技術検討作業班報告書（案）概要
－電気通信事故報告制度について－

平成30年6月7日

IPネットワーク設備委員会
技術検討作業班
事務局

「IoTの普及に対応した電気通信設備に係る技術的条件」に係る検討事項

（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、必要に応じて見直しの検討を行う（IoT機器を含む脆弱な端末設備のセキュリティ対策に係る検討を含む。）。

（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。

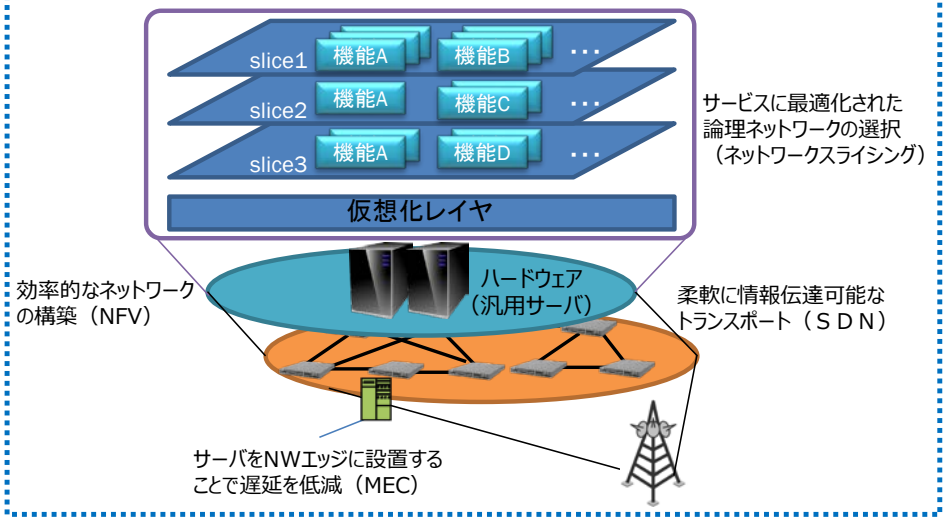
（3） IoT時代における重大事故に関する事故報告等の在り方

今後、IoTサービスが多様化し、従来の設備故障以外を原因とした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（大規模なインターネット障害発生時の対策に係る検討を含む。）。

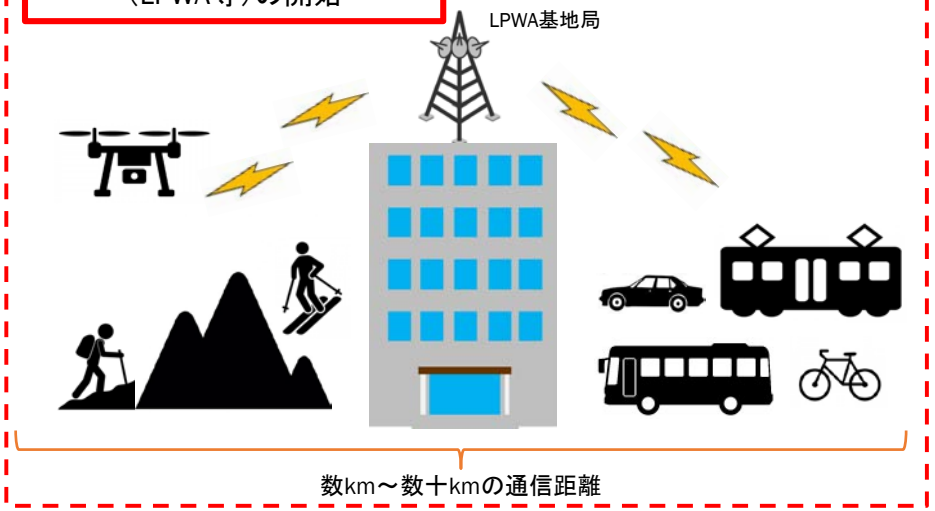
（4） その他

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。

ネットワーク技術のソフトウェア化等の進展



新たなIoT用無線通信サービス（LPWA等）の開始



検討事項（３）に係る検討経過

第31回（平成30年３月16日）

- LPWAサービスやIoTサービスに係る各社の取り組みや、LPWAサービスの電気通信事故報告基準の検討における課題について、構成員より説明が行われた。
- 「LPWAサービスの事故報告基準の検討」における論点を整理し議論を行った。
- 「大規模インターネット障害発生時の対策」について、IPネットワーク設備委員会の検討を踏まえ、論点を整理し議論を行った。

第32回（平成30年４月９日）

- 前回の議論を踏まえ、「LPWAサービスの事故報告基準」について、また「大規模インターネット障害発生時の対策」のうち、「障害情報の共有の在り方」について検討を行った。

第33回（平成30年５月10日）

- 第31回作業班の検討を踏まえ、「大規模インターネット障害発生時の対策」のうち、「電気通信事業者に推奨する対策」について検討を行った。
- 前回の議論を踏まえ、「LPWAサービスの事故報告基準」及び「大規模インターネット障害発生時の対策」における「障害情報の共有の在り方」について、取りまとめの方向性の整理を行い、それらを含めた作業班報告書骨子案について検討を行った。

第34回（平成30年６月７日）【予定】

作業班におけるこれまでの検討を踏まえ、作業班報告書案の審議を行い、取りまとめる予定。

具体的な検討課題

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として注目され、進展が期待されている。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、拡大する可能性があるため、「LPWAサービスの事故報告基準」について検討を行うこととした。

また、「電気通信事故検証会議報告書」や、「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」において、「大規模なインターネット障害発生時の対策」として、「障害情報の共有」や経路情報のフィルター設定等「電気通信事業者に推奨する対策」について、制度的対応の検討が必要とされたこと等を受け、同対策について検討を行うこととした。

さらに、事故報告制度に係るその他の検討として、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状況を踏まえ、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「サイバー攻撃の事故報告」についても検討を行うこととした。

