に関係していることから、「IoT の普及に対応した電気通信設備に係る技術的条件」の中で追加の課題として検討を行うこととした。

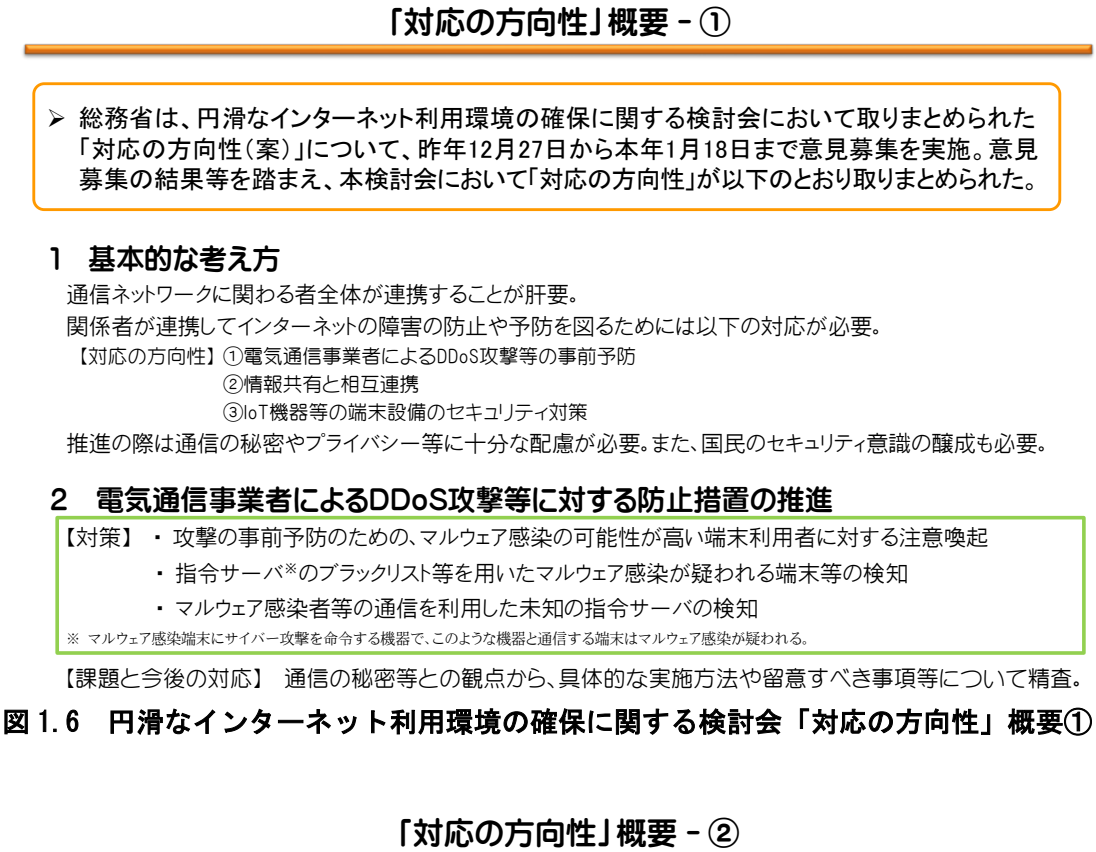


図 1.6　円滑なインターネット利用環境の確保に関する検討会「対応の方向性」概要①

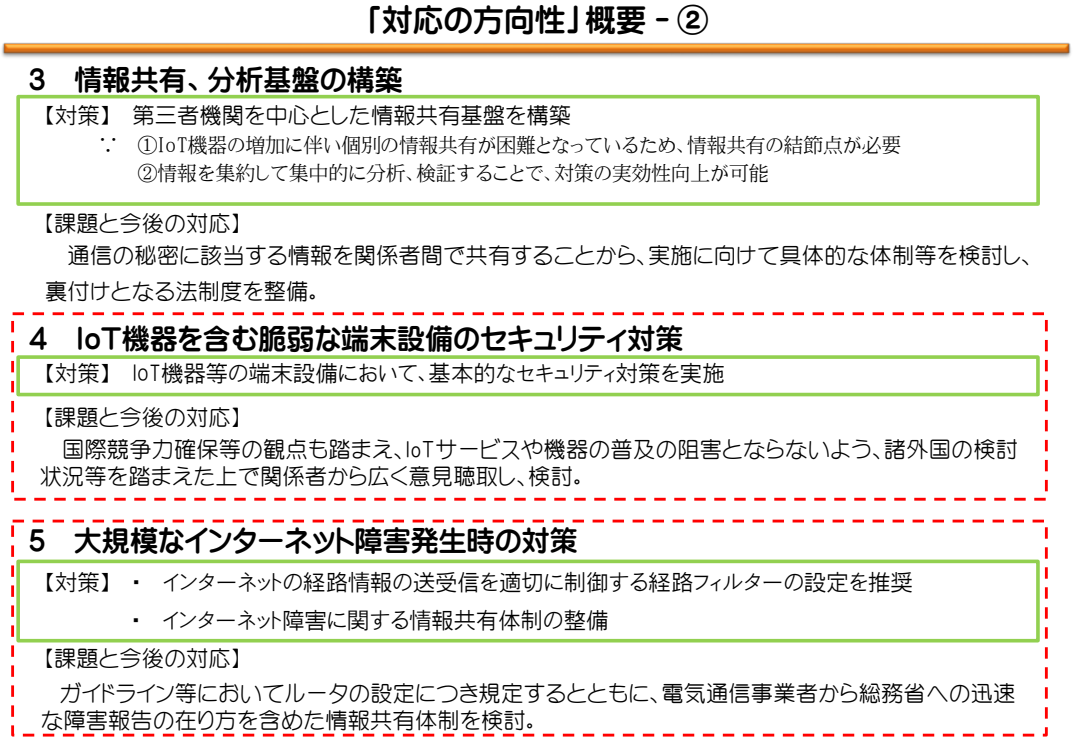


図 1.7　円滑なインターネット利用環境の確保に関する検討会「対応の方向性」概要②

1.4　第一次報告における検討課題

IoT の普及に対応した電気通信設備に係る技術的条件に関する検討課題については、課題が多岐にわたることから、まずは特に早急に対応が求められる以下の２つの課題について先行的に議論を行い、第一次報告として取りまとめることとした。

①IoT 機器等の電気通信設備の技術的条件（IoT 機器を含む端末設備のセキュリティ対策を含む。）

②IoT 時代における重大事故に関する事故報告等の在り方（大規模なインターネット障害発生時の対策を含む。）

なお、その他の検討課題については、引き続き委員会において検討を行うこととした。

［参考］　電気通信設備の技術関連制度の現状

電気通信事業法では、ICT サービスを提供する上での基盤となる電気通信設備について、サービス中断等の事故が発生した場合、国民生活や社会経済活動に深刻な影響を与えかねないため、ICT サービスが安定的に提供される環境を確保するため、図 1.8 に示すようにネットワーク設備や端末設備等の電気通信設備の安全・信頼性を確保するための制度を設けている。

これらの制度の概略について以下に述べる。

図 1.8　電気通信設備の安全・信頼性の確保に関する制度

（１）　事業用電気通信設備に係る技術基準

（ア）　制度の枠組み

電気通信事業法では、図 1.9 のとおり回線設置事業者及び指定を受けた回線非設置事業者（有料かつ利用者 100 万以上のサービスを提供するもの）に対し、事業用電気通信設備に係る技術基準への適合維持義務を規定している。また、当該事業者に対する自己確認及び管理規程の届出等や、電気通信設備統括管理者及び電気通信主任技術者の選任・届出等に係る義務を規定している。

	技術基準 適合維持 （設備を技術基準に適合するように維持）	自己確認 （設備の技術基準適合への適合を自己確認し届出）	管理規程 （設備の管理規程を定め届出）	電気通信設備 統括管理者 （経営層における設備管理の責任者を選任し届出）	電気通信 主任技術者 （現場での設備管理の監督責任者を選任し届出）
回線設置事業者	○	○	○	○	○
指定を受けた 回線非設置事業者	○	○	○	○	○
指定を受けていない 回線非設置事業者	－	－	－	－	－

図 1.9　事業用電気通信設備に係る技術基準の枠組み

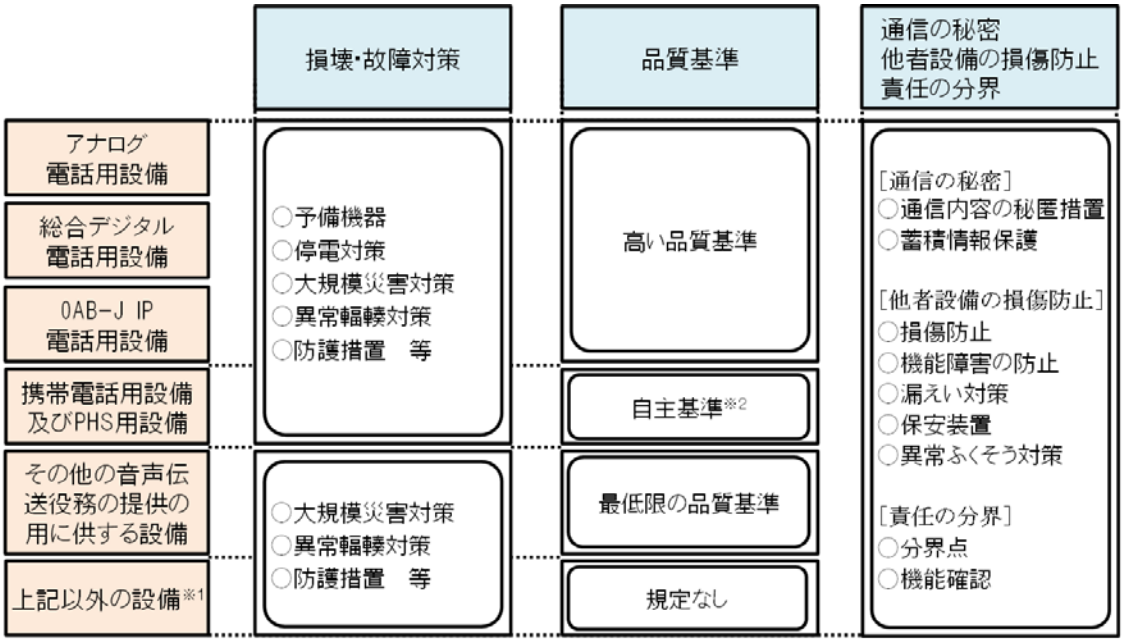
（イ）　事業用電気通信設備の技術基準

事業用電気通信設備に係る技術基準は、

- 設備の損壊・故障による役務提供への支障を防止すること
- 品質が適正であるようにすること
- 通信の秘密が侵されないようにすること
- 他者設備の損傷を防止すること
- 責任の分界が明確であるようにすること

が確保されるものとして、その詳細を事業用電気通信設備規則において規定しており、図 1.10 のように電気通信事業者が提供する電気通信役務の内容に応じた基準が設けられている。

電気通信事業者は、事業用電気通信設備が当該技術基準に適合していることを自己確認し、総務大臣に届け出るとともに、事業用電気通信設備が当該技術基準に適合するよう維持する義務が課されている。



※1 データ伝送役務の提供の用に供する設備等が該当。
※2 携帯電話については、電波の伝搬状態に応じて通話品質が影響を受けることを考慮し、基準を一律に定めるのではなく、自主基準としている。

図 1.10　事業用電気通信設備の技術基準

（２）　利用者が接続する端末設備等の接続の技術基準

（ア）　利用者が接続する端末設備等の接続の技術基準の考え方

電気通信事業法では、図 1.11 のように電気通信事業者の電気通信回線設備に接続して使用する端末設備について、次の事項を確保するものとして総務省令に定める技術基準に適合することを求めている。

- 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
- 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
- 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を明確であるようにすること

また、自営電気通信設備の接続の技術基準として、端末設備に係る技術基準が準用されている。

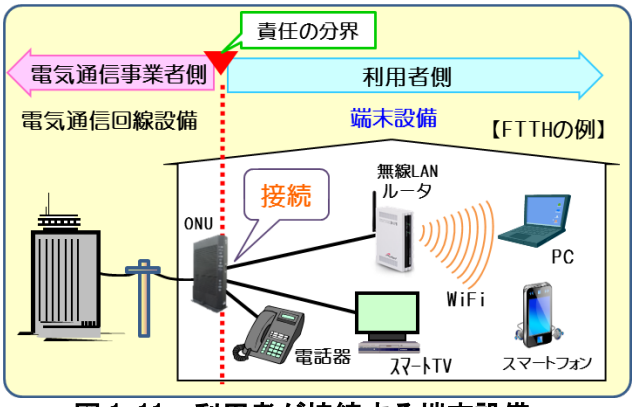


図 1.11　利用者が接続する端末設備

（イ）　端末設備の接続と技術基準の確保

電気通信事業者は、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、その接続が技術基準に適合しない場合等を除き、その請求を拒むことができないとされている。

また、利用者は、技術基準に適合している旨の表示（いわゆる技適マーク）が付された適合表示端末機器を接続する場合等を除き、電気通信事業者による接続の検査を受け、技術基準に適合する端末設備と認められなければ、当該設備を使用できないとされている。

さらに、利用者は、端末設備を電気通信回線設備に接続するとき、これに係る工事を工事担任者に行わせ、又は実地に監督させる必要がある。

（３）　端末機器の基準認証制度

端末機器の基準認証制度とは、事業用電気通信設備に接続して使用される端末機器やその設計について、接続の技術基準に適合していることを登録認定機関等が認定する制度であり、

- 端末機器を１台毎に認定する技術基準適合認定
- 端末機器の設計を認証する設計認証
- 製造者等が技術基準に適合していることを自ら確認し、総務省に届け出る技術基準適合自己確認

のいずれかの方法により認定を取得することができる（図 1.12）。

また、「特定機器に係る適合性評価手続の結果の外国との相互承認の実施に関する法律」に基づき、相互認証協定を締結した相手国の評価機関が実施した技術基準への適合性評価の結果について、日本国と相手国の間で相互に受け入れることが可能となっている（相互承認協定（MRA））。

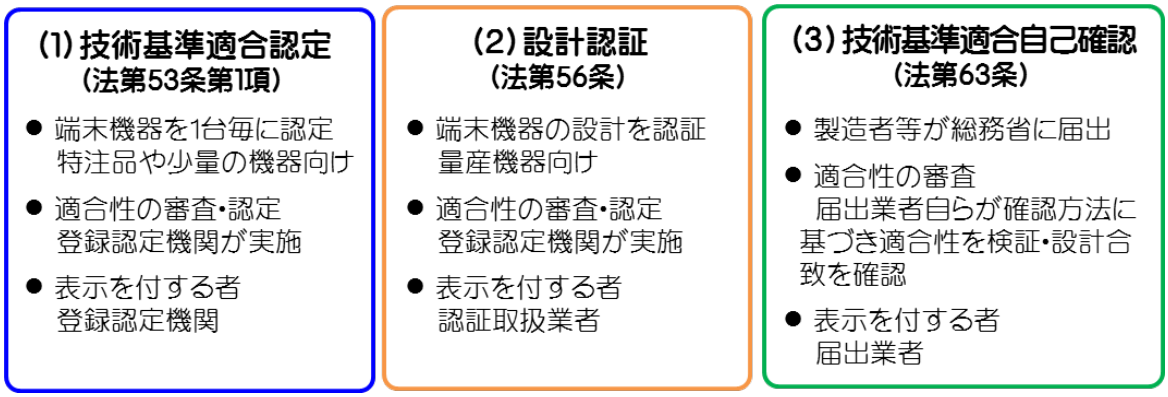


図 1.12　認定を取得する方法

（４）　事業用電気通信設備の管理規程

事業用電気通信設備の技術基準適合維持義務が適用される電気通信事業者に対しては、電気通信役務の確実かつ安定的な提供を確保するため、事業用電気通信設備に関する事故の事前防止や事故発生時に必要な取組みのうち、技術基準等で画一的に定めることが必ずしも適当でなく、事業者ごとの特性に応じた自主的な取組みにより確保すべき事項について、図 1.13 のように当該事項を規定した「管理規程」の作成・届出義務を課している。

