資料 40－2

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 技術検討作業班
報告

―IoT時代における重大事故に関する事故報告等の在り方―

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
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のうち、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係る技術検討作業班の検討結果を取りまとめたものである。

Ⅱ　作業班の構成

作業班の構成は、別表 1 のとおりである。

Ⅲ　検討経過

これまで、技術検討作業班（第 31 回～第 34 回）を開催して検討を行い 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報告を取りまとめた。

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い、検討状況を委員会に報告することとした。

④　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 時代における重大事故に関する事故報告等の在り方

1.1　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対策のうち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

④電気通信事故報告制度に係るその他の検討について

1.2　LPWA サービスの事故報告基準について

1.2.1　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 サービスは電気通信事業法施行規則第 58 条第１項第１号表中第４号に掲げる役務に該当するため、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している。

一方、LPWA サービスは現時点では主に、相当数のセンサー機器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るものの、数時間おきに通信を行う低頻度のものが存在する。また、相当数の機器が接続されるものであることから、現行の事故報告制度の基準に照らして重大事故の報告を求める場合、事故によって影響を受ける利用者の感覚と制度上の取り扱いに差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。

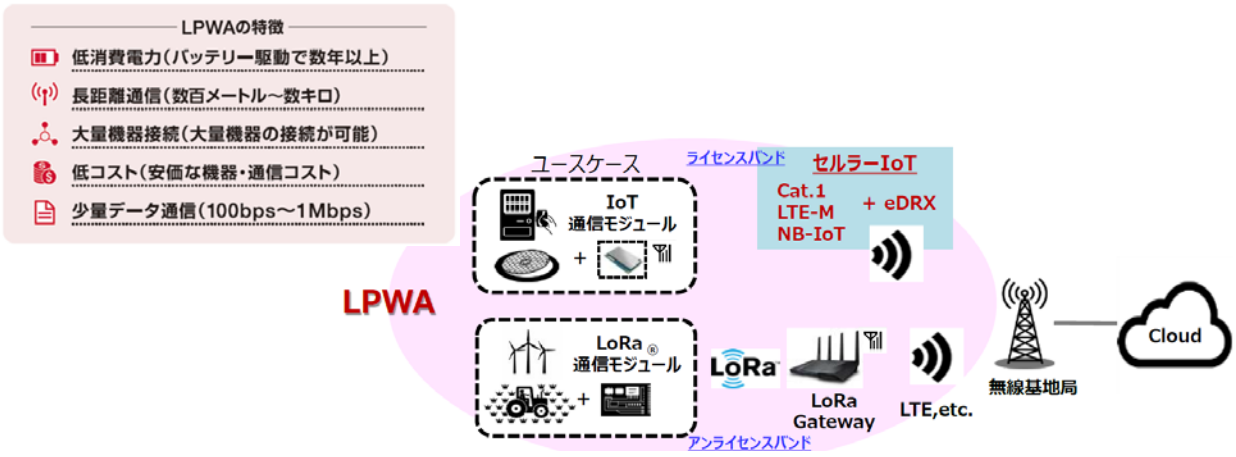


図 1.1　LPWA の特徴等
（第 35 回委員会　NTT ドコモ説明資料より抜粋）

1.2.2　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。

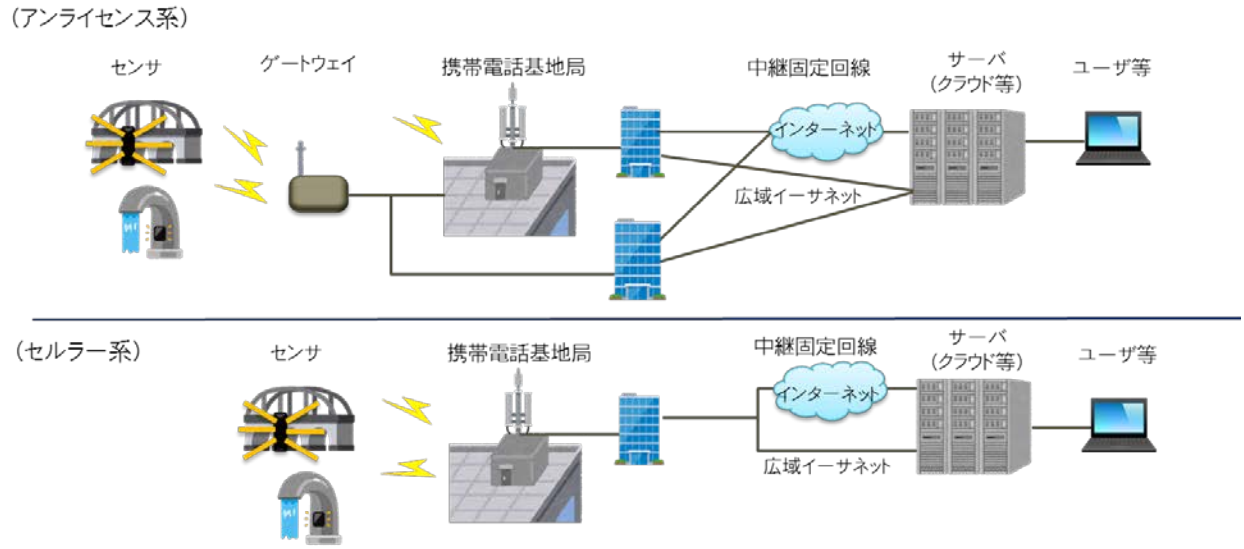


図 1.2　LPWA サービスのネットワーク構成イメージ

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。

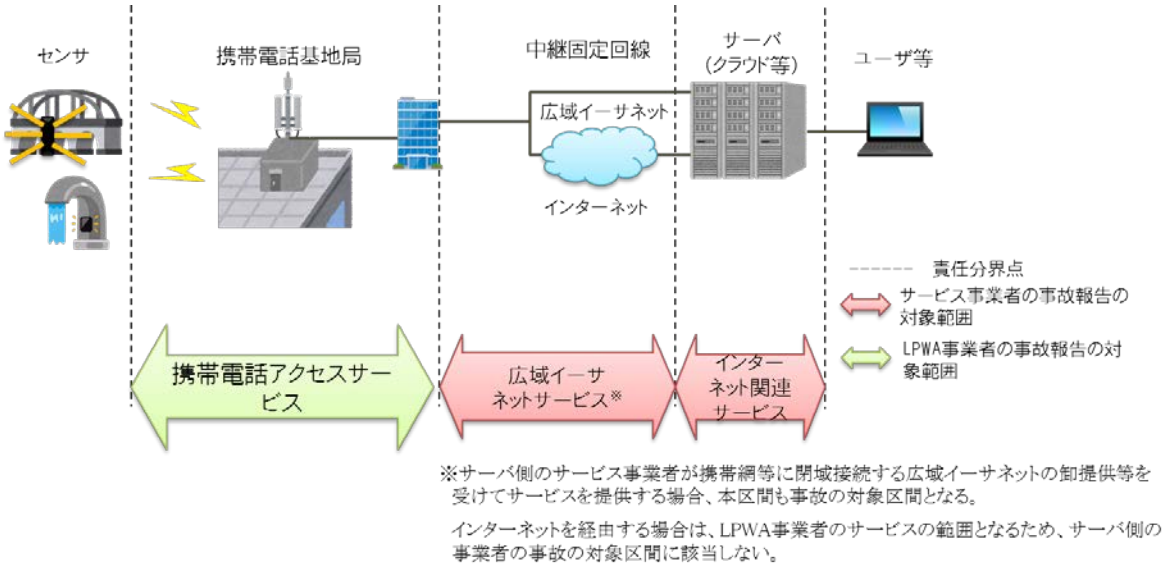


図 1.3　LPWA サービス（セルラー系）の事故報告範囲

次に、LPWA サービス（アンライセンス系）については、

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。

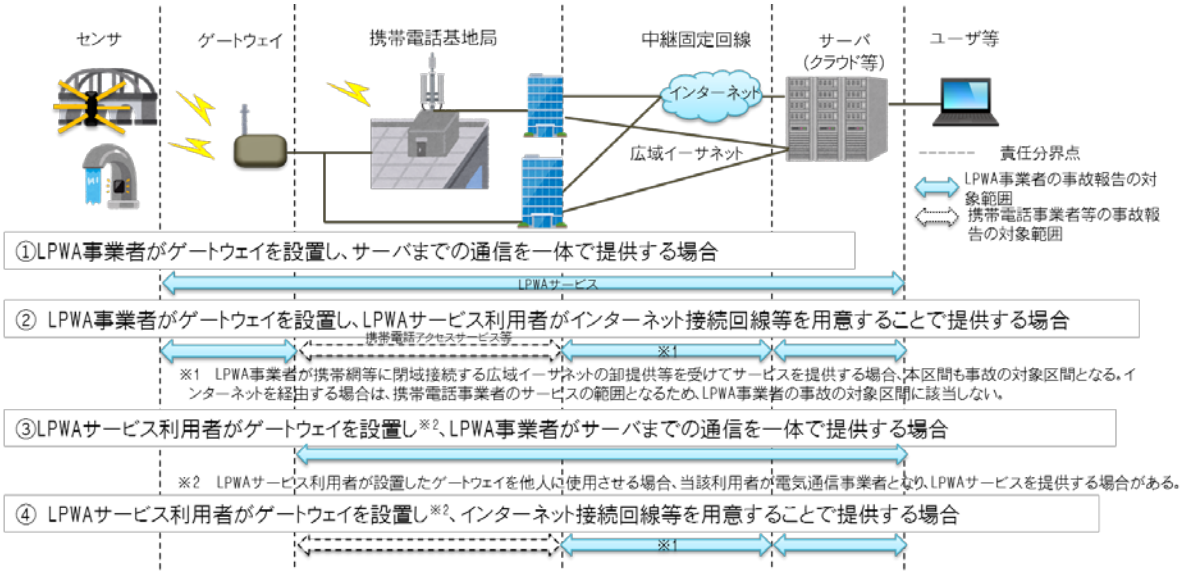


図 1.4　LPWA サービス（アンライセンス系）の事故報告範囲

（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 サービスは M2M の通信がメインであり、その通信主体は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。

しかしながら現状においては、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ことを踏まえ、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。