①LPWAサービスの事故報告基準の検討

②大規模なインターネット障害発生時の対策の検討

（ア）障害情報の共有の在り方

（イ）電気通信事業者に推奨する対策

③電気通信事故報告制度に係るその他の検討

①LPWAサービスの事故報告基準の検討

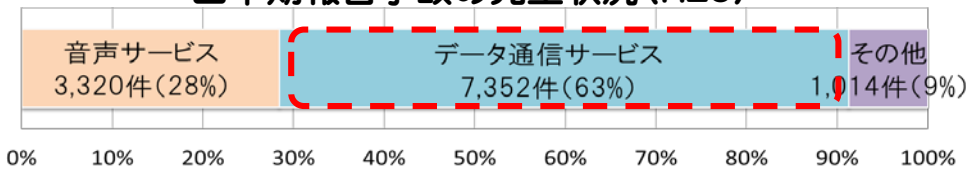
検討事項：IoT時代における重大事故に関する事故報告等の在り方

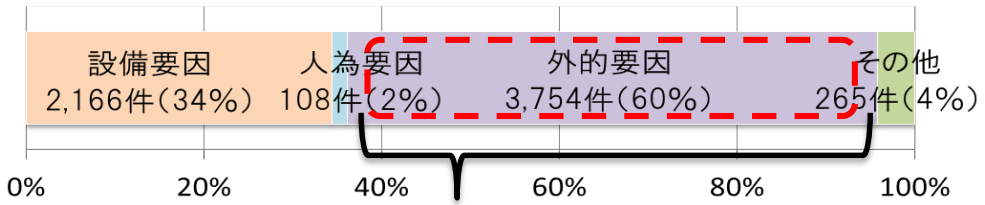
○　IoTサービスが進展し、ネットワークに接続される機器が急速に増大するため、ひとたび障害が発生すれば多数の機器に影響を及ぼす可能性がある。

○　また、ソフトウェア技術によるネットワーク機能が実現されることにより、サービスの提供に必要なネットワーク機能を他事業者に依存することが容易になるため、他の電気通信事業者の障害を起因とする障害が増加する可能性がある。更に、多様なサービスの出現により、障害の責任の所在があいまいとなるケースが増える可能性もある。

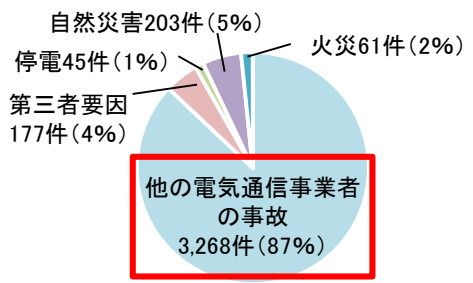
○　ネットワークの安全・信頼性を確保するためには、現行の重大事故等に関する事故報告制度の検証を行い、こうした課題に対応したネットワーク障害に関する報告の在り方等について検討が必要。

＜四半期報告事故の発生状況（H28）＞

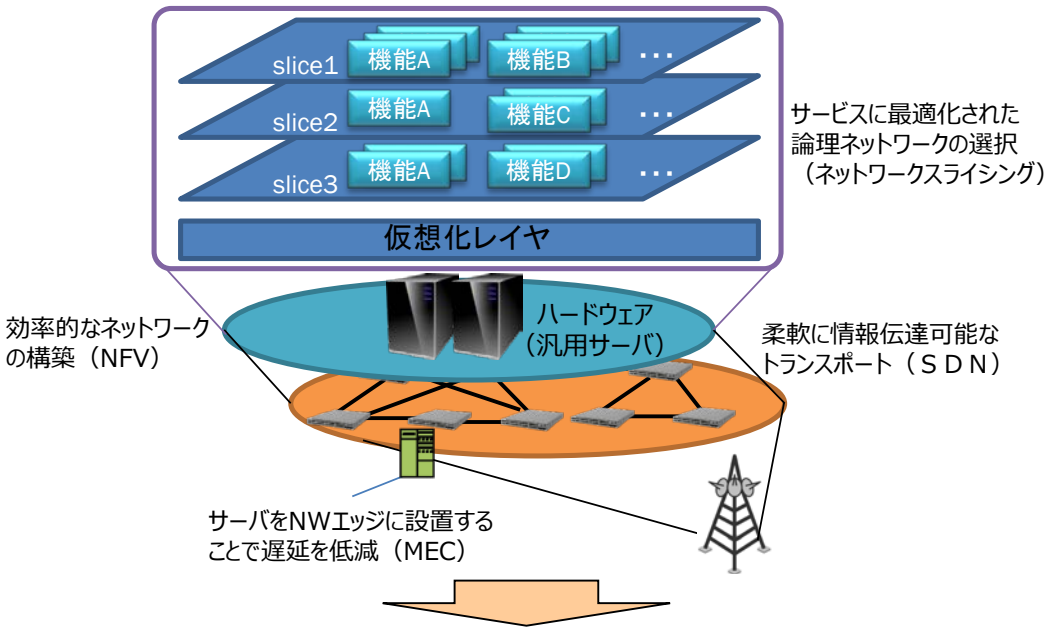




（外的要因の事故内訳）



＜ソフトウェア技術によるネットワーク機能を用いた構成例＞



サービスの提供に必要なネットワーク機能を他事業者に依存することが容易になる

LPWAサービスの概要及び事故報告基準の検討の論点

LPWA(Low Power Wide Area:低消費電力長距離通信)はIoT時代のネットワークとして注目され、進展が期待されている。

大量の機器が接続されるものであり、社会インフラ、農業、物流など様々な分野において、センサー機器等を用いた状態監視に利用される。通信頻度は、基本的には低頻度であり、分野によって10分に1回の場合や12時間に1回の場合など様々。