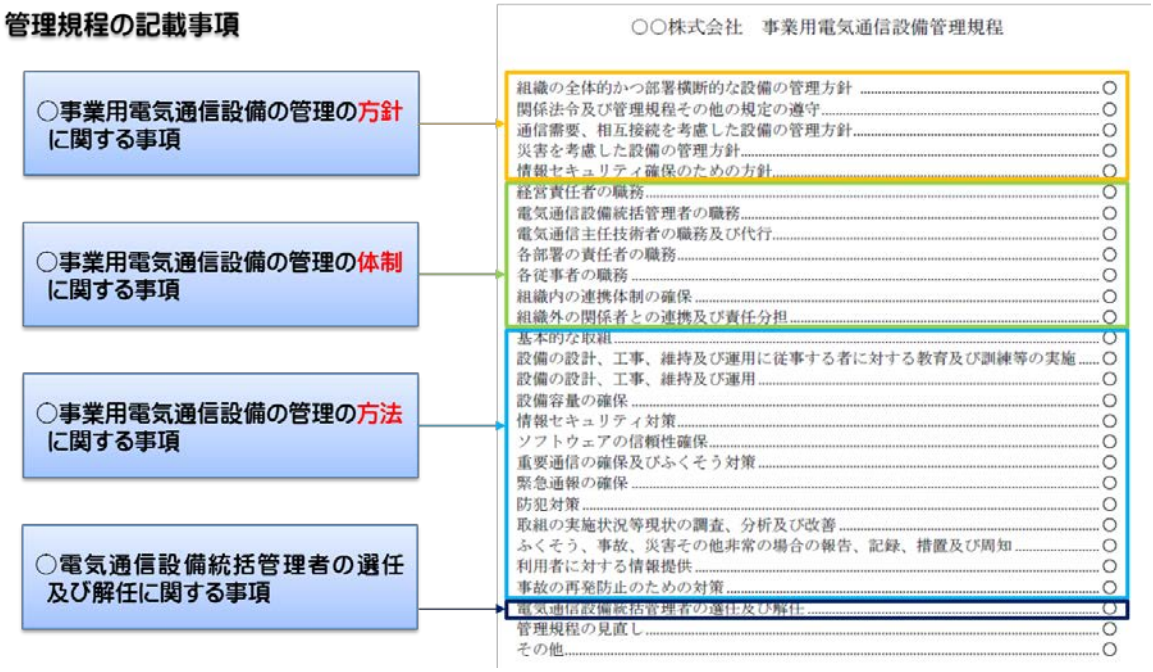


図 1.13　管理規程の記載事項

（５）　情報通信ネットワーク安全・信頼性基準

全ての電気通信事業者に対して、情報通信ネットワーク全体から見た安全・信頼性対策について網羅的に整理、検討を行い、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持・運用等を総合的に取り入れた、安全・信頼性に関するガイドライン（「情報通信ネットワーク安全・信頼性基準」（昭和 62 年郵政省告示第 73 号））を策定している（概要は図 1.14 のとおり）。

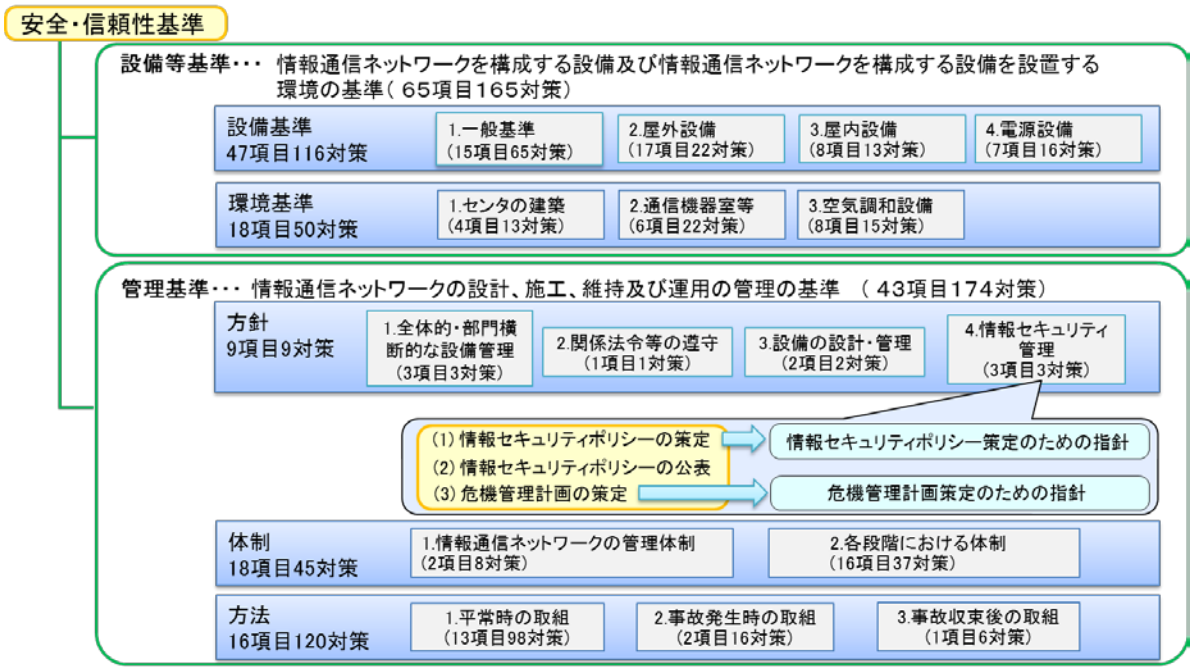


図 1.14　情報通信ネットワーク安全・信頼性基準

（６）　電気通信設備統括管理者

技術基準適合維持義務が適用される電気通信事業者に対しては、経営陣の事故防止の取組に関する認識の向上や関与の強化を図るため、図 1.15 の要件を満たす管理的地位にある責任者である「電気通信設備統括管理者」の選任を義務付けている。設備管理の専門化・細分化や外部委託等が進む中で、社内・社外の全体調整を含め、事故防止の方針・体制・方法への経営陣の主体的関与を強化し、「管理規程」等に基づく事故防止の取組の実効性を確保している。

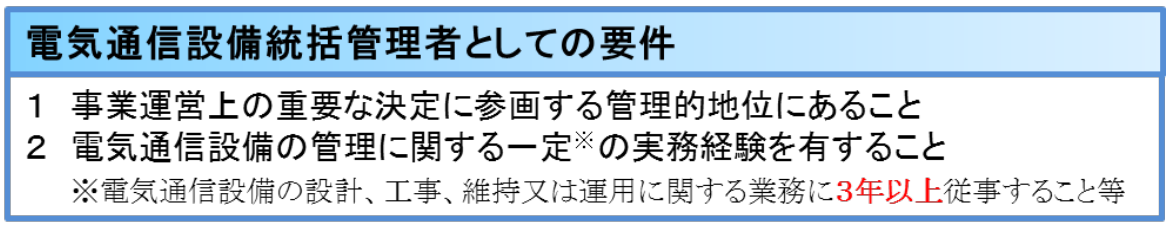


図 1.15　電気通信設備統括管理者としての要件

（７）　電気通信主任技術者資格

技術基準適合維持義務が適用される電気通信事業者に対しては、事業用電気通信設備の工事・維持・運用に関する事項を監督する電気通信主任技術者の選任義務が課されている。ただし、その事業用電気通信設備が小規模であって、一定の

条件を満たしている場合等はこの限りではない。電気通信主任技術者は電気通信主任技術者資格者証を持つ者の中から選任する必要があり、図 1.16 のとおりネットワークを構成する設備に着目して資格が区分されている。

資格区分	監督の範囲
伝送交換	事業用電気通信設備のうち、伝送交換設備及びこれらに附属する設備の工事、維持及び運用
線路	事業用電気通信設備のうち、線路設備及びこれらに附属する設備の工事、維持及び運用

図 1.16　電気通信主任技術者の資格区分と監督の範囲

（８）　工事担任者資格

電気通信事業法では、利用者が端末設備又は自営電気通信設備を事業者の電気通信回線設備に接続するとき、これに係る工事を工事担任者に実施又は実地で監督させなければならないとされている。工事担任者は、接続及びこれに伴う調整、並びに屋内配線の設置工事など端末設備等の接続により通信が可能となる一切の工事について責任を負うことになる（ただし、適合表示端末機器等の接続の方式が告示で定めるプラグジャックや電波等の方式であるときには、工事担任者による接続の工事は不要）。

工事担任者資格は、図 1.16 のとおり工事を行う範囲に応じて資格が区分されている。

資格区分	工事の範囲
AI第一種	アナログ回線及びISDN回線に端末設備等を接続するための工事全て
AI第二種	50回線（内線200回線）以下のアナログ回線及び64kbps換算で50回線以下のISDN回線に端末設備等を接続するための工事
AI第三種	1回線のアナログ回線及び基本インターフェースが1回線のISDN回線に端末設備等を接続するための工事
DD第一種	デジタル回線（ただしISDN回線を除く）に端末設備等を接続するための工事（以下、DD種の工事）全て
DD第二種	DD種の工事の内、100Mbps以下（ただしインターネット接続工事の場合は1Gbps以下）の工事
DD第三種	DD種の工事の内、1Gbps以下のインターネット接続工事
AI・DD総合種	アナログ回線及びデジタル回線に端末設備等を接続するための工事全て

図 1.17　工事担任者の資格区分と工事の範囲

（９）　電気通信事故の報告

電気通信事業は、社会経済活動に不可欠なサービスを提供する公共性の高い事業であり、継続的・安定的なサービス提供が求められる。そのため、全ての電気通信事業者に対し、一定の規模を超える事故が生じたときは、重大事故として総務大臣への報告義務を課しており、総務省において、必要に応じて再発を防止するための適切な措置を講ずることとしている。

総務省への報告義務のある電気通信事故は、次の二つに大別される。

① 重大な事故（サービスごとの影響利用者数・継続時間の基準（図 1.18）に該当する事故）
　－事故後３０日以内に報告書を提出

② 四半期報告事故（「影響利用者数３万人以上」又は「継続時間２時間以上」の事故）
　－四半期ごとに報告

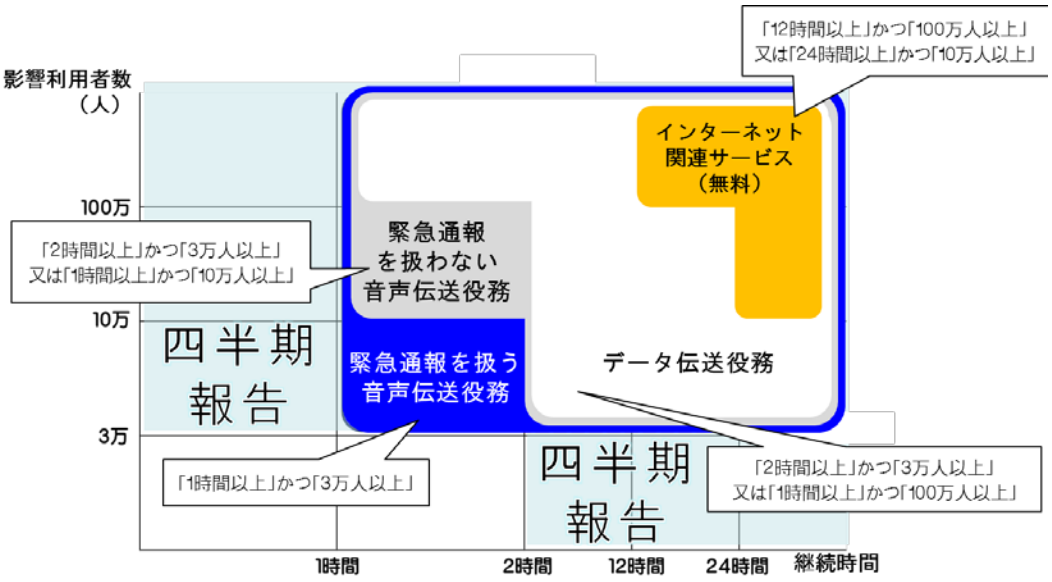


図 1.18　重大な事故の基準

第２章　IoT 機器等の電気通信設備の技術的条件

2.1　検討課題

本報告では、「IoT 機器等の電気通信設備の技術的条件」として、以下の２点を取りまとめた。

①LPWA サービス用電気通信設備の技術基準の適用について

②IoT 機器を含む端末設備のセキュリティ対策について

2.2　LPWA サービス用電気通信設備の技術基準の適用について

2.2.1　検討の目的等

現在、LoRa 等の IoT サービス用の新しい無線通信技術である LPWA（Low Power Wide Area）を活用したサービス（以下「LPWA サービス」という。）が進展しつつある。LPWA サービスは、図 2.1 のように携帯電話サービス等の事業用電気通信設備と比較して、極めて簡易な設備のみを設置して電気通信役務を提供することが可能となっており、今後、こうした LPWA サービスを提供する電気通信事業者が増加していくことが想定される。

このような簡易な設備を用いて LPWA サービスを提供する場合において、サービス展開の自由度を確保しつつ、ネットワークの安全・信頼性を確保するための対策について検討を行った。

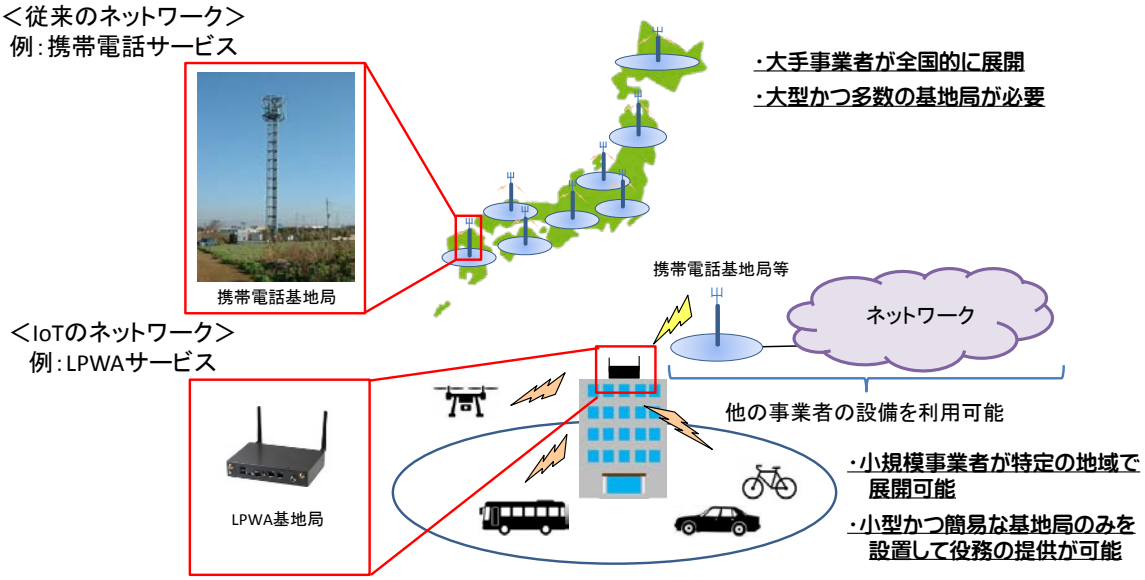


図 2.1　従来のネットワークと IoT のネットワークとの比較

今後、様々な LPWA サービスが提供されると見込まれる中、技術基準の検討に当たっては、用途、通信頻度、機器数、事故の際の影響度等について、LPWA の特性を十分に考慮することが必要である。