ただし、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。

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。

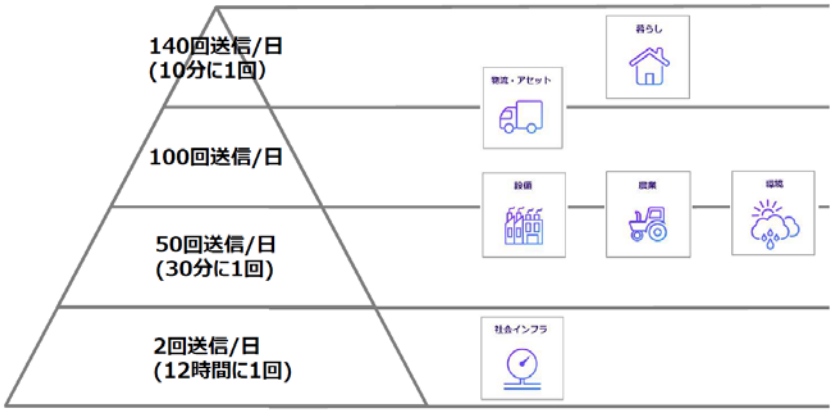


図 1.5　用途と通信頻度
（第 31 回技術検討作業班　京セラコミュニケーションシステム説明資料より抜粋）

（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。

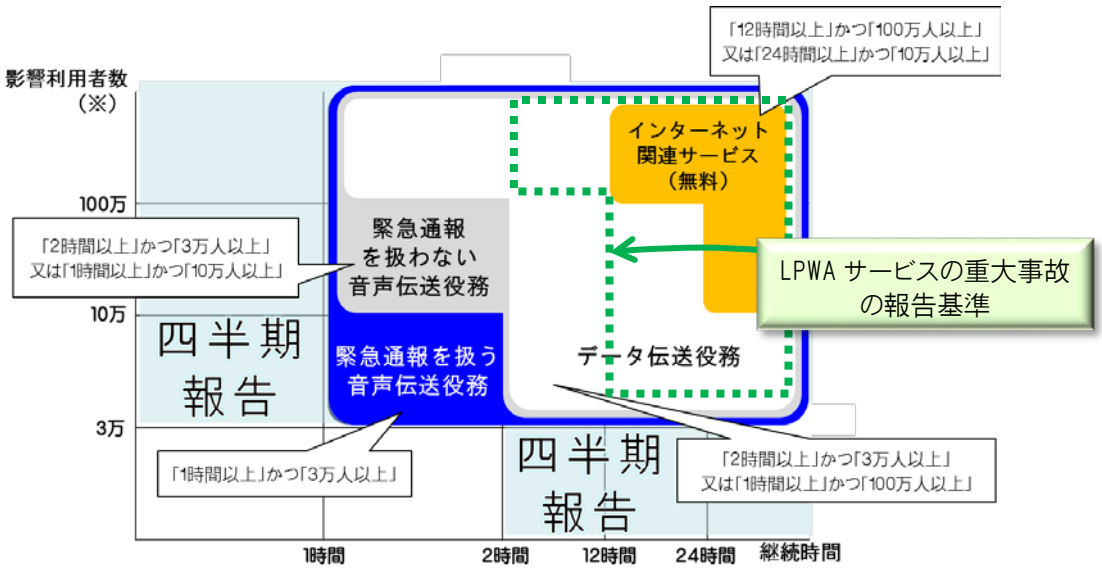
また、総務省においては、事故の発生原因等様々な切り口から統計分析を行うことを目的として、重大事故に至らない事故であっても一定規模以上であれば、四半期毎

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、または 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 1.6　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、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。

1.3　大規模なインターネット障害発生時の対策のうち障害情報の共有について

1.3.1　検討の目的等

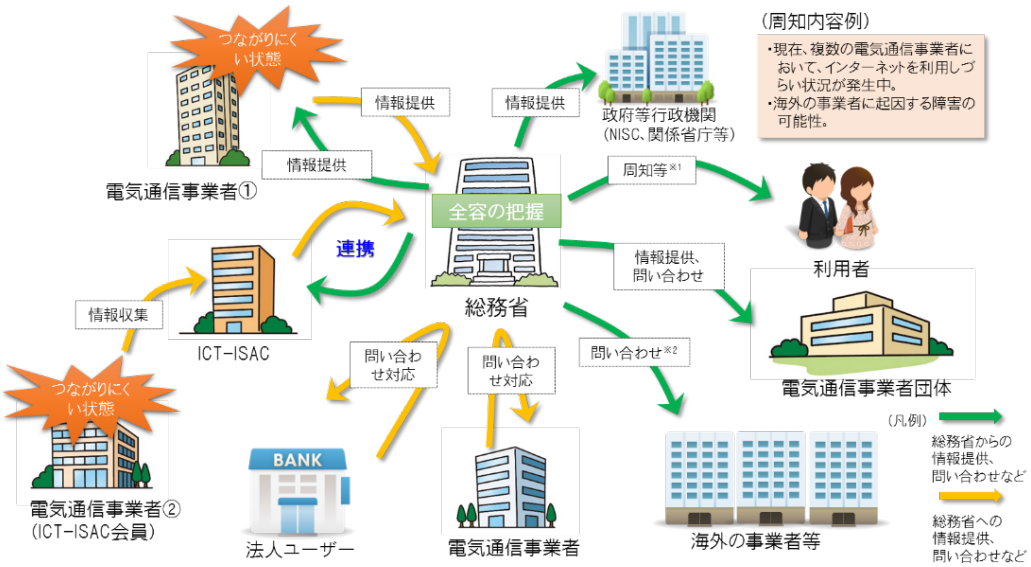
大規模なインターネット障害やサイバー攻撃事案等、複数のネットワークに跨がって発生する障害は、利用者に対して大きな影響を及ぼす。そうした事態に迅速かつ的確に対応するためには、その全容を速やかに把握することが重要であるものの、複数の事業者が関与する場合は困難であることが多い。

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知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、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 1.7　障害情報の共有

1.3.2　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。

1.4　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

1.4.1　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。

1.4.2　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間の手作業は必ず含まれる。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。
〇　：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おいては、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ひとつとなった。

対策として、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。	◎	◎	「－」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どうか、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また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また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、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 <u>が発生した場合、又は利用者の混乱が懸念される障害</u> 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。	◎	◎	◎	－	－

1.5　電気通信事故報告制度に係るその他の検討について

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している。

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おり、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、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 16 日に成立した、「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。

別表１　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	障害対策担当	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	○	○