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。LPWAサービス(アンライセンス系)はアンライセンスバンドを利用することから、意図しない障害の発生を防ぐことは困難。

(1)LPWAサービスの事故報告基準の検討に際して、以下の点について整理が必要。

①アンライセンス系とセルラー系のLPWAサービスのネットワーク構成と、事故報告の対象範囲。なお、アンライセンス系のLPWAサービスにおいては、ライセンスバンドを利用することによる意図しない障害が必然的に発生する。

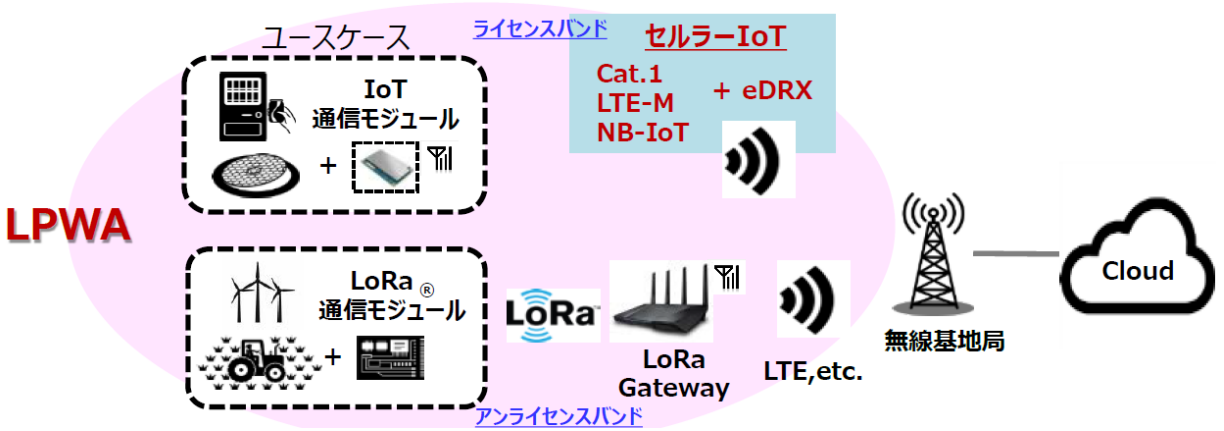
②事故報告基準における影響利用者数について、接続される機器の数と契約数のどちらを取り扱うべきか。また、事故の継続時間の報告基準については、LPWAサービスの通信頻度を踏まえるべき。(利用者数や時間といった基準ではなく、サーバ等コアネットワークの故障等が発生した際に報告を求めるのが良いかどうかを含め検討)

③LPWAサービスの特性(用途、通信頻度、機器数、影響度など)を考慮したものとすべき。

(2)卸提供事業者など他の事業者に起因する事故に関する情報共有体制の構築について検討が必要。

LPWAの特徴

- 低消費電力(バッテリー駆動で数年以上)
- 長距離通信(数百メートル~数キロ)
- 大量機器接続(大量機器の接続が可能)
- 低コスト(安価な機器・通信コスト)
- 少量データ通信(100bps~1Mbps)



LPWAの特徴等(第31回作業班におけるNTTdocomo説明資料より抜粋)

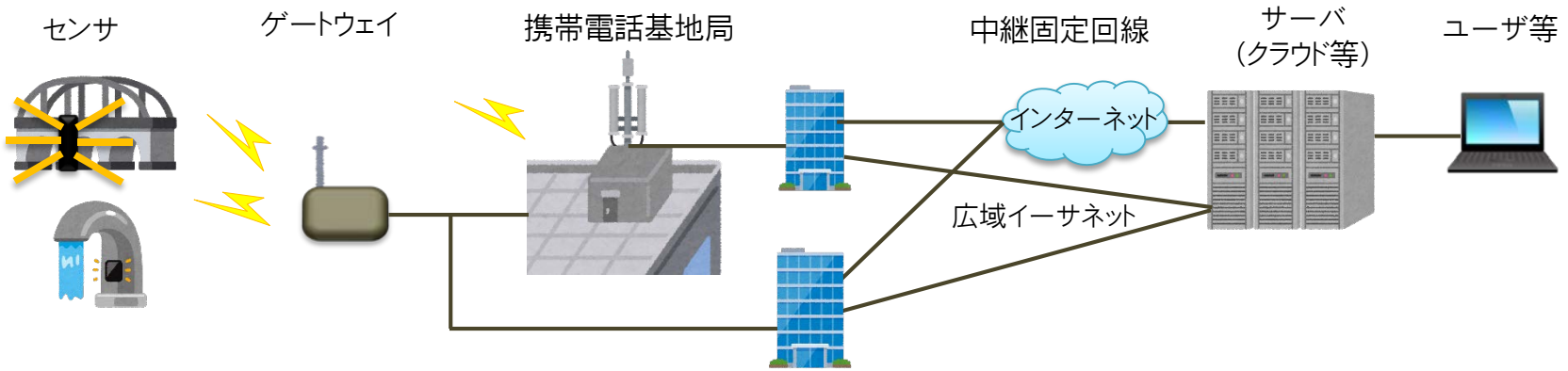
ＬＰＷＡサービス全般のネットワーク構成イメージ

LPWAサービス※は、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)があり、設備形態に違いはあるものの、どちらも目的用途は同じ。