特に、クラウド技術を活用した ICT サービスが普及する中、クラウド設備に故障等が発生し、それらの設備により実現しているコアネットワークに障害が発生した場合には、そのサービス提供に重大な支障を及ぼすこととなる。このようなクラウド技術を活用したコアネットワークの全部又は一部について、他事業者から卸電気通信役務を受けてサービスを提供するケースが今後増加すると想定される。こうした点を踏まえ、LPWA サービス用の電気通信設備に対して現行の技術基準を適用することについて考え方を整理した。

更に、クラウド上の通信機能を利用し、図 2.1 のように携帯電話基地局等について他事業者から卸電気通信役務を受けて役務を提供する LPWA サービスは、極めて簡易かつ無線局免許を要しない設備（例：図 2.1 の「LPWA 基地局」）のみを自ら設置してサービス提供することも可能である。そのようなケースでは、設備の故障等が発生し

たとしても、復旧が容易であると考えられることから、その点を踏まえて電気通信主任技術者の資格者の配置要件についても検討を行った。

図 2.2　LPWA サービスの活用分野
（第 35 回委員会　京セラコミュニケーションシステム説明資料より抜粋）

また、LPWA は、アンライセンスバンドを利用しており、様々なシステムが周波数を共用することから、無線環境が変化することなどにより通信が行えなくなるなど、意図しない障害が発生する場合がある。

さらに、IoT デバイスの要件によって求められる品質レベルが異なるため、例えば、LPWA 事業者において、提供するサービスに適した用途などを SLA(Service Level Agreement：サービス品質保証)化して提供することや、セキュリティ等のオプションの選択肢を提供すること、さらには、利用者側においてデータの再送を行うことにより品質を確保することが有効なケースもある。

2.2.2　検討結果

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には、図 2.3 の構成例のように、(a)クラウド事業者が提供するハードウェアや OS 等（以下「プラットフォーム」という。）を利用して LPWA 事業者が自らクラウド上の通信機能を実装して役務を提供するケースと、(b)他の事業者がクラウド上で提供する通信機能を利用して役務を提供するケースが想定される。いずれのケースにおいても、センサー情報等を集約するクラウド設備に故障があった場合、その役務の提供に重大な支障を及ぼすこととなる。そのため、LPWA サービスを提供する事業者に対し、以下のアからエまでに掲げる技術基準を適用することが適当である。

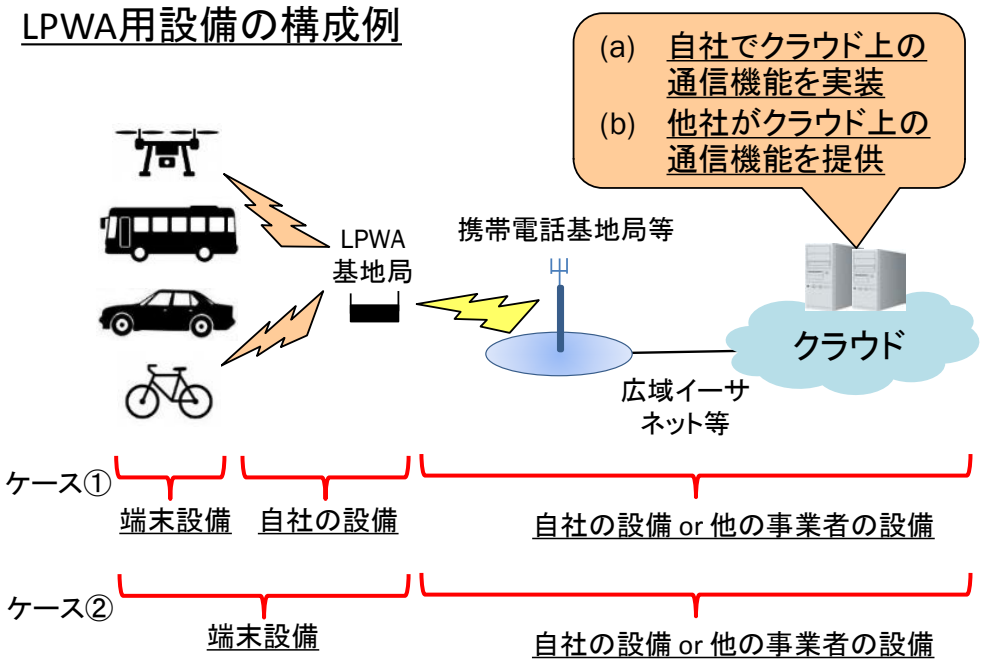


図 2.3　LPWA 用設備の構成例

ア　クラウド事業者が提供するプラットフォームを利用して LPWA 事業者が自らクラウド上の通信機能を実装して役務を提供する場合（(a)の場合）、責任の分界や技術基準の適用については以下の通りとすることが適当。

- クラウド上の通信機能を実装する LPWA 事業者は、当該通信機能に関し、事業用電気通信設備に係る技術基準に適合する必要がある。
- 異常ふくそう対策や設備の分散設置等については、物理的な設備の増強や複数設置等の従来の方法に加え、クラウド事業者が提供するプラットフォームの機能を活用することが可能。
- 電源停止の検知等の措置については、クラウド事業者において対応していることを LPWA 事業者が確認することが必要。

イ　他の事業者がクラウド上で提供する通信機能を利用して役務を提供する場合（(b)の場合）は、当該他の事業者が技術基準に適合していることを LPWA 事業者において確認することが適当。また、クラウド上の通信機能に異常があった場合に、LPWA 事業者において検知できるようにすることが適当。

ウ　クラウド上の通信機能を利用する LPWA サービスのうち、簡易かつ無線局免許を要しない設備のみを自ら設置して提供するサービスについては、設備の故障等が発生したとしても、遠隔からの操作による復旧や資格者によらない簡易な工事等により容易に復旧できると考えられる。このような場合については、アクセスポイントのみを自ら設置して公衆無線 LAN アクセスサービスを提供する場合と同様に、電気通信主任技術者の都道府県ごとの選任を要しないとすることが適当。

エ　LPWA 基地局に使用する機器は、サービスの提供形態によって端末設備にも事業用電気通信設備にもなり得るが、その場合の技術基準の適用については、設置方法に応じて端末設備又は事業用電気通信設備の技術基準を適用することが適当。

2.3　IoT 機器を含む端末設備のセキュリティ対策について

2.3.1　検討の目的等

近年、Web カメラやルータ等の IoT 機器が乗っ取られ、インターネットに障害を及ぼすような DDoS 攻撃等のサイバー攻撃に悪用される事案が増加している。

一方、情報通信ネットワークの安全・信頼性を確保するために、電気通信事業法においては、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさない等を原則とする端末設備の接続の技術基準が定められている。

委員会では、そのような制度の枠組みの中で、大規模 DDoS 攻撃等のサイバー攻撃を抑止するため、IoT 機器を含む端末設備がマルウェアに大量感染しないこと等を目的とするセキュリティ対策を技術基準に追加することについて検討を行った。

2.3.2　検討結果

（１）端末設備の接続の技術基準にセキュリティ要件を追加する必要性について

近年増加しているマルウェア「Mirai」等による大規模 DDoS 攻撃を抑止するためには、攻撃の踏み台となる IoT 機器がマルウェアに大量感染しないような対策を取ることが重要である。

大規模 DDoS 攻撃については、電気通信事業者による対応が期待されることは言うまでもない。しかしながら、電気通信事業者は、電気通信事業法第 4 条に基づき、その取扱中に係る通信の秘密は侵してはならないとされていることから、原則として、通信内容を確認することは不可能である。このため、仮に IoT 機器からの大量通信が発生した場合であっても、通信内容を確認して正常な通信なのか、DDoS 攻撃に加担しているものであるか判別することができない。また、マルウェア感染した IoT 機器のみの通信を止めることについても、技術面から困難であるため、電気通信事業者が取り得る対応も制約がある状況となっている。

なお、本年５月に成立した「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」により、電気通信事業者によるセキュリティ対策を強化するため、電気通信事業者による情報共有体制などの新たな取組みが導入されることとなっている。

- 2016年10月 米国Dyn社のサービスを標的とした大規模DDoS攻撃が発生
- TwitterやSpotify、Netflix、WSJなどの大手サイトがアクセスしにくくなる事象が発生。
  米国を中心に約6時間にわたってサービスが利用できなかった。
- 本攻撃は電子機器メーカーHangzhou Xiongmai Technologyの防犯カメラ（DVR）やIPカメラなど10万台以上のIoT機器の脆弱性を悪用し感染させたMiraiと名付けられたマルウェアからの悪性通信によって引き起こされた。
- Mirai系マルウェアに感染しているIoT機器は、主に工場出荷時のID/パスワードを使っており簡単に感染させられるものであることが指摘されている

攻撃概要 (出典) Cyber Attack dot Net


感染地域 (出典) Downdetector

- 2016年11月には英国人男性ハッカー(逮捕済み)によってドイツテレコムが各家庭に設置したルータ約90万台にMirai型マルウェアの感染を狙ったサイバー攻撃が行われる。顧客のサービスに障害が発生。ネットにアクセスできないなどの影響が出た。
- 2017年10月スウェーデンの交通機関や当局のネットワークを提供しているISPであるTDCとDGCへの大規模DDoS攻撃が発生。
  - 列車運行を管理する産業省交通局のシステムが麻痺。列車の運行停止や遅延が発生。
    列車遅延は一日中続いた。
  - サイトやメールシステムもダウンしたため、遅延情報も通知できなかった。交通局では局員個人のFacebookアカウントで乗客に情報提供を実施するなど混乱が発生した。

図 2.4　IoT 機器を感染対象としたマルウェア：Mirai
（第 36 回委員会　ICT-ISAC 説明資料より抜粋）

大規模 DDoS 攻撃に対処する上では、IoT 機器の利用者における対策も重要である。しかしながら、例えば機器メーカ等がソフトウェアの更新を呼びかけたとしても、技術的に対策が難しい等の理由で全ての利用者に対応を求めることは容易ではない。

また、IoT 機器が目的どおり動作している限り、そもそも利用者は攻撃の踏み台となっていることを認知することが難しいという課題も存在する。

実際に過去の事例では、利用者に注意喚起を行った後、脆弱性のある機器の約 8 割に対処が行き届くのに約３年を要したものもあった。

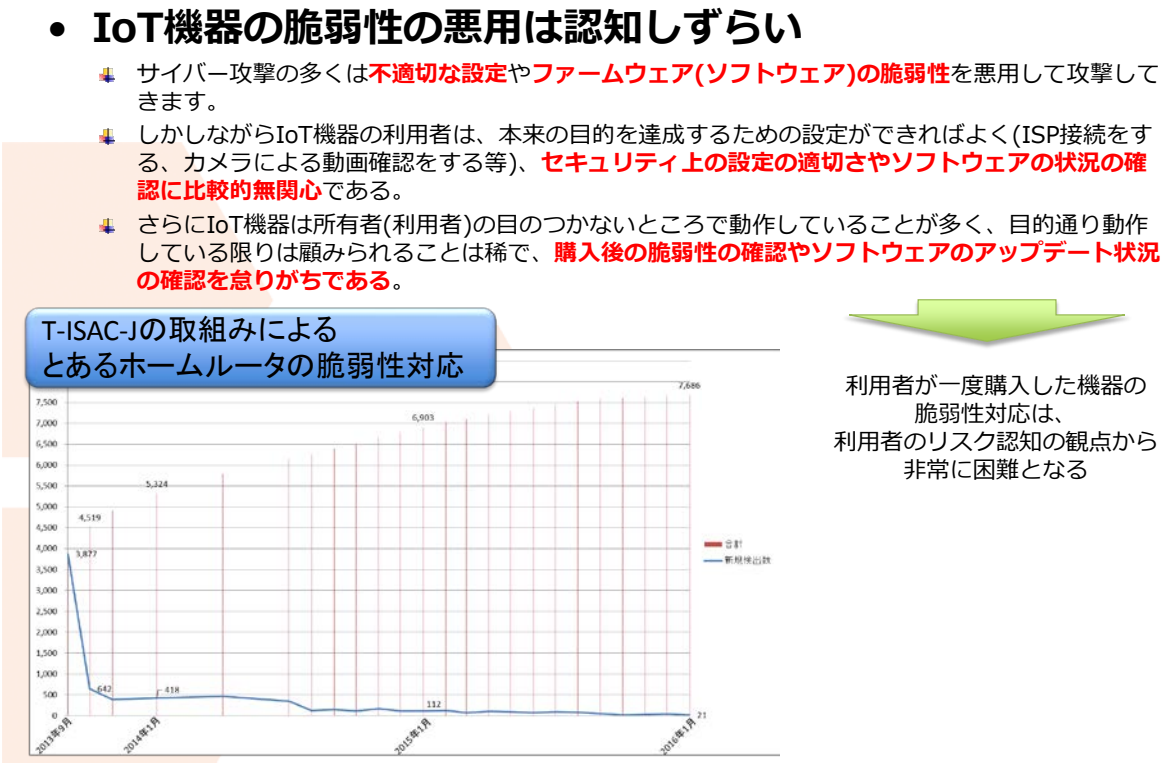


図 2.5　IoT 機器のセキュリティ上の問題
（第 36 回委員会　ICT-ISAC 説明資料より抜粋）

一方、現在の IoT 機器に対するサイバー攻撃は、グローバル IP アドレスを有する機器を対象として、セキュリティ上の不適切な設定や利用者に認知されていない脆弱性等を悪用したサイバー攻撃が多い。平成 28 年 10 月に、米国を中心に大手インターネットサービスの障害を引き起こしたマルウェア「Mirai」の事例では、本来不要な通信機能のアクセス制御のため、主に工場出荷時の ID/パスワードをそのまま使用していた IoT 機器が数多く乗っ取られ、大規模 DDoS 攻撃が行われた。このような事例でも、IoT 機器において比較的な簡易なセキュリティ対策を行うことで大半の攻撃を防ぐことが可能である。

また、アクセス制限がない機器、ハードコーディングされた ID/パスワードを持っている機器、既知の脆弱性が埋め込まれている機器等が出荷された場合には、その脆弱性を事後に修正することは困難なものとなる。そのため、出荷前に必要な対策を講じることが有効であると考えられる。

これらを踏まえると、IoT 機器を含む脆弱な端末設備に対するセキュリティ対策として、電気通信事業法の枠組みの中で、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさないといった端末設備の接続の技術基準の原則の範囲内において、その技術基準にセキュリティ要件を追加することが適当である。

なお、当該セキュリティ要件は、IoT 機器のマルウェア大規模感染を防止することを目的としているものである。IoT セキュリティを確保するためには、これらの対策だけでは不十分であり、IoT 機器が使用される分野や用途に応じたガイドラインに基づくセキュリティ対策や、利用者等への周知啓発など総合的な対策が必要である。そ