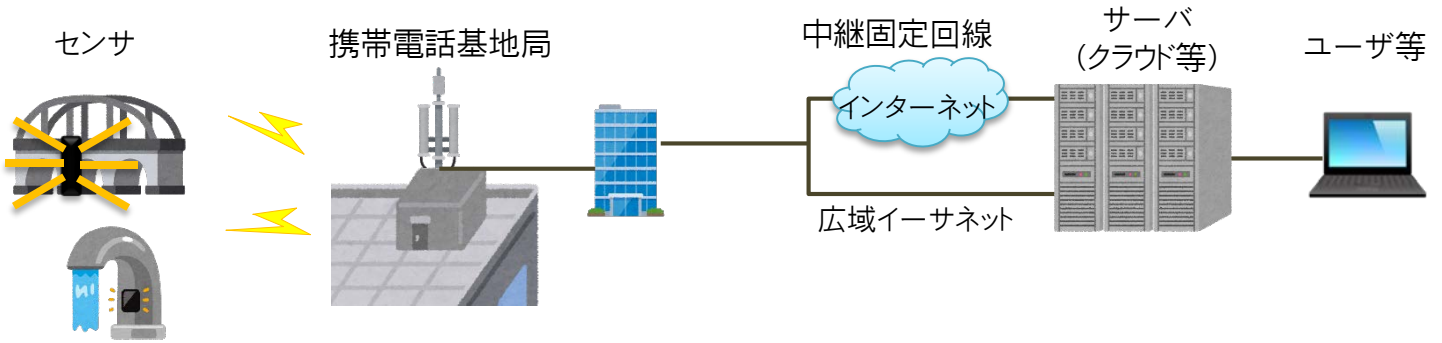
LPWAサービスのネットワーク構成イメージは次の通り。

※本資料においては、アンライセンス系又はセルラー系と明示しない限りは、両方を指す。

(アンライセンス系)



(セルラー系)



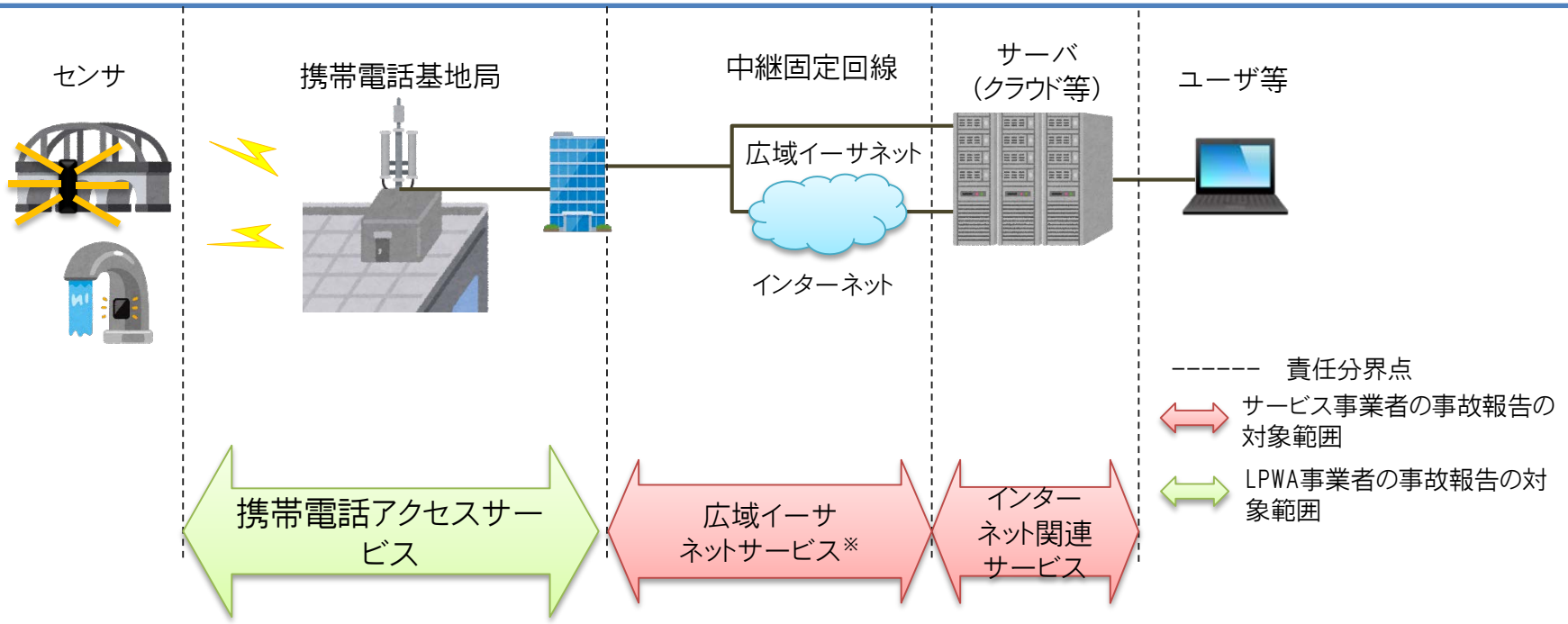
LPWAサービス（セルラー系）の事故報告の対象範囲

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。

本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。

そのため、既存の役務の基準にそって事故報告を求めることが適当。

＊LPWAサービス（セルラー系）については、既存の電気通信役務との切り分けが可能であって、エンドエンド（以降の整理に基づき、「契約単位」を指す。）で管理して提供される場合は、後述するLPWAサービスの事故報告基準に沿って事故報告を求めることとする。