れらについてはIoT推進コンソーシアム等の場において引き続き検討され、必要な対策が実施されていく必要がある。

（２）IoTセキュリティ対策に関する国内外の動向

IoTセキュリティ対策については、現在、欧米等においても議論が活発に行われているところである。

米国においては、「ボットネット等の脅威に対するインターネットの強固性と通信のエコシステムの強化」に関する報告書が取りまとめられた。当該報告書では、IoTセキュリティに関し、初期設定及び自動ソフトウェアの更新機能などの重要性を指摘するとともに、機器の大半は国外に存在するため、国際的に認められた標準に基づくセキュリティの向上が重要であるとして、今後、具体的な施策の検討が行われていくことが見込まれる。

一方、欧州においては、ICT機器やサービスに対し、既知の脆弱性を含まないソフトウェアが提供され、安全にソフトウェア更新がおこなわれることを保証すること等を目的として、「ICTサイバーセキュリティ認証に関する規則案」が公表され、引き続き欧州議会で検討が行われているところである。

機器を対象としたセキュリティ認証に係る国際標準については、政府調達機器の一部に関し、国際標準ISO/IEC15408に基づくCC(Common Criteria)認証が行われている。CC認証は、世界28カ国で受け入れられている認証制度であり、複合機の例では、他の利用者による不正な操作や通信データの盗聴・改ざん、管理機能への不正なアクセス等を脅威として想定し、識別・認証・権限付与やアクセス制御、ファームウェアに電子署名を付すといった高信頼な通信等のセキュリティ機能を保証するとともに、セキュリティ機能自体の脆弱性評定も実施している。

IoTセキュリティ対策に関する国際標準は、ISO/IEC JTC1/SC27において検討が開始されたところであり、現時点で確立しているものではない。しかし、IoTのグローバル市場への展開や国際競争力確保といった観点から、CC認証をはじめとした国際標準との整合性を図るとともに、今後も、国際的な動向の把握に努める必要がある。

また、日本からは現在、IoT推進コンソーシアムにおいて定められた「IoTセキュリティガイドライン ver1.0」の内容について国際標準の議論の場に提案が行われているところであり、今後も積極的に我が国の取組みを発信していくことが重要である。

（３）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

これまで述べてきたようなIoT機器に対するサイバー攻撃等の現状や国内外の動向等を踏まえると、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は、インターネットプロトコルを使用する端末設備であって、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について、大量感染を防ぐための最低限のセキュリティ要件として、アクセス制御機能、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及び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を具備することを要件とすることが適当である。また、具体的な機能については、表2.1のとおりとすること

が適当である。

表 2.1 端末設備に最低限必要なセキュリティ要件の具体的な機能

セキュリティ要件	具体的な機能
アクセス制御機能	・電気通信回線設備を介して接続されることにより当該端末が不正に操作されないことを目的として、当該操作の前にアクセス制御を行うことが必要。
アクセス制御の際に使用する ID/ﾊﾟｽﾜｰﾄﾞの適切な設定を促す等の機能	・アクセス制御を識別符号によって行う場合は、当該識別符号が他人から容易に推測できないものとして設定されることを目的として、当該端末の利用者に対し当該識別符号について初期値の変更を促す（二以上の識別符号の組み合わせによるものの場合は少なくとも一つの識別符号が対象。以下同じ。）若しくは識別符号の初期値について機器毎に別のものを付す、又はそれらに準じる措置を行うことが必要。
ファームウェアの更新機能	・端末に記憶されている当該電気通信の送受信の機能に係るソフトウェアの更新が可能であることが必要。当該更新は安全かつ自動で行われることが推奨されるが、IoT 機器は多種多様であり、更新の手法は機器の種別毎に異なることから、安全かつ自動の更新までは要件とはしない。 ・端末への電力供給が停止した場合であっても、当該更新されたソフトウェアや変更されたアクセス制御の設定内容を維持することが必要。
同等以上の機能	・CC 認証などの国際標準に基づくセキュリティ認証を取得した複合機など、上記の機能と同等以上のセキュリティ機能を有すると認められるものについては、当該セキュリティ要件を満足するものとみなす。

なお、PC やスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能であり、それにより上記セキュリティ要件に関する機能が出荷時とは異なるものになることが想定される機器については、当該セキュリティ要件を適用することが馴染まないことから、本要件の規定の対象外とすることが適当である。しかしながら、その場合においては、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。

（４）技術基準適合認定等の対象機器の範囲

セキュリティ要件が追加された技術基準に関し、当該技術基準適合認定等を求める端末機器の範囲については、インターネットプロトコルを使用する全ての機器に対し、セキュリティ対策を求めることが理想的ではあるが、より効率的かつ効果的な対策とするため、セキュリティ対策を行うことが効果的な機器の範囲を明確にすることが適

当である。

マルウェアに感染している IoT 機器に関する研究では、感染機器の９割以上が不明であるものの、判明している範囲では海外製品のインターネットカメラ、デジタルビデオレコーダ、ルータ等が多い。国内製品においても、ルータ、ゲートウェイ、ネットワークストレージ、太陽光パネル管理システム、電力デマンド監視システムといった機器に感染事例が見つかっているという報告がなされている。

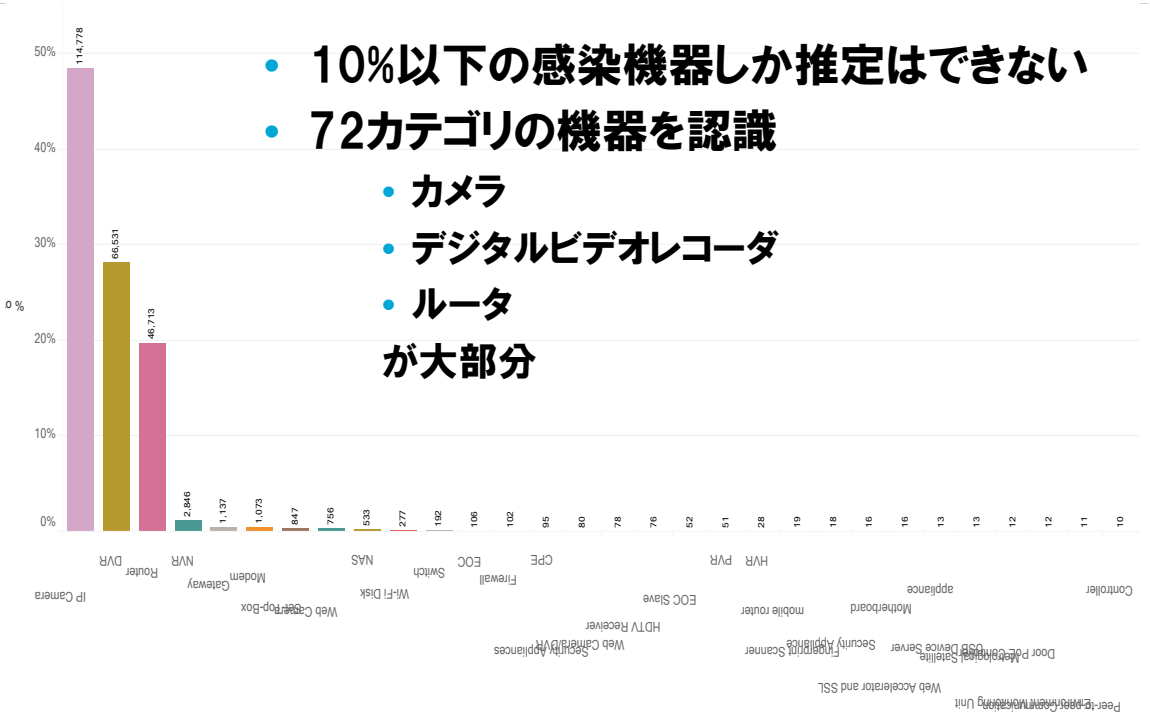


図 2.6　ハニーポットで観測された感染機器の種類
（第 37 回委員会　吉岡オブザーバ説明資料より抜粋）

現在の IoT 機器に対するサイバー攻撃は、グローバル IP アドレスを有する機器へのインターネット側からの直接的攻撃が主流であり、ルータ等の直接接続される機器に感染した後、更に家庭内の機器にまで感染活動を行うものは５%程度という分析事例 [1]がある。そのため、インターネット側からアクセスし操作可能なネットワークサービス（Web 管理、telnet 等）を使用する機器については、特に脆弱性対策が必要と考えられる。

現状の技術基準適合認定等は、基本的に電気通信回線設備に直接接続される端末機器を対象に実施しているが、上記を踏まえれば、現状においてネットワーク側からサイバー攻撃を受けた際に乗っ取られるリスクが特に高いのは、電気通信事業者の電気通信回線設備に直接接続される端末機器であることから、セキュリティ要件が追加された技術基準適合認定等の対象についても、従来と同様に電気通信回線設備に直接接続される端末機器とすることが適当である。

[1]熊佳、楊志勇、鉄穎、中山颯、江澤優太、藤田彬、吉岡克成、松本勉、″実攻撃の観測と疑似攻撃の試行に基づくホームネットワークセキュリティ評価フレームワークの検討,″ 2018 年暗号と情報セキュリティシンポジウム, 2018.

その際、直接接続される機器とは、電気通信回線設備に物理的かつ技術的に直接接続可能な端末機器を指すが、その中でも恒常的に既認定機器を介して接続する機器（屋外に持ち出す等により電気通信事業者の回線設備に直接接続して使用することを全く想定していない機器(例：大型白物家電等）)については、今後、技術基準適合認定等の対象外とすることが適当である。

この場合、利用者が認定等を取得していない機器を誤って直接接続しないようにするため、例えば、取扱説明書等において、①当該機器は既認定機器に接続する必要があることや、②電気通信事業者の電気通信回線設備に直接接続する場合には、電気通信事業者による検査が義務付けられていることを記載すること等をガイドライン等により明示することについて検討する必要がある。

また、認定等を取得していない機器の乗っ取りを防ぐためには、IoT 機器メーカやIoT システム/サービス提供者等において、IoT 推進コンソーシアムにおいて定められた「IoT セキュリティガイドライン ver1.0」等に基づき、直接接続される既認定機器における対策も含む適切なセキュリティ対策を検討・実施する必要がある。

今後、端末機器の接続が多様化することが想定されるが、認定等が必要な機器の範囲等については、機器メーカ等が判断できるように、ガイドライン等により明示することについて速やかに検討を開始する必要がある。

（５）セキュリティ要件の追加に係る経過措置

端末設備の接続の技術基準へのセキュリティ要件の規定の追加が制度化された場合には、IoT 機器メーカや登録認定機関等の対応を考慮して、一定の期間を設けて施行することとなるが、その期間は 1 年から 2 年程度とすることが適当である。

また、従来の制度に基づき、新制度の施行前に取得した技術基準適合認定等については、施行後も引き続き有効であり、当該認定等に基づく機器も引き続き使用することを可能とすることが適当である。

（６）技術基準適合認定等の審査方法等

登録認定機関等による技術基準適合認定については、セキュリティ要件の対象となる機器の審査が円滑に行われるよう、その審査方法や機器の審査単位等について通信事業者、機器メーカ等が参画可能な場で別途議論を行うことが適当である。

また、利用者にとっては、ファームウェアの更新や ID/パスワードの設定方法が難しい場合があることから、利用者向けのマニュアルに係るガイドラインを検討していくことも重要である。

こうした利用者向けのマニュアルに係るガイドラインのほか、技術的に詳細な検討が求められる審査に係る試験方法等については、民間標準化機関等が中心になって国際標準化も見据えながら検討を行っていくことが重要である。

第３章　IoT 時代における重大事故に関する事故報告等の在り方

3.1　検討課題

本報告では、「IoT 時代における重大事故に関する事故報告等の在り方」として、以下の４点を取りまとめた。

①LPWA サービスの事故報告基準について

②大規模なインターネット障害発生時の障害情報の共有について

③大規模なインターネット障害に関して電気通信事業者等に推奨する対策について

④電気通信事故報告制度に係るその他の対策について

3.2　LPWA サービスの事故報告基準について

3.2.1　検討の目的等

LoRa 等に代表される IoT 向けの無線通信技術（LPWA）は IoT 時代のネットワーク技術として注目され、その進展が期待されている。一方、LPWA サービスにおいては、従来の電気通信事故と異なる特徴を持つ事故が発生、拡大する可能性が指摘されている。

電気通信事業法の事故報告制度においては、電気通信役務の区分ごとに重大な電気通信事故の発生について報告を求める基準を定めている。LPWA サービスに対して、現行の制度を適用すると、①二時間以上電気通信役務の全部又は一部の提供を停止又は品質を低下し、その影響利用者数が三万以上の事故の場合、又は、②一時間以上電気通信役務の全部又は一部の提供を停止又は品質を低下し、その影響利用者数が百万以上の事故の場合について、重大事故として報告を求めることとなる。

一方、LPWA サービスは現時点では主に、相当数のセンサー端末等を用いた状態監視に利用されることが想定されており、その通信頻度は分野によって様々であり、中には数時間おきに低頻度の通信を行うものも存在する。また、相当数のセンサー端末等が接続されて一つのサービスが提供されるケースが多いことから、現行の事故報告制度の基準に基づいて一律に重大事故の報告を求めると、事故の内容によっては影響を受ける利用者の感覚と制度上の取り扱いにギャップが生じる可能性がある。

上記を踏まえ、LPWA サービスの特徴を勘案し、事故報告基準の検討を行った。

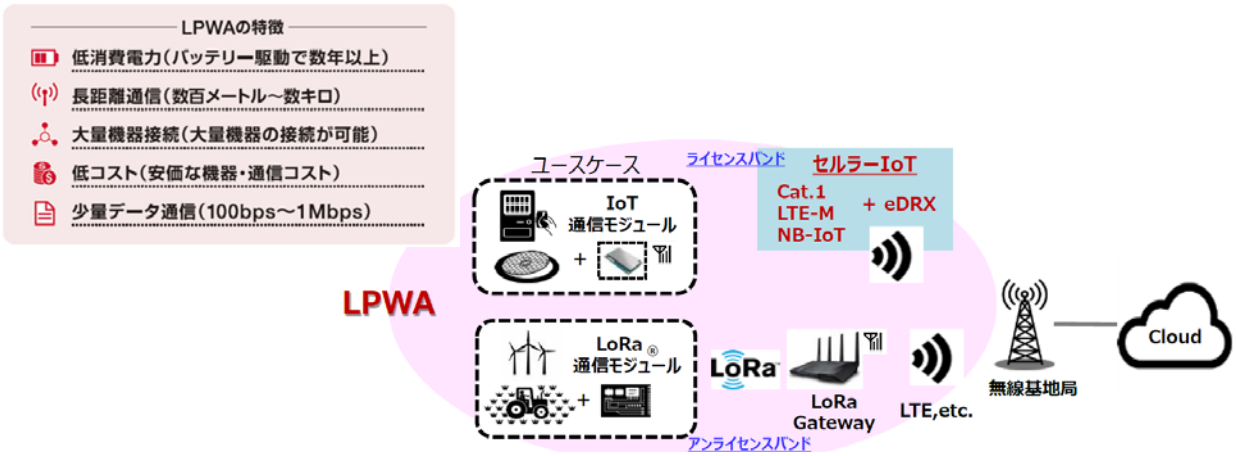


図 3.1　LPWA の特徴等
（第 35 回委員会　NTT ドコモ説明資料より抜粋）

3.2.2　検討結果

（１）　LPWA サービスのネットワーク構成及び事故報告の対象範囲

LPWA サービスは、図 3.2 のようにアンライセンスバンドの電波を使用する無線局の無線設備（LoRa, SIGFOX 等）を各センサー機器等が行う通信のゲートウェイとして用いて提供されるもの（アンライセンス系）と、携帯電話用の電波（NB-IoT, eMTC 等）を使用して、各センサー機器等と携帯電話基地局が直接データを送受信する形で提供

されるもの（セルラー系）がある。事故報告基準の検討に際して、これらのネットワーク構成を踏まえ、事故報告の対象範囲の整理を行った。

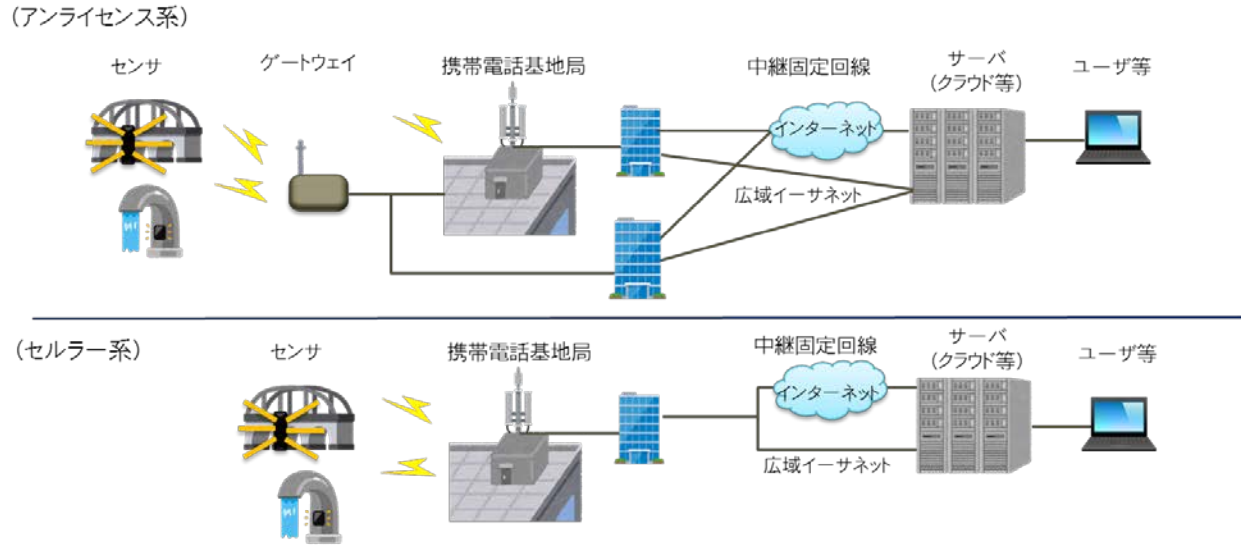


図 3.2　LPWA サービスのネットワーク構成イメージ

LPWA サービス（セルラー系）は、携帯電話アクセスサービスの提供事業者が携帯電話用の電波を用いて、利用者のセンサー機器等から、インターネットや広域イーサネットまでの通信を提供し、センサー機器等からのデータを蓄積するクラウドサーバ等との通信を可能とするサービス形態が考えられる。

このサービス形態においては、当該事業者は、携帯電話アクセスサービスの範囲内で LPWA サービスを提供することが想定され、LPWA サービスの事故が発生した場合、携帯電話アクセスサービスとの切り分けは困難と考えられる。

そのため、図 3.3 のとおり、既存の電気通信役務の基準に沿って事故報告を求めることが適当と考えられる。

なお、LPWA サービスの事故が発生した場合において、既存の電気通信役務との間で切り分けが可能な場合であって、契約単位（後述の（２）（ア）の検討結果に基づく。）で通信の管理が可能な場合は、LPWA サービスの事故報告を求めることが適当と考えられる。

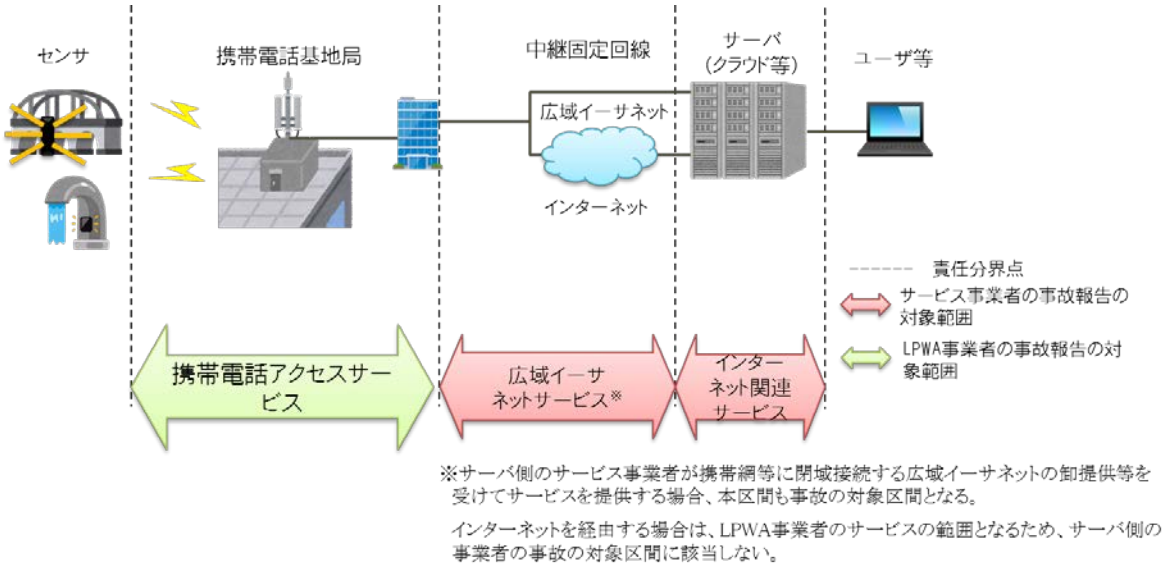


図 3.3　LPWA サービス（セルラー系）の事故報告範囲

次に、LPWA サービス（アンライセンス系）については、主に

①LPWA 事業者がゲートウェイを設置し、携帯電話アクセス区間や中継固定回線区間については卸提供等を受けて、センサー機器等からのデータを蓄積するクラウドサーバ等までの通信を一体で提供する場合

②LPWA 事業者がゲートウェイを設置し、LPWA サービス利用者がインターネット接続回線等を用意することで、クラウドサーバ等との通信を提供する場合

③LPWA サービス利用者がゲートウェイを設置し、LPWA 事業者がクラウドサーバ等までの通信を一体で提供する場合

④LPWA サービス利用者がゲートウェイを設置し、インターネット接続回線等を用意することで、LPWA 事業者がクラウドサーバ等との通信を提供する場合

の４つのサービス提供形態が考えられる。

本サービス形態においては、LPWA 事業者がクラウドサーバ等を管理し、LPWA サービスを提供することが想定され、LPWA サービスの事故が発生した場合、既存の電気通信役務との間で切り分けが可能と考えられる。その場合であって、契約単位の通信の管理が可能な場合は、図 3.4 のとおり LPWA サービスの事故報告を求めることが適当と考えられる。なお、そうでない場合は、既存の電気通信役務の基準にそって事故報告を求めることが適当と考えられる。

また、センサー端末等からゲートウェイの区間においては、アンライセンスバンドを利用するため、意図しない障害が必然的に発生することから、それによって、センサー端末等との通信が遅延等した場合は事故の対象外とすることが適当と考えられる。

なお、ゲートウェイの設備故障によってセンサー端末等との通信が停止した場合は事故の対象となることから、そういった事態を防止するため、ゲートウェイを複数設置することにより一部のゲートウェイの故障が生じた場合でも他のゲートウェイを通じて通信を行えるよう対策することが有効と考えられる。

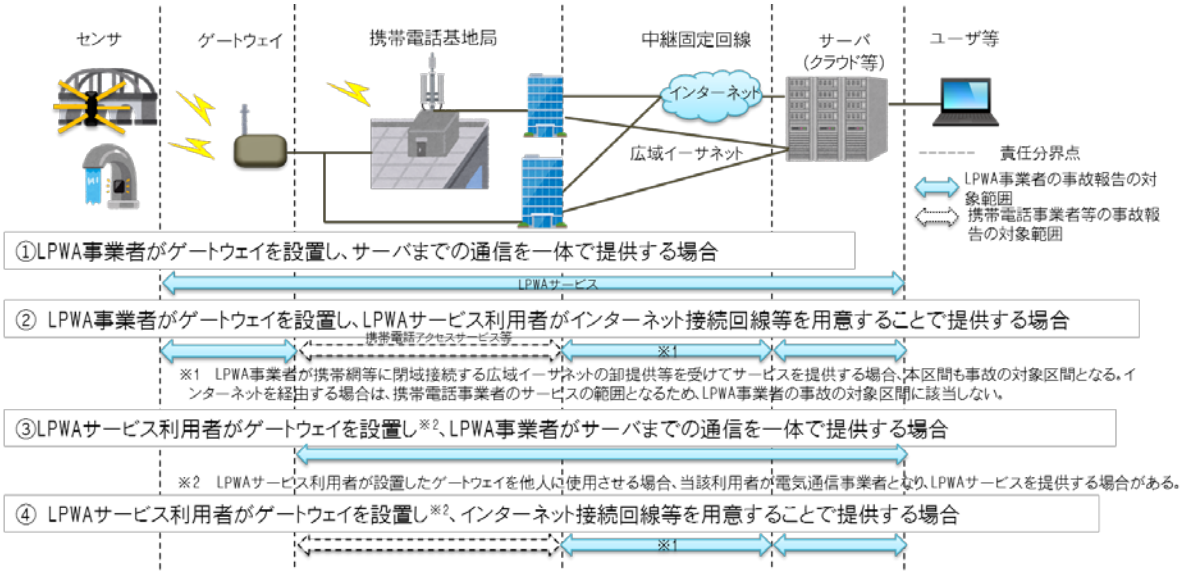


図 3.4　LPWA サービス（アンライセンス系）の事故報告範囲

（２）　LPWA サービスの事故報告基準

（ア）　影響利用者数の考え方

事故報告基準は、事故の影響利用者数と継続時間から構成される。

一方、既存の電気通信役務の通信主体がヒトであることに対し、LPWA サービスの多くは M2M の通信であり、その通信主体がセンサー端末等のモノであることを踏まえ、LPWA サービスの事故報告基準における影響利用者数の取り扱いについて整理を行った。

LPWA サービスの契約は、相当数のセンサー端末等を接続するものであることや、現状では遠隔検針、設備の状態監視、交通監視、環境計測又はスマートハウス等の状態監視が主な用途であることに鑑みれば、個々のセンサー端末等の通信が停止する事態が LPWA サービス利用者に大きな影響を与えるとは考えにくい。そのため、個々のセンサー端末等へのアクセス回線の数を、影響利用者数としてカウントすることは適当ではないと考えられる。

また、LPWA サービスの普及に伴い、センサー端末等は膨大な数になっていくと想定されることから、アクセス回線毎の管理では LPWA 事業者側の負担も同様に増え、LPWA サービスの発展性や柔軟性を阻害する懸念がある。

以上を踏まえると、同一の目的で利用される複数のアクセス回線を束ねた契約単位で管理することが望ましく、事故が発生した場合においては LPWA サービスの事故報告基準における影響利用者数は、契約数をカウントすることが適切と考えられる。ただし、LPWA サービスと他の電気通信役務の影響利用者数を切り分けられない場合等においては、必ずしも契約数によるカウントを求めるものではない。

（イ）　継続時間の考え方

LPWA サービスの事故報告基準における継続時間を検討する上で、通信頻度を考慮することが適当であるものの、LPWA サービスの通信頻度は用途によって様々である。

現状においては、LPWA サービスは主に状態監視を目的として利用されている状況であるものの、将来的には高頻度の通信を前提とするサービスが普及する可能性がある。中でも日常生活に密接に関連する分野等においては、利用者数が相当規模になる可能性もあることから、事故が発生した場合の社会的影響に鑑みれば、迅速な復旧対応を促す基準についても併せて検討することが適当と考えられる。

このため、委員会では、LPWA サービス全般に対して共通的に用いられる基準を検討することとし、いずれのサービスの通信頻度も包含するものとすることが適当と考えられる。

なお、低頻度の通信を前提とするサービスについても、相当規模の利用者に影響を与える事故であれば迅速な復旧対応を行う必要があると考えられる。

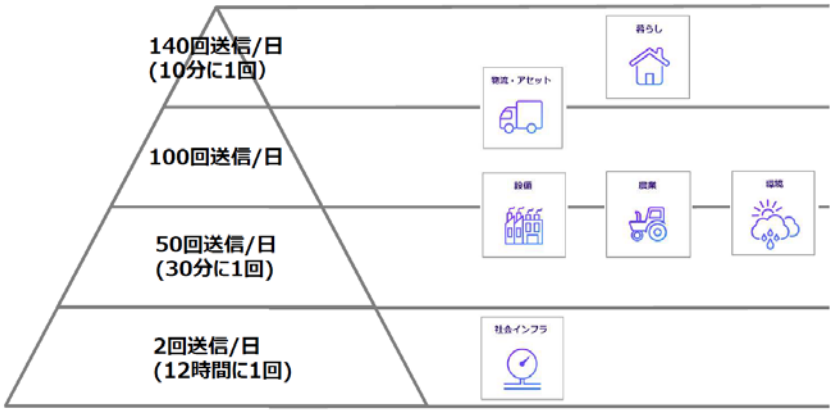


図 3.5　用途と通信頻度
（第 31 回技術検討作業班　京セラコミュニケーションシステム説明資料より抜粋）

（ウ）　LPWA サービスの事故報告基準

LPWA サービスは、図 3.5 のように現状では通信頻度が 12 時間に 1 回と低頻度のものも想定されることから、それらも含めた LPWA サービス全般の重大事故の共通的な基準としては、LPWA サービスの全部又は一部の提供を停止又は品質を低下させた事故が 12 時間以上継続するものであって、他の役務と同様に、3 万以上の利用者に影響を与えるものである場合に重大事故の報告を求めることが適当と考えられる。

一方、より頻度の高い通信を前提とする LPWA サービスについては、利用者数が相当規模になる場合には、より迅速な復旧対応が行われることが求められる。そのため、データ伝送役務の事故基準を踏まえるとともに、サービスの揺籃期であることを考慮し、事故が２時間以上継続し、100 万以上の利用者に影響を与えるものである場合に、重大事故の報告を求めることが適当と考えられる。

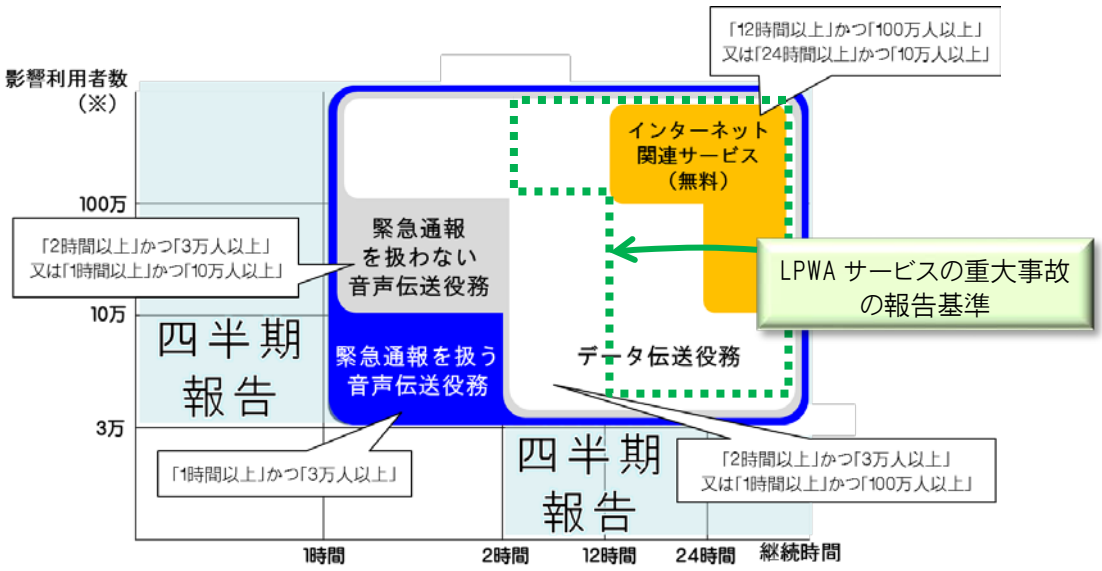
また、総務省においては、事故の発生原因等様々な切り口から統計分析を行うことを目的として、重大事故に至らない事故であっても一定規模以上であれば、四半期毎