※サーバ側のサービス事業者が携帯網等に閉域接続する広域イーサネットの卸提供等を受けてサービスを提供する場合、本区間も事故の対象区間となる。

インターネットを経由する場合は、LPWA事業者のサービスの範囲となるため、サーバ側の事業者の事故の対象区間に該当しない。

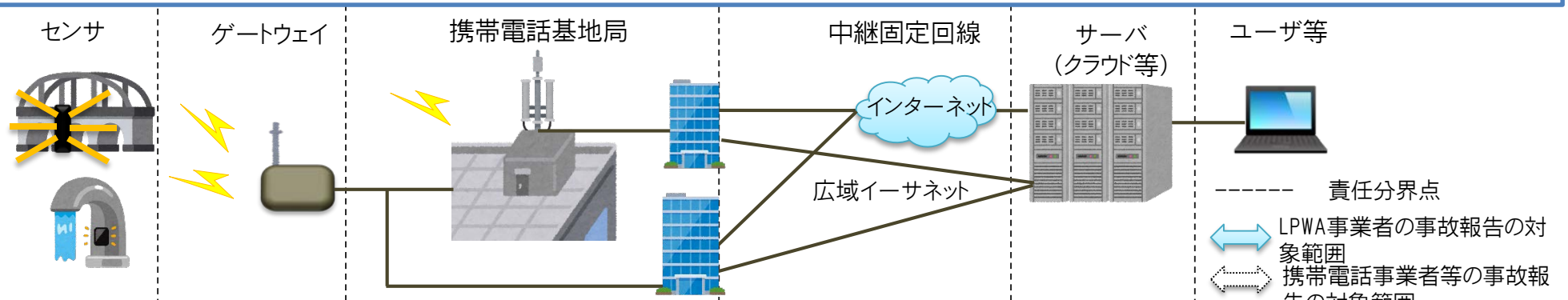
LPWAサービス（アンライセンス系）の事故報告の対象範囲

LPWAサービス（アンライセンス系）は、LPWA事業者がクラウドサーバ等を管理し、以下の4つのサービス形態によりLPWAサービスを提供することが想定される。

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であって、エンドエンド（契約単位）の通信の管理が可能な場合は、下図のとおり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、当該管理が困難な場合は、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。

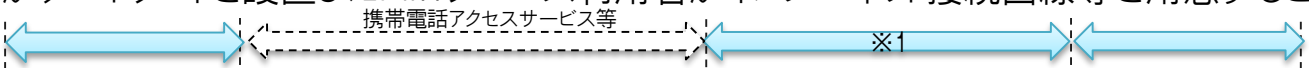
なお、センサーからゲートウェイの区間において、アンライセンスバンドに起因する混雑によってセンサーとの通信が遅延等した場合は事故の対象外となると考える。また、ゲートウェイの設備故障によってセンサーとの通信が停止した場合は事故の対象となると考える※。

※ゲートウェイを複数設置し、一部のゲートウェイの故障が生じた場合においても、他のゲートウェイを通じて、役務の停止が発生しない場合は事故としないことが適当と考える。



①LPWA事業者がゲートウェイを設置し、サーバまでの通信を一体で提供する場合

② LPWA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提供する場合



※1　LPWA事業者が携帯網等に閉域接続する広域イーサネットの卸提供等を受けてサービスを提供する場合、本区間も事故の対象区間となる。インターネットを経由する場合は、携帯電話事業者のサービスの範囲となるため、LPWA事業者の事故の対象区間に該当しない。

③LPWAサービス利用者がゲートウェイを設置し※2、LPWA事業者がサーバまでの通信を一体で提供する場合

※2　LPWAサービス利用者が設置したゲートウェイを他人に使用させる場合、当該利用者が電気通信事業者となり、LPWAサービスを提供する場合がある

④ LPWAサービス利用者がゲートウェイを設置し※2、インターネット接続回線等を用意することで提供する場合

LPWAサービスの事故報告基準における影響利用者数の考え方

LPWAサービスの接続形態や用途、また今後において想定されるサービス展開を踏まえ、LPWAサービスの事故報告基準における影響利用者数は、センサー端末等に割り当てられた回線数ではなく、契約数とすることが適切。

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となることを踏まえ、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を鑑みれば、個々の端末（モノ）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、そのモノに割り当てられた回線の数を、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サービスの展開が進むにつれて、センサー端末は膨大に増えていくと想定されるが、回線毎の管理ではLPWA事業者側の負担も同様に増えていくと考えられる。そのため、事業の発展性や柔軟性を阻害する懸念がある。

上記を踏まえ、同一の目的で利用される複数の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、必ずしも契約数によるカウントを求めるものではない。

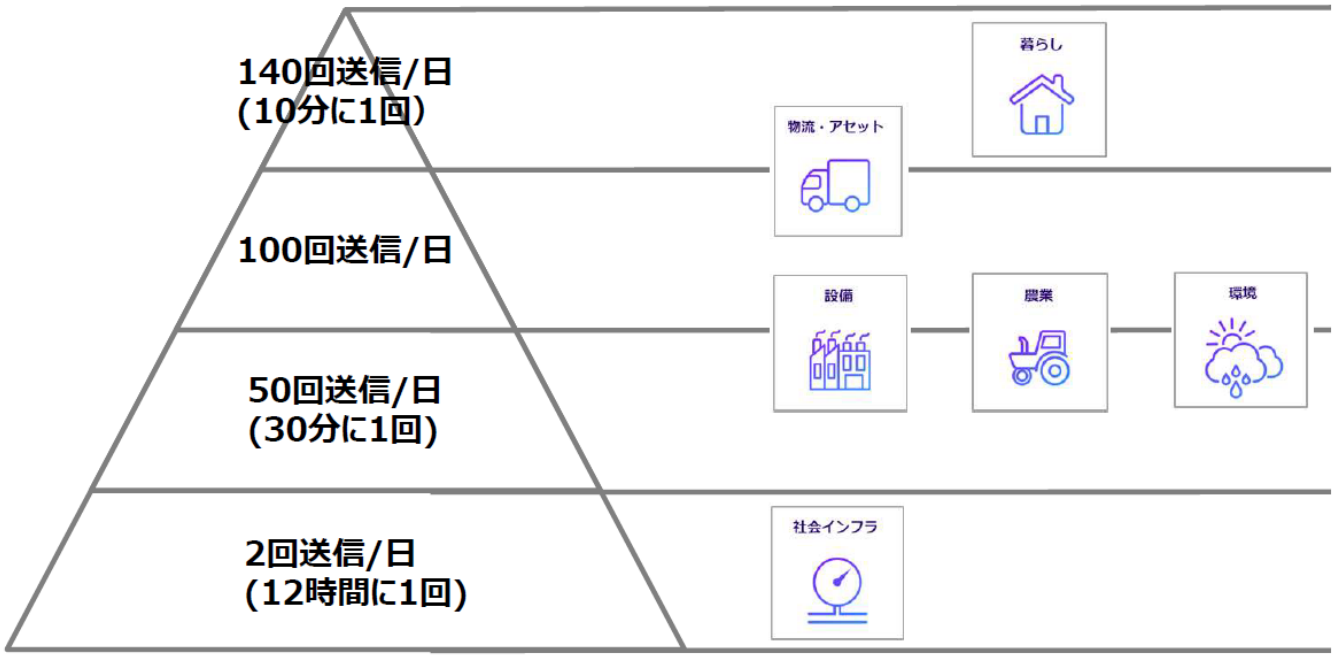
LPWAサービスの用途ごとの通信頻度を踏まえた事故報告基準の考え方

LPWAサービスの事故報告基準を検討する上で、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た上で、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。なか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を鑑みれば、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※。

※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。



用途と通信頻度
(第31回作業班における京セラコミュニケーションシステム説明資料より抜粋)

LPWAサービスの事故報告基準

LPWAサービスについて、以下に該当す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。
- 12時間以上役務の提供を停止又は品質を低下させた事故であって、3万以上の利用者※1が影響を受けたもの
- 2時間以上役務の提供を停止又は品質を低下させた事故であって、100万以上の利用者※1が影響を受けたもの

また、LPWAサービスについて、2時間以上役務の提供を停止もしくは品質を低下させた事故又は3万以上の利用者がその影響を受けた事故については、四半期毎に報告を求めることが適当と考えられる。

※1　LPWAサービスの場合、影響利用者数は契約数を指す。

LPWAサービスは、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※2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、事故が12時間以上継続するものとすることとし、また影響利用者数については他の役務と同様に、3万以上に影響を与えるものとすることが適当と考えられる。　※2　前ページの図「用途と通信頻度」参照。

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。そのため重大事故の基準として、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、100万以上に影響を与えるものとすることが適当と考えられる。

さらに、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。

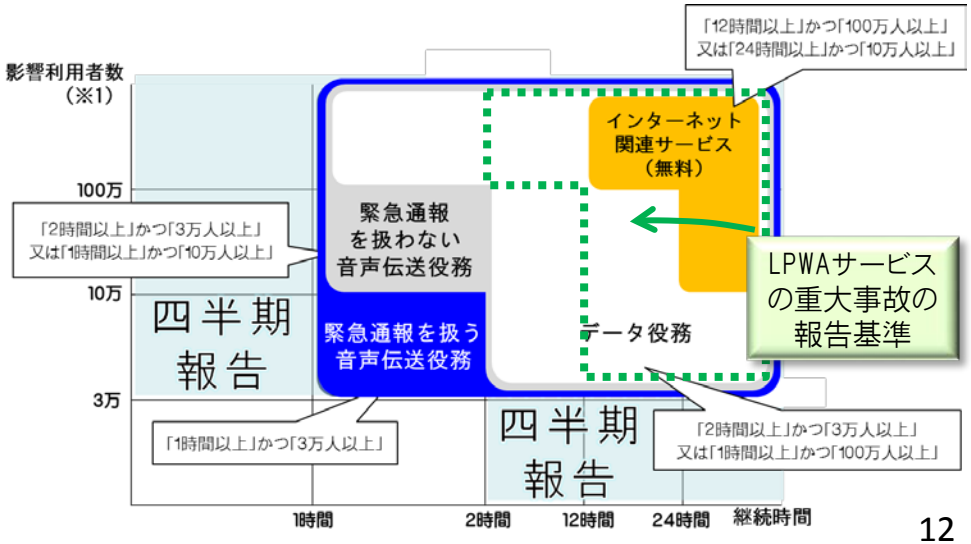
役務に一定の信頼性を確保する観点からも、四半期毎の報告は有効と考えられることから、LPWAサービスについても他の役務と同様に、事故が2時間以上継続した場合、または3万以上の利用者が影響を受けた場合に報告を求めることが適当と考えられる。

＊影響利用者数の算定は、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。

＊LPWAサービス提供事業者に卸電気通信役務を提供又は接続する事業者（中継系事業者）は、上記基準と同一とするとともに、影響利用者数の算定は、他の役務と同様に、可能な限りLPWAサービスの影響利用者数を用いることが適当と考える。

＊事故報告制度において、データ伝送役務（ベストエフォートサービス）について、現時点では、品質の低下は扱われていないことから、LPWAサービスについても同様。

＊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。



その他（バックエンド回線として利用する他事業者との障害の切り分け）

バックエンド回線を提供する他の事業者と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共有を含む連携を図るよう、情報通信ネットワーク安全・信頼性基準において推奨することが適当。なお、その他、LPWAサービス事業者にネットワークの安全・信頼性を確保するために同基準において推奨すべき対策があれば同様に整理する必要がある。

しかしながら、LPWAサービスはスタートされたばかりであり、実態を踏まえて、事業者に推奨すべき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、検討することが適当。

また、他事業者に起因する障害の場合、復旧までの時間が長期化することが考えられるものの、現行の他の電気通信役務においても起こりうるものであり、上記の連携を図りながら対応いただくことになると考える。

②大規模なインターネット障害発生時の対策の検討

（ア）障害情報の共有の在り方

大規模なインターネット障害発生時における障害情報の共有に係る課題と検討の論点

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事態に　おいては、利用者に対して大きな影響があるものであり、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。