の報告を求めている。役務に一定の信頼性を確保する観点からも、四半期毎の報告は有効と考えられることから、LPWA サービスについても他の役務と同様に、事故が 2 時間以上継続した場合、又は 3 万以上の利用者が影響を受けた場合に報告を求めることが適当と考えられる。

さらに、LPWA サービス提供事業者と接続する、あるいは卸電気通信役務を提供する中継系事業者が原因で事故が発生する場合においても、同様の基準を適用することが適当と考えられる。

なお、「電気通信事故に係る電気通信事業法関係法令の適用に関するガイドライン（第２版）」において、データ伝送役務（ベストエフォートサービス）における役務の提供の停止又は品質の低下に係る判断基準については、「利用者の端末機器等と事業者側の集線装置等との間でのリンク又はセッションが確立できない状態は、「役務の停止」とする」旨の記載があるものの、「品質の低下」に係る基準は設けられていないことから、LPWA サービスについても同様の整理とすることが適当と考えられる。

上記の LPWA サービスの事故報告基準は、今後のサービスの進展によって、電気通信事故の発生状況や影響度等を踏まえ、適宜、適切な時期に見直すことが重要である。



※　LPWA サービスの場合、影響利用者数は契約数を指す。

図 3.6　LPWA サービスの事故報告基準

なお、影響利用者数の算定については、実数による算定を基本とするが、困難な場合は、既存の電気通信役務の算出方法と同様に、事故の１週間前までのいずれかの日の同じ時間帯の利用者数等により合理的に算出することとする。

また、中継系事業者の影響利用者数の算定においては、現行の事故報告制度における考え方に基づき、LPWA 事業者の影響利用者数が把握できる場合には、その数で算定し、把握できない場合には LPWA 事業者の数をもって影響利用者数とすることが適当と考えられる。

（３）　その他の検討結果

バックエンド回線を卸提供する事業者など他の事業者に起因する事故が発生する可能性がある。その場合、復旧までの時間が長期化することが考えられる。

そのため、卸提供事業者等と LPWA 事業者の間で、障害発生時に障害の切り分けに必要な情報を共有する等の連携を図ることが重要である。

一方、LPWA サービスは揺籃期であり、電気通信事業者に推奨すべき事故対策を示すことが現時点では困難であることから、今後のサービスの発展状況を踏まえた上で、事業者間連携以外の他の対策も含めて、情報通信ネットワーク安全・信頼性基準等に規定すること等により推奨していくことが適当である。

3.3　大規模なインターネット障害発生時の障害情報の共有について

3.3.1　検討の目的等

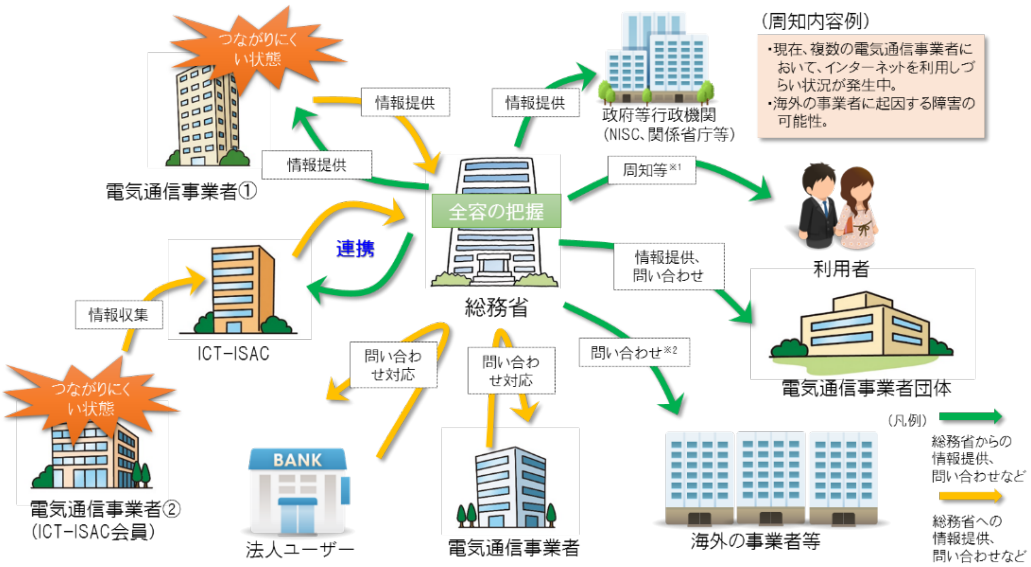
大規模なインターネット障害やサイバー攻撃事案等、複数のネットワークに跨がって発生する障害は、利用者に対して大きな影響を及ぼす。そうした事態に迅速かつ的確に対応するためには、その全容を速やかに把握することが重要であるものの、複数の事業者が関与する場合は困難であることが多い。

また、事業者は、自らに発生した障害の原因が自らのネットワーク内にあるのか否かについてすぐには判断できない。さらに、自らの障害が原因で他の事業者のサービスや業務に障害が生じている場合に、その障害の規模や業務に与える影響の大きさを把握することは困難と考えられる。

一方、電気通信事業法上の重大事故となる恐れがないものについては、現状では事業者に対して速やかな報告は求めていない。また、品質低下でインターネットに接続しづらいといった内容の障害は、電気通信事故として取り扱うものとして整理されておらず、電気通信事業法上の事故報告の対象外とされている。

重大事故に該当しないものであっても、電気通信事業者から速やかに障害等の情報提供を得られれば、総務省において、各事業者から得られた障害情報等（ICT-ISAC との連携により把握した情報や電気通信事業者団体への問い合わせにより把握した情報、また、総務省から海外の事業者等への問い合わせにより把握した情報を含む。）をもとに全容を把握し、政府内や事業者団体、国民生活センター・消費生活センター等との情報共有、外部からの問い合わせ対応の他、利用者周知の観点から必要に応じ速やかに事案を公表することにより、事態の早期沈静化を図ることができると考えられる。

そのため、委員会では障害情報の共有の在り方について検討を行った。



※1　総務省電気通信消費者相談センターにおいては、一般利用者からの個別の問い合わせに対し、総務省が把握した障害情報に基づく情報提供を行う。
※2　海外事業者起因の障害であって、国内事業者の自力での問い合わせが困難であり、総務省からの対応が適切な場合を想定。

図 3.7　障害情報の共有

3.3.2　検討結果

大規模なインターネット障害やサイバー攻撃事案など、複数のネットワークに跨がって発生する障害の早期沈静化を図るためには、障害発生時の情報共有を効果的に実施することが重要である。

そのため、電気通信事業者と総務省との情報共有の在り方について以下の整理を行った。

- 共有すべき情報の内容については、発生日時、発生場所、発生状況、影響、対応状況等が想定されるものの、具体性や情報量は問わない。事態の早期沈静化が目的であることに鑑みれば、基本的には迅速性が優先されることから、発生した障害に係る全てを把握してからではなく、状況把握等に有益な情報であれば提供されることが望ましい。なお、提供される情報が混乱の原因とならないように留意する必要があるとともに、利用者に広く周知可能な情報か、あるいは国民生活センター等に共有できる情報か、さらに他の電気通信事業者に共有できる情報かといった観点を考慮した上で提供されることが望ましい。
- 続報の必要性については、原因解明や復旧に有益な情報であれば続報されることが望ましい。総務省側での調査の状況に応じて続報の協力をお願いすることがある。なお、一報した全ての障害について最後まで情報提供を求めることはしない。
- 通信手段については、電話、メール、FAX のいずれでも可とする。事業者から総務省への情報提供は、基本的には既存の連絡窓口（24 時間、365 日対応可能）に行うこととし（総合通信局が既存の窓口の場合は総合通信局へ）、本省と総合通信局の間でも情報共有を行うこととする。なお、事業者側に 24 時間、365 日の対応をお願いするものではない。
- 他の電気通信事業者や自社のサービスを利用する法人ユーザーへの影響の可能性に係る情報を可能な範囲で提供されることが望ましい。

上記を踏まえ、個々の事項について、関係する事業者団体において一定の方向性を整理した上で、各社判断で詳細を定め実施することにより、実効性ある対応が期待できる。

そのため、電気通信事業者団体のガイドラインにおいて情報共有の在り方に係る事項を定めていくことが望ましいと考えられる。

他方、インターネットに接続しづらい障害については、問い合わせ等に基づき把握する場合を除き、事業者が障害を自覚しその深刻度等状況を把握することは、ネットワーク監視だけでは困難であり、また、利用者が障害として認識するかどうかは利用者の利用状況や利用形態、また利用者の感覚によっても異なる。そのため、総務省において、利用者の生の声を反映した SNS 等への投稿情報をもとに、統計的な視点による分析に基づき、障害の発生の把握を行うことも、全容の把握を行う上で有効である。

3.4　大規模なインターネット障害に関して電気通信事業者等に推奨する対策について

3.4.1　検討の目的等

総務省においては、情報通信ネットワークの安全・信頼性対策の普及・促進を目的として、指標となる対策を「情報通信ネットワーク安全・信頼性基準」（安信基準）において規定している。また、その具体的な説明を「情報通信ネットワーク安全・信頼性基準解説」に掲載し公表することで、対策の実施を促している。

今回、大規模なインターネット接続障害に関して、電気通信事故検証会議において取りまとめられた教訓を踏まえ、同様の障害の防止又は被害の最小化を目的として、電気通信事業者や利用者である法人に対して推奨すべき対策について整理を行うとともに、安信基準に規定化することについて検討を行った。なお、規定化の検討においては以下の観点に留意した。

- 安信基準に新たな規定を追加する場合、汎用的な記載とすること。ただし、重要性に鑑み、具体的な記載とすることが適当な場合はその限りでない。
- 今回整理する対策が安信基準の現行の規定に包含される場合、解説のみに追記すること。ただし、重要性に鑑み、新たな規定を追加することが適当な場合はその限りでない。
- 解説に記載する内容が読み手の十分な理解を得られるものとすること。特に経路情報の設定については、現行の解説には具体的な記載がないが、重要性に鑑み、分かりやすく明確な記載が必要と考えられる。

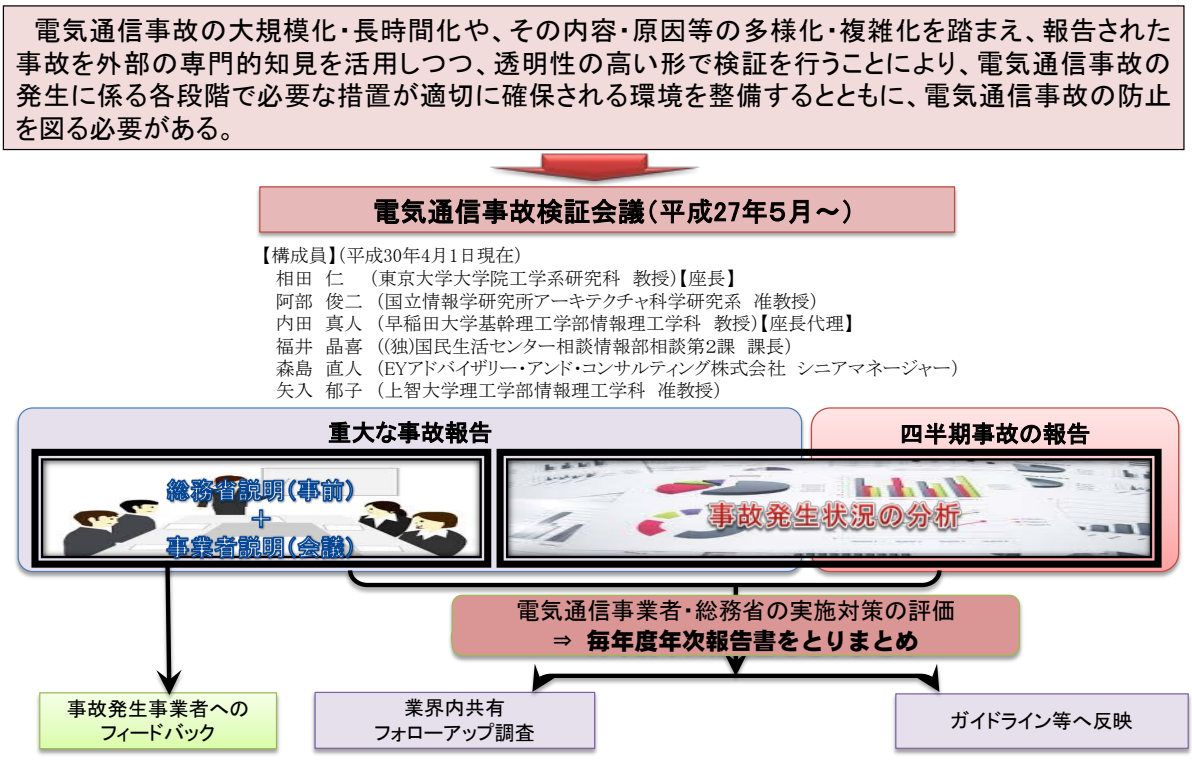


図 3.8　電気通信事故検証会議の概要

3.4.2　検討結果

（１）　インターネットの経路設定時の人為的ミスの防止（電気通信事故検証会議において取りまとめられた教訓その１）

本教訓を踏まえ、電気通信事業者等に推奨すべき対策として、以下の通り未然防止を前提とした手法と、事後措置を前提とした手法について整理を行った。少なくともいずれかの対策の実施を推奨することが適当である。また、個々の対策については以下の通り安信基準等に反映することが適当である。

（ア）　未然防止を前提とした手法

①経路情報の設定作業における誤り防止

経路情報の設定作業は、自動処理で行われる部分はあるものの、新規接続先情報の入力など人手による作業が必ず含まれる。そのため、経路情報の設定作業のみならず、様々な作業工程においても人為的ミスを完全に防ぐことはできない。

しかしながら、経路情報に不具合が発生した場合、インターネット全体に甚大な影響が出るおそれがあることに鑑みれば、経路情報の設定作業においては、人為的ミスによる障害を避けるため、設定が反映される前に、システムによる人為的ミスの防止を目的とした処理の実施や、複数人体制によるチェックの徹底が重要である。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞１．（５）に本対策の規定を以下の通り汎用的な内容で追加し、解説に上記説明を盛り込むことが適当である。

（想定される追加規定）	設	特	他	自	ユ
データ投入等における高い信頼性が求められる作業において、容易に誤りが混入しないよう措置を講ずること。	◎	◎	◎	○	○