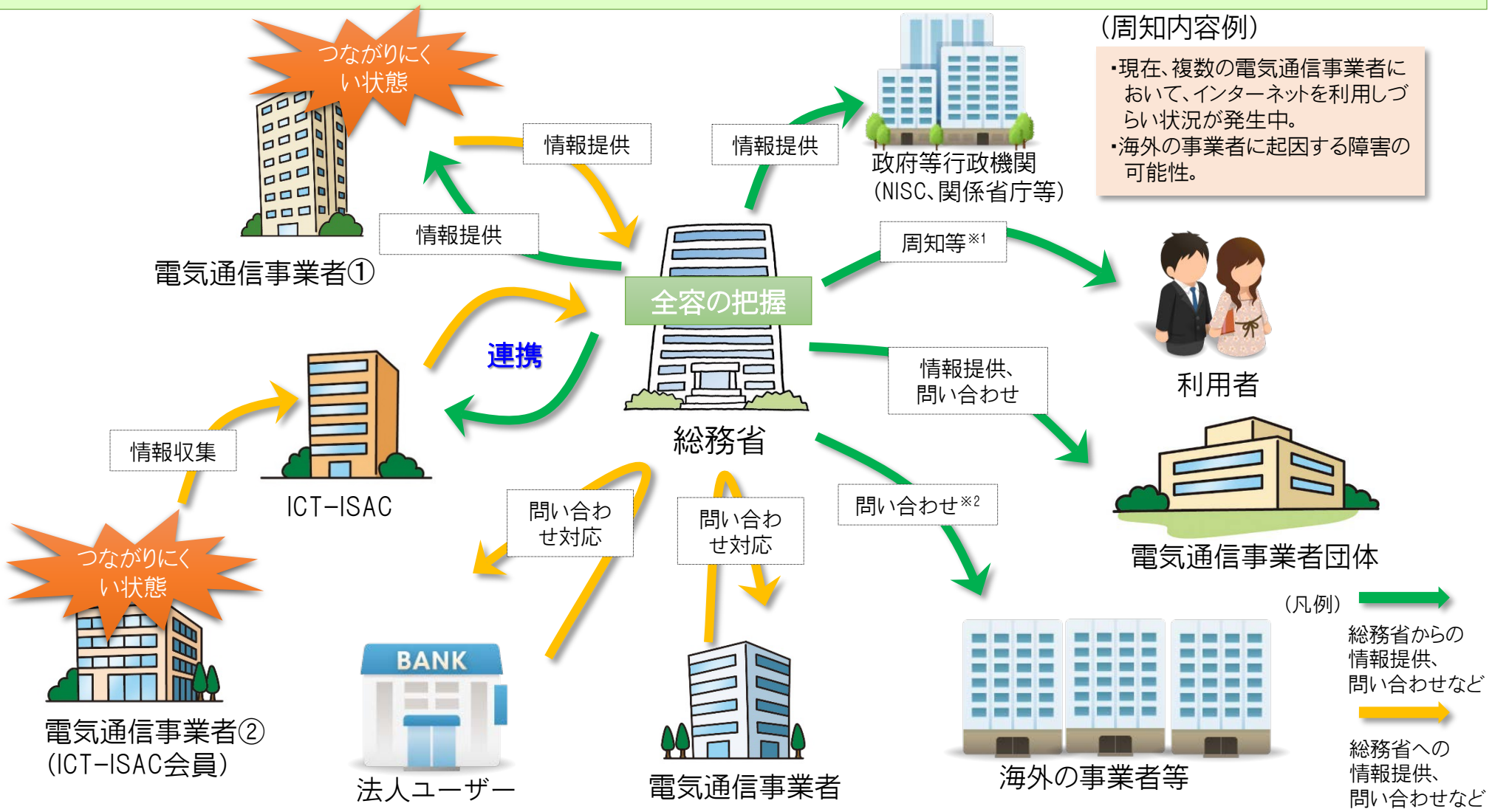
一方、事業者は、自らに発生した障害の原因が自らのネットワーク内にあるか外部にあるのか否かはすぐには判断できない、また自らの障害が原因で他の事業者のサービスや業務に障害が生じている場合において、その障害の規模や業務に与える影響の大きさを知ることは困難と考えられる。

他方、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、速やかな報告は現状求めていない。また、品質低下でインターネットに接続しづらい障害は、電気通信事故として取り扱う整理がなされておらず、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等情報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のではないか。

提供された障害情報の利用

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得られた障害情報をもとに、総務省において、全容の把握に努めるとともに、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。



※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。

情報提供された障害情報の総務省ＨＰにおける公表イメージ

提供された情報をもとに、総務省においても調査を行い、電気通信役務障害情報（速報）として総務省HPに公表。その後随時更新。

(1)〇△通信会社から総務省へ障害情報の提供

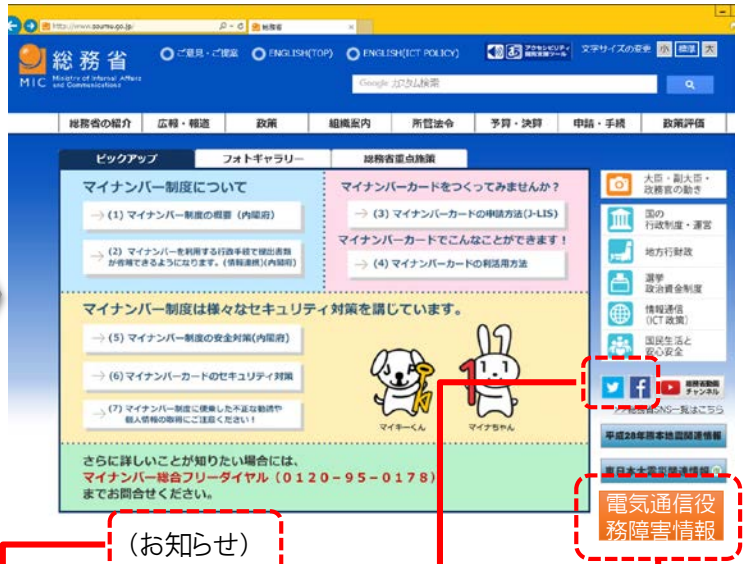
現在、一部のユーザーに、インターネットを利用しづらい状況が発生しており、他の事業者にも同様の事象が起きているかもしれないので、自社HPに利用者周知を行ったところ。海外の事業者に起因する障害と考えられる。
また、回線を提供している一部の法人ユーザーから重大な問い合わせを受けているところであり、その関係性を確認中。