なお、安信基準においては情報通信ネットワークを５つに分類しており、上表においては、規定ごと(対策ごと)に各ネットワークにおける実施の必要性を示している（以下、同じ）。

（表中の上段の説明）

設：電気通信回線設備事業用ネットワーク（回線設置事業者のネットワーク）。
特：特定回線非設置事業用ネットワーク（MVNO・FVNO や大規模 ISP のネットワーク）
他：その他の電気通信事業用ネットワーク（「設」や「特」に該当しない事業者のネットワーク）
自：自営情報通信ネットワーク（自営で回線設備を設置したネットワーク）
ユ：ユーザネットワーク上記のいずれにも該当しないネットワーク）

（下段の説明）

◎　：実施すべきである。
◎*　：技術的な難易度等を考慮して段階的に実施すべきである。
○　：実施が望ましい。
－　：対象外。

②経路情報の設定に係る教育・訓練

経路情報に不具合が発生した場合、インターネット全体に甚大な影響が出るおそ

れがあることに鑑みれば、経路情報を設定してからそれによる影響が出るまでの仕組みや、想定される影響等を含む BGP 全般に係る内容に加え、経路情報の設定作業における複数人体制によるチェック等必要な措置についても、教育・訓練を行うことが重要である。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞１．（２）エの規定に含まれる対策であり、解説に上記説明を盛り込むことが適当である。

（現行の規定）	設	特	他	自	ユ
データ投入等における信頼性の高い作業能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎	◎

（イ）　事後措置を前提とした手法

①トラヒックの疎通状況の監視等

経路情報は、通信の到達性を確保するため、各事業者が設定し、接続する事業者間であらかじめ送受信されている。誤り等により大量かつ詳細な経路情報が設定された場合、大量の通信が意図しない経路に流入（元の経路から流出）することとなり、インターネット全体に甚大な影響を及ぼすことが想定される。

このような事態を可能な限り迅速に収束させるためには、各事業者がトラヒックに異常な増大や減少が発生していないか等を自動でチェックし、異常等をアラートで知らせる機能を設けることが有効である。

【想定される安信基準等への反映】

別表第１　設備等基準＞第１．設備基準＞１．（８）オの規定に含まれる対策であり、解説に上記説明を盛り込むことが適当である。

（現行の規定）	設	特	他	自	ユ
交換設備には、トラヒックの疎通状況を監視し、異常ふくそう等を速やかに検知し、通報する機能を設けること。（以下略）	◎	◎	◎	○	○

②復旧対応手順の作成

経路情報の設定後において、トラヒックに異常な増大や減少が発生した場合に、原因や影響を把握するために確認すべき事項や復旧のために行うべき措置等について、あらかじめ手順書を作成することが重要である。なお、復旧のために行った措置が二次被害を発生させる原因となる恐れがあることに留意する必要がある。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞１．（５）エの規定に含まれる対策であり、解説に上記説明を盛り込むことが適当である。

（現行の規定）	設	特	他	自	ユ
保全・運用作業の手順化を行い、手順書の作成を行うこと。	◎	◎	◎	◎	◎*

③対応に関する教育・訓練の実施

経路情報の設定後において、トラヒックに異常な増大や減少が発生した場合に、原因や影響を把握するために確認すべき事項や復旧のために行うべき措置等について、教育・訓練を行うことが重要である。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞１．（２）エの規定に含まれる対策であり、解説に上記説明を盛り込むことが適当である。

（現行の規定）	設	特	他	自	ユ
データ投入等における信頼性の高い作業能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎	◎

（２）　誤送信された経路情報の受信防止及び不要な経路情報の送信防止（教訓その２）

本教訓を踏まえ、電気通信事業者に推奨すべき対策として、以下の通り整理を行った。また、個々の対策については以下の通り安信基準等に反映することが適当である。

①不要又は不正な経路情報の送受信の防止機能

経路情報は、通信の到達性を確保するため、接続する事業者間であらかじめ送受信されており、ある事業者の誤設定により大量かつ詳細な経路情報が不要に送信又は受信されてしまうと、他の事業者に広範囲かつ甚大な影響を及ぼすことが想定される。同様に、不正な経路情報が送信又は受信されてしまうと、他の事業者に重大な影響を及ぼす懸念がある。

インターネットの安定性を確保するため、不要又は不正な経路情報をルータにおいてフィルターする仕組みや、一定量以上の経路情報を受け取らないようリミッターを設定する仕組みがあり、このような設定は、経路情報の受信防止又は送信防止の有効な手段になり得る。

例えば、他の電気通信事業者から経路情報を受信する際は、Prefix フィルター[2]により、細かい経路情報を受信しないよう設定したり、AS-PATH フィルター[3]により、長い AS-PATH 長の経路を受信しないよう設定したり、リミッターにより、設定した

[2] Prefix は、IP アドレスの中のネットワークアドレスを示す部分をいう。Prefix の長さはアドレス空間の深さを表し、Prefix フィルターはその Prefix の長さを基にフィルタリングを行うフィルターをいう。

[3] AS は Autonomous System の略で、ある経路制御方針によって運営されるネットワークのことをいう。宛先に到達するまでに経由した AS のリストを AS-PATH といい、AS-PATH フィルターはこの AS-PATH を基にフィルタリングを行うフィルターをいう。

閾値以上の経路情報を受信しないよう設定したりする対応が考えられる。また、経路情報を他の電気通信事業者等に配信する際は、Prefix フィルターにより、自らの AS 内部で使用している細かい経路情報をそのまま外部に配信しないようにする設定が考えられる。

しかしながら、こうした設定が自らの利用者や他事業者にも影響を与える恐れがあることから、各事業者がそれぞれのネットワーク構成及び他事業者との接続状況等を熟知した上で当該設定の影響を十分に検討し、かつ、それぞれの運用の考え方に照らして、柔軟かつ適切な設定を行うことが重要である。

なお、不要又は不正な経路情報の送受信による障害の発生を防止するためには、あらかじめ接続先と当該情報の送受信の範囲を明確にすることも有効である。

【安信基準等への反映について】

別表第１　設備等基準＞第１．設備基準＞１．（８）に本対策の規定を以下の通り汎用的な内容で追加し、解説に上記説明を盛り込むことが適当である。

（想定される追加規定）	設	特	他	自	ユ
インターネットの経路情報等制御信号のうち不要又は不正なものの送受信を防ぐために有効な機能を設けること。	◎	◎	◎	―	―

②経路情報の急増等を考慮した設計

平成２９年８月に発生した大規模インターネット障害については、約 10 万件を超える情報（障害発生当時、一度に約２年分の経路情報に相当。）が配信されたことが原因の一つとなった。

対策としては、同様の障害を想定し十分な余裕をもった処理能力を確保することが考えられるものの、不要な経路制御の送受信を防ぐために有効な機能を設ける観点から設計を行うことも有効である。

しかしながら、こうした機能が自らの利用者や他事業者に影響を与える恐れがあることに留意する必要があるほか、経路情報の瞬間的かつ急激な増加を考慮しないことによる影響についても留意する必要がある。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞１．（３）イの以下の通り汎用的な内容で改正し、解説に上記説明を盛り込むことが適当である。

（想定される規定の改正）※改正部分は下線部	設	特	他	自	ユ
トラヒック及びインターネットの経路情報等制御信号の瞬間的かつ急激な増加の対策を講じた設計とすること。	◎	◎	「ー」から「◎」に改正	―	―

③将来の経路情報の増加の考慮

現状において、インターネットの経路情報は、日々増えているところであり、ルータの設計においては経路情報の将来的な増加（瞬間的かつ急激な増加を除く。）の見通しを踏まえて検討することが重要である。

【想定される安信基準等への反映】

別表第２　管理基準＞第３．方法＞　１．（３）アの規定に以下の通り汎用的な内容で追記し、解説に上記説明を盛り込むことが適当である。

（想定される規定の改正）※改正部分は下線部	設	特	他	自	ユ
将来の規模の拡大、トラヒック増加（端末の挙動によるものを含む。）、インターネットの経路情報等制御信号の増加及び機能の拡充を考慮した設計とすること。	◎	◎	◎	◎	◎

（３）　経路設定誤り又はサイバー攻撃による障害に関する情報の事業者間での共有（教訓その３）

本教訓を踏まえ、電気通信事業者等に推奨すべき対策として、以下の通り整理を行った。また、個々の対策については以下の通り安信基準等に反映することが適当である。

①電気通信事業者間での情報共有及び情報収集

インターネットにおける障害においては、まず、発生した事象が自社単独で起きている事象なのか、他の電気通信事業者でも同様に起きている事象なのか、あるいは、他の電気通信事業者がどのように復旧対応したかを把握することが、自らの対応策を検討する上で大変重要であり、自社内の状況確認に加え、必要に応じて契約関係等がある電気通信事業者との状況確認や、ネットワーク技術者間の情報交換など一定程度の取り組みが行われている。

誤った経路情報やサイバー攻撃による障害等、ネットワークを跨がって発生する障害については、障害の発生状況や影響範囲、収束状況などの把握が困難な場合があることから、報道や SNS、総務省への確認等を通じて幅広く情報収集を行うことが有効である。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞２．（１）に本対策（情報収集に係る部分）の規定を以下の通り追加し、解説に上記説明を盛り込むことが適当である。

（想定される追加規定）	設	特	他	自	ユ
事故又は障害発生時に迅速な原因分析、状況把握及び復旧対応等のため、電気通信事業者間での情報共有を含め、複数のルートを活用し幅広く情報収集に努めること。	◎	◎	◎	○	○

②契約関係等がある事業者（海外の事業者を含む。）との連携

事故又は障害発生時に有益な情報共有が行われるよう、直接接続関係にあり、契約を締結している事業者（海外の事業者を含む。）との障害対応時の連絡先を把握しておくことが重要である。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞２．（１）アの規定に含まれる対策であり、解説に上記説明を盛り込むことが適当である。

（現行の規定）	設	特	他	自	ユ
迅速な原因分析のための関連事業者等（接続先、委託先、製造業者等をいう。）との連携を図るよう取り組むこと。	◎	◎	◎	○	○

（４）　ネットワーク構成に係る対策

電気通信事故検証会議において取りまとめられた検証報告書を踏まえ、電気通信サービスの利用者に推奨すべき対策として、以下の通り整理を行った。また、個々の対策については以下の通り安信基準等に反映することが適当である。

①重要な回線の信頼性の向上

重要な回線については事故又は障害の発生時に大きな影響を受ける恐れがあることから、信頼性の向上を図ることが重要である。具体的な手段としては、異なる２者以上の電気通信事業者から提供を受けることによる冗長化のほか、拠点引き込みの異経路化や収容ビルの分散等の方法が考えられ、サービス提供者においては電気通信事業者とネットワーク構成等を相談の上、実施判断することが重要である。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞１．（３）に本対策の規定を以下の通り追加し、解説に上記説明を盛り込むことが適当である。

（想定される追加規定）	設	特	他	自	ユ
重要な回線については異なる２者以上の電気通信事業者から提供を受ける等により、信頼性の向上を図ること。	－	－	－	○	○

（５）　利用者周知（教訓その４）

本教訓を踏まえ、電気通信事業者に推奨すべき対策として、以下の通り整理を行った。また、個々の対策については以下の通り安信基準等に反映することが適当である。

①利用者に対する情報公開

インターネットにつながりにくい障害であって、接続先や他の事業者のネットワークに起因するものの場合、自社に原因がないもの又は自社に原因があるか不明なものについては、迅速な原因分析や状況把握が困難である可能性がある。そのため、利用者への情報提供に時間を要する可能性があるが、情報提供の遅れが利用者の混

乱を拡大させる恐れがある。法人ユーザーの顧客が多数存在する場合は混乱が相当規模に発展する恐れもある。

そのため、利用者の混乱を防止する観点から、発生事実のみであっても利用者に公開することが重要と考えられる。なお、対象が特定の法人ユーザー等限定的な場合は、個別に情報提供する方が、無用な混乱を防ぐ観点から適当と考えられる。

また、あらかじめ、その周知内容を決めておくことが重要と考えられる。

【安信基準等への反映について】

別表第２　管理基準＞第３．方法＞２．（２）アの規定に以下のとおり汎用的な内容を追記し、解説に上記説明を盛り込むことが適当である。

（想定される追加規定）※改正部分は下線部	設	特	他	自	ユ
事故・ふくそうが発生した場合、又は利用者の混乱が懸念される障害が発生した場合に、速やかに利用者に対して公開すること。	◎	◎	◎	―	―

3.5　電気通信事故報告制度に係るその他の対策について

電気通信事業法における事故報告制度においては、四半期毎に事故の発生状況の報告を求めており、その中でサイバー攻撃を原因とする事故については、「第三者要因」の事故や「その他」の発生原因の事故として分類されて報告されている。これは、発生原因の分類に「サイバー攻撃」が設定されていないためであり、発生原因がサイバー攻撃である事故を明確に把握できていない。

しかし、サイバー攻撃のうち、特に電気通信事業者が保有する電気通信設備の機能に障害を与えるものは、一定規模以上の電気通信役務の停止や品質の低下による事故を引き起こす恐れがあることから、総務省が発生状況を把握した上で、政策等に的確に反映することが必要である。

本年５月に成立した、「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」においては、電気通信事業法において「送信型対電気通信設備サイバー攻撃」を新たに定義している※。

このため、四半期毎の報告様式における発生原因の分類のひとつに、新たに送信型対電気通信設備サイバー攻撃を追加し、当該四半期報告において送信型対電気通信設備サイバー攻撃を発生原因とする事故を明らかにすることが適当と考えられる。

※　情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する攻撃のうち、送信先の電気通信設備の機能に障害を与える電気通信の送信（当該電気通信の送信を行う指令を与える電気通信の送信を含む。）により行われるものをいう。

第４章　今後の検討課題

4.1　検討課題

以下の２点については、今後の検討課題として委員会において引き続き議論を行う。

①IoT サービスの安全・信頼性を確保するための資格制度等の在り方について

②新たな技術を活用した通信インフラの維持・管理方策について

4.2　IoT サービスの安全・信頼性を確保するための資格制度等の在り方について

4.2.1　検討の目的等

ネットワーク機能のソフトウェア化や高速伝送技術の進展等により、通信ネットワークの高機能化や設備構成の複雑化が進み、サイバー攻撃等によるインターネット障害等が増加する中、ネットワークの工事・維持・運用や、端末設備・自営電気通信設備の接続の工事等において、ソフトウェアやセキュリティ技術に関して十分な知識を有する技術者のニーズが高まっている。また、求められるスキルは、技術革新に伴い今後も変化していくものと考えられる。

このように IoT が普及していく中で ICT サービスの安全・信頼性を確保するためには、現状のニーズを踏まえながら、電気通信主任技術者や工事担任者に求められるスキルや役割を整理する必要がある。

4.2.2　今後の論点

（１）　電気通信主任技術者に求められるスキル等について

現在、電気通信主任技術者の資格制度は、伝送交換設備及びこれらに附属する設備の工事、維持及び運用を監督する「伝送交換」と、線路設備及びこれらに附属する設備の工事、維持及び運用を監督する「線路」の２区分に分かれている。

しかし、ネットワーク技術の高度化・複雑化が進展している中、電気通信主任技術者には、ネットワークの仮想化技術等の新たなスキルや、従来の伝送交換、線路といった区分を跨ぐような知識が求められるようになっている。

更に、今後 LPWA サービス等の多種多様なサービスを提供する電気通信事業者が増加していくと見込まれる中、こうしたサービスを利用者が安心して利用するためには電気通信事業者が行うセキュリティ対策の重要性がますます高まっていくと想定される。そのため、電気通信主任技術者に対し、サイバーセキュリティに関する知見や能力を求めていくことも重要と考えられる。

◆ リモート保守による技術集約が加速。また仮想化に伴いソフトウエア人材も必要。
◆ オンサイトについても線路／無線／端末などスキルの複合化が急務。
➢ 技術の高度化・複合化により、従前の伝送線路／交換等の区分は馴染まなくなる。

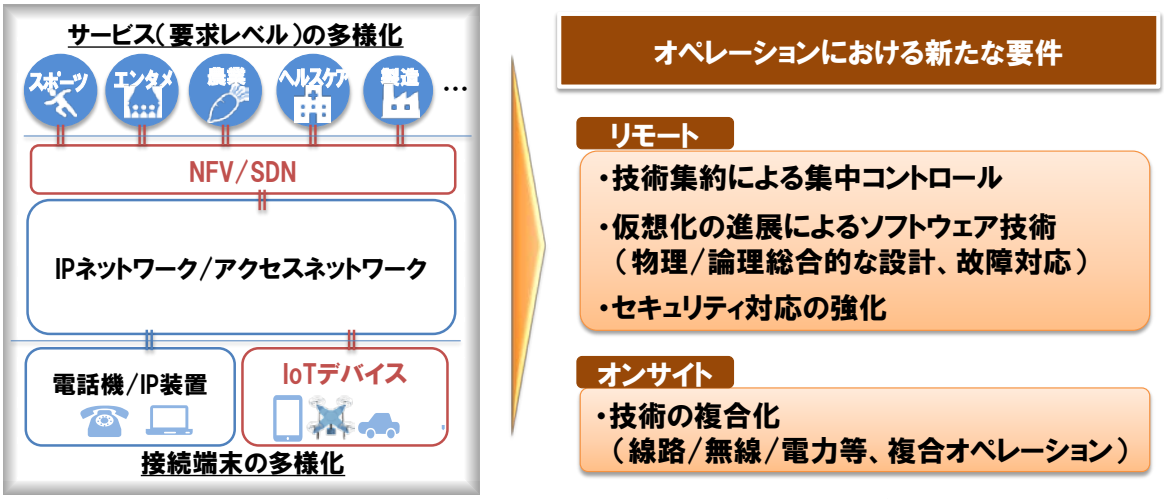


図 4.1　ネットワーク技術の高度化・複合化（第 34 回 NTT 説明資料より抜粋）

電気通信主任技術者に求められるスキル等については、以上の点を踏まえながら、資格区分の見直しも含め、委員会において引き続き議論を行うことが適当である。

（２）　工事担任者に求められるスキル等について

電気通信事業法では、利用者が端末設備又は自営電気通信設備を事業者の電気通信回線設備に接続するとき、これに係る工事を工事担任者に実施又は実地で監督させなければならないとされている。ただし、適合表示端末機器等の接続の方式が告示で定めるプラグジャックや電波等の方式であるときには、工事担任者による接続の工事は不要となっている。

一方、IoT の普及に伴い、多種多様な端末設備等が事業者の電気通信回線設備に接続されるようになることから、端末設備等の接続の工事の実施等を行う工事担任者が果たす役割は重要になっていくと考えられる。

また、図 4.2 のように近年の工事担任者試験の申請者数は減少傾向にあるが、工事担任者の試験内容は、情報通信を専攻する学生が学ぶべき内容も多いことから、他の国家試験の取組みも参考にしつつ、工事担任者の育成方策を検討することも重要と考えられる。

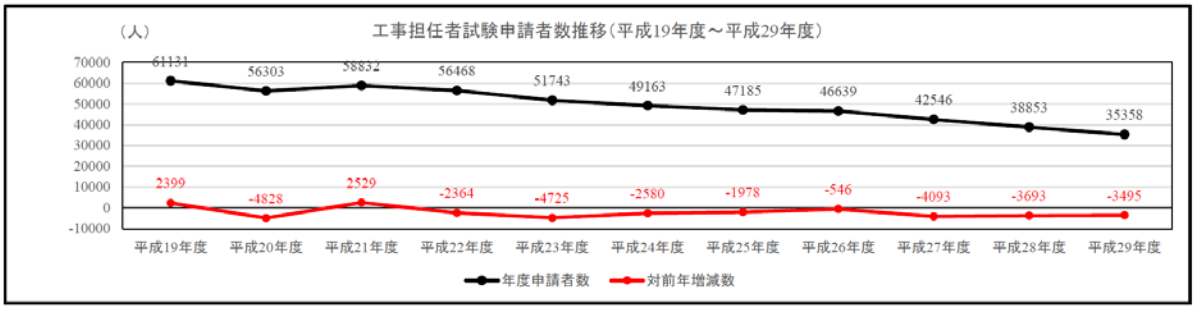


図 4.2　工事担任者試験申請者数推移
（第 39 回委員会　日本データ通信協会説明資料より抜粋）

さらに、工事担任者資格は、一度取得すれば永久的に有効な資格となっているが、その資格者は、端末設備等の接続に関する知識及び技術の向上を図るように努めなければならないとされている。今後、技術革新が益々加速していく中で、工事担任者の資格者がどのようにして最新の知識及び技術の向上を図っていくべきかという点についても検討が必要である。

工事担任者に求められる役割やスキル等については、以上の点を踏まえながら、委員会において引き続き議論を行うことが適当である。

4.3　新たな技術を活用した通信インフラの維持・管理方策について

4.3.1　検討の目的等

通信インフラの維持・管理には膨大な人的コストが必要であるが、維持・管理に携わる人材は減少傾向にある。こうした中で、今後も安定的に通信インフラを維持・管理していくためには、AI 等の新たな技術を活用した技術が必要となってきている。

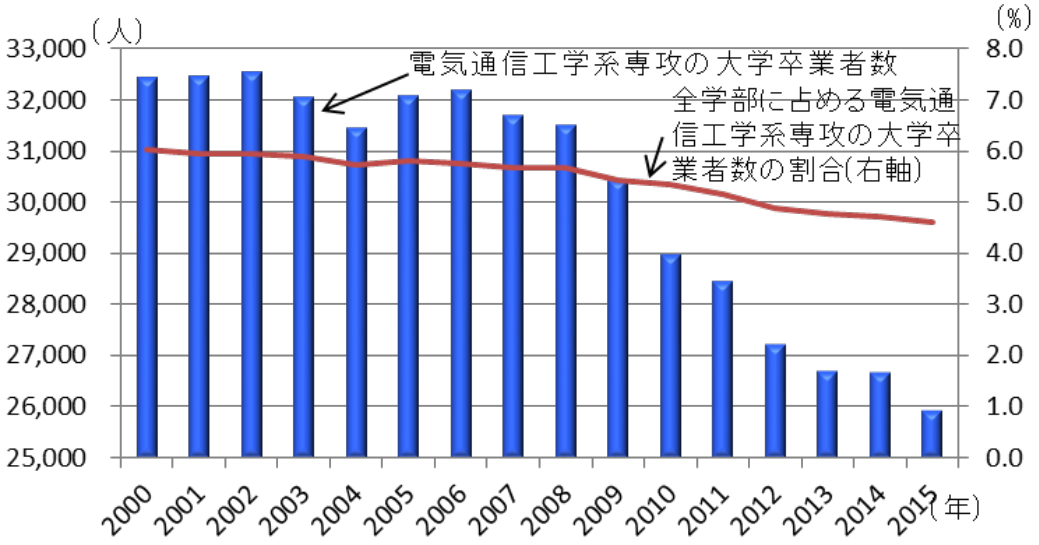


図 4.3　電気通信工学系専攻の大学卒業者数の推移

また、大規模災害時には、土砂崩れ等に伴う道路の寸断等により、作業員の現場の立ち入りが困難となり復旧作業が長時間化する事例が発生するなど、大規模災害時により早く通信を復旧させるための新たな方策を検討する必要がある。

4.3.2　今後の論点

労働人口の急激な減少が進む中、今後も安定的に通信インフラの維持・管理を行うためには、リモート保守によるネットワークの集中管理や、AI／ロボットなどを活用し、大量のデータを自動取得・自動解析することによって効率的なインフラ維持・管理を行っていくなど最新技術を活用することが一層重要となる。

また、ドローンの活用については、例えば、鉄塔点検において、地上から確認できない角度からボルト劣化などを詳細かつ安全に確認でき、災害対策においては、陸路が寸断されてしまった地域のエリア化が可能で、通信エリアの更なる早期復旧に大きな貢献が期待されるなど、危険を伴う高所作業や迅速性を求められる災害対応などにおいて有効であると考えられる。

新たな技術を活用した通信インフラの維持・管理方策と実現に向けた課題整理について、以上の点を踏まえながら、委員会において引き続き議論を行うことが適当である。

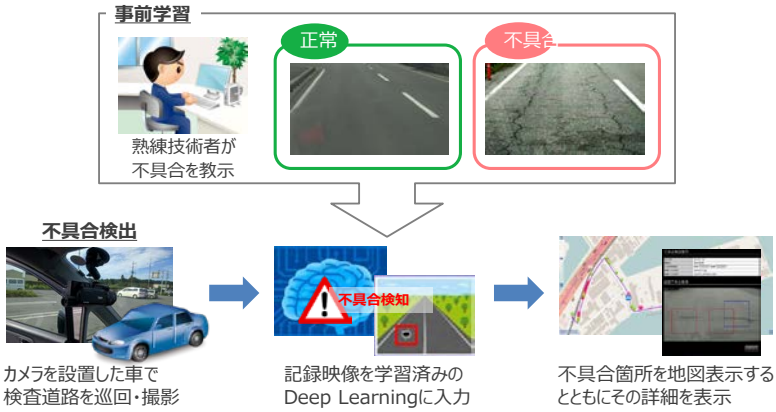


図 4.4　ＡＩ等を活用したインフラ維持のイメージ
（第 34 回委員会　NTT 説明資料を基に作成）

図 4.5　ドローン活用のイメージ（第 34 回委員会　KDDI 説明資料を基に作成）

別表１　IP ネットワーク設備委員会 構成員

情報通信審議会 情報通信技術分科会
IP ネットワーク設備委員会 構成員

（平成 30 年 6 月時点　敬称略　五十音順）

	氏　名	所　属
主査	相田　　仁	東京大学大学院 工学系研究科 教授
主査代理	岡野　直樹	国立研究開発法人 情報通信研究機構 理事
	会田　容弘	一般社団法人 日本インターネットプロバイダー協会 会長
	有木　節二	一般社団法人 電気通信事業者協会 専務理事
	内田　真人	早稲田大学 基幹理工学部 情報理工学科 教授
	江﨑　　浩	東京大学大学院 情報理工学系研究科 教授
	大矢　　浩	一般社団法人 日本 CATV 技術協会 副理事長
	尾形わかは	東京工業大学 工学院 情報通信系 教授
	片山　泰祥	一般社団法人 情報通信ネットワーク産業協会 専務理事
	前田　洋一	一般社団法人 情報通信技術委員会 代表理事専務理事
	松野　敏行	一般財団法人 電気通信端末機器審査協会 専務理事
	向山　友也	一般社団法人 テレコムサービス協会 技術・サービス委員会 委員長
	村山　優子	津田塾大学 学芸学部 情報科学科 教授
	森川　博之	東京大学大学院 工学系研究科 教授
	矢入　郁子	上智大学 理工学部 情報理工学科 准教授
	矢守　恭子	朝日大学 経営学部 経営情報学科 教授

別表２　技術検討作業班 構成員

情報通信審議会 情報通信技術分科会
IP ネットワーク設備委員会 技術検討作業班 構成員

（平成 30 年 6 月時点　敬称略　五十音順）

	氏　名	所　属	事故報告等担当	端末ｾｷｭﾘﾃｨ担当
主任	内田　真人	早稲田大学 基幹理工学部 情報理工学科 教授	○	○
主任代理	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	○	○
	大内　良久	ＫＤＤＩ株式会社 技術統括本部 運用本部 運用品質管理部　部長	○	
	岡田　昌己	エヌ・ティ・ティ・コミュニケーションズ株式会社 カスタマサービス部 危機管理室長	○	
	尾形わかは	東京工業大学 工学院 情報通信系 教授	○	
	小畑　和則	株式会社ＮＴＴドコモ Ｒ＆Ｄ戦略部 担当部長	○	○
	木村　　孝	一般社団法人 日本インターネットプロバイダー協会 会長補佐	○	
	喜安　明彦	一般社団法人 電気通信事業者協会 安全・信頼性協議会 会長	○	
	桑田　雅彦	日本電気株式会社 デジタルプラットフォーム事業部 シニアエキスパート		○
	小林　　努	株式会社インターネットイニシアティブ サービス基盤本部 副本部長	○	○
	阪田　　徹	一般財団法人 電気通信端末機器審査協会 機器審査部 部長代理		○
	四ノ宮大輔	一般社団法人 情報通信ネットワーク産業協会 通信ネットワーク機器 セキュリティ分科会 主査		○
	渋谷　香士	ソニー株式会社 品質・環境部 シニア製品セキュリティマネジャー		○
	高橋慎一郎	株式会社ＮＴＴドコモ 情報セキュリティ部 サイバーセキュリティ統括室 室長		○
	高橋　　範	株式会社ソラコム 事業開発マネージャー	○	
	田島　佳武	日本電信電話株式会社 技術企画部門 セキュリティ戦略 担当部長		○
	中野　　学	パナソニック株式会社 製品セキュリティセンター 製品セキュリティグローバル戦略室 主幹技師		○
	中村　康洋	シャープ株式会社 ＩｏＴ事業本部 ＩｏＴクラウド事業部 イノベーション開発部 技師		○
	西川　嘉之	ＵＱコミュニケーションズ株式会社 渉外部 部長	○	

西部　喜康	一般社団法人 ＩＣＴ―ＩＳＡＣ 脆弱性保有ネットワークディバイス調査ＷＧ 主査		○
野呂田みゆき	東日本電信電話株式会社 ＩＴイノベーション部 技術部門 企画担当		○
花石　啓介	日本電信電話株式会社 技術企画部門 災害対策室長 兼 ビジネスプロセス戦略担当 担当部長	○	
日比　　学	京セラコミュニケーションシステム株式会社 ＬＰＷＡソリューション事業部 ＬＰＷＡソリューション部 副責任者	○	
福井　晶喜	独立行政法人 国民生活センター 相談情報部 相談第２課 課長	○	○
福島　　敦	株式会社ジュピターテレコム 技術運用副本部長	○	
堀内　浩規	一般社団法人 日本ケーブルテレビ連盟 理事 兼 通信制度部長	○	
前田　真弓	東芝クライアントソリューション株式会社 技監		○
松本　勝之	ソフトバンク株式会社 ＩＴサービス開発本部 セキュリティ事業統括部 セキュリティオペレーションセンター部 サイバーインシデントレスポンス課 課長		○
松本　佳宏	株式会社ケイ・オプティコム 計画開発グループ グループマネージャー	○	
向山　友也	一般社団法人 テレコムサービス協会 技術・サービス委員会 委員長	○	
毛利　政之	ＫＤＤＩ株式会社 技術企画本部 電波部 管理グループリーダー		○
矢入　郁子	上智大学 理工学部 情報理工学科 准教授	○	
山口　琢也	ソニーネットワークコミュニケーションズ株式会社 ネットワーク基盤事業部門 ネットワーク部 ネットワーク運用課 課長	○	
渡部　康雄	ソフトバンク株式会社 技術管理本部 業務管理統括部 技術渉外部 部長	○	○