(2)必要に応じてSNSやネットニュース等を活用し、該当すると思われる他の事業者や法人ユーザーの状況を総務省においても調査

（他事業者HPの記述）何らかの原因により、一部のユーザーに、インターネットを利用しづらい状況が発生しており、他の事業者にも。。。

（法人ユーザーHPの記述）当社サイトをご使用のお客様に多大な影響が出ています。

(3)総務省HPに「電気通信役務障害情報」のボックスを表示



障害状況の概要を掲載

(4)〇△通信会社から続報

問い合わせを受けている法人ユーザーの障害の重大な原因が当社によるものと判明した。なお、復旧はしていない。

(5)〇△株式会社から復旧の報告

原因が判明したため復旧措置を行い、復旧を確認した。

電気通信役務障害情報	電気通信役務障害情報	電気通信役務障害情報
・現在、複数の電気通信事業者において、インターネットを利用しづらい状況が発生しています。 ・海外の事業者に起因する障害と考えられます。	・現在、複数の電気通信事業者において、インターネットを利用しづらい状況が発生しています。 ・海外の事業者に起因する障害と考えられます。 ・一部の法人のサイトが閲覧しづらい状況が発生しています。	・現在、複数の電気通信事業者において、インターネットを利用しづらい状況が発生していましたが、復旧しました。

（注）上記は、続報や復旧報が最後まで寄せられる場合をイメージしたものであり、必ずしも全ての障害について、続報や復旧報を求めるものではない。

障害に係る情報共有の在り方に係る整理

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事態の早期沈静化を図るためには、障害発生時の情報共有が重要であるが、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ことが必要と考えられる。

（情報共有の在り方）

情報の内容

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を鑑みれば、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、右表の観点を考慮した上で提供されることが望ましい。

情報共有時に考慮いただくことが望ましい観点
利用者に広く周知可能な情報か
国民生活センター等に共有できる情報か
他の電気通信事業者に共有できる情報か

続報の必要性

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

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（総合通信局が既存の窓口の場合は総通局へ）とし、本省と総合通信局の間でも情報共有を行うこととする。

※　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。

個々の事項は、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。

②大規模なインターネット障害発生時の対策の検討

（イ）電気通信事業者等に推奨する対策

電気通信事業者等に推奨する対策の検討について

大規模なインターネット接続障害から得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及びその具体的な説明について整理を行った。また、以下の観点に留意し、安信基準への規定化や、解説への追記等についても検討をおこなった※。

＊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。個々の規定は基本的には汎用的な内容であるため、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、公表している。

（安信基準への規定化等の検討における留意点）

- ✓ 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、重要性を鑑み、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、重要性を鑑み、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、重要性を鑑み、分かりやすく明確な記載が必要と考えられる。

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、次ページ以降の【想定される安信基準等への反映】欄中の表においては、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。

（表の例）

設	特	他	自	ユ
◎	◎*	○	ー	ー

（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。
ー :対象外。

電気通信事業者等に推奨する対策及び制度への反映の検討結果

インターネットの経路設定時の人為的ミスの防止に係る対策

＊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があり、少なくともいずれかの実施を推奨。

（未然防止を前提とした手法）

・経路情報の設定作業において、容易に誤りが混入しないよう措置を講ずること（新）

・経路情報の設定に係る教育・訓練を実施すること（既）

（事後措置を前提とした手法）

・経路情報の設定後のトラヒックの疎通状況を監視し、異常等をアラートで知らせる機能を設けること（既）

・経路情報の設定に伴い、トラヒックの疎通に係る異常等が発生した場合を想定し、復旧対応手順を作成すること（既）

・経路情報の設定後に、トラヒックの疎通に係る異常等が発生した場合の対応について、教育・訓練を実施すること（既）

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に係る対策

・不要又は不正な経路情報の送受信を防ぐために有効な機能を設けること（新）

・経路情報の瞬間的かつ急激な増加を考慮した設計とすること（改）

・将来の経路情報の増加を考慮した設計とすること（改）

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に係る対策

・事故又は障害発生時に迅速な原因分析や状況把握等のため、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（新）

・契約関係等がある事業者（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（既）

ネットワーク構成に係る対策

・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こと等により、信頼性の向上を図ること（新）

利用者周知に係る対策

・インターネットにつながりにくい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（改）

（凡例）
（新） 安信基準に規定を新たに追加し、解説に具体内容を掲載する。
（既） 安信基準の既存の規定が存在する。なお、解説に具体内容を追記する。
（改） 安信基準の既存の規定に趣旨を追加する改正を行い、解説に具体内容を追記する。

インターネットの経路設定時の人為的ミスの防止に係る対策と解説（未然防止を前提とした手法）

＊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があり、少なくともいずれかの実施を推奨。

・経路情報の設定作業において、容易に誤りが混入しないよう措置を講ずること。

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を鑑みれば、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、複数体制によるチェックの徹底が重要である。

【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. (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を想定。

(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。	◎	◎	◎	―	―

・経路情報の設定に係る教育・訓練を実施すること。

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を鑑みれば、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。

【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. (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を想定。

(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。	◎	◎	◎	◎	◎

インターネットの経路設定時の人為的ミスの防止に係る対策と解説（事後措置を前提とした手法）

・ 経路情報の設定後のトラヒックの疎通状況を監視し、異常等をアラートで知らせる機能を設けること。

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を想定。

(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)	◎	◎	◎	○	○

・経路情報の設定に伴い、トラヒックの疎通に係る異常等が発生した場合を想定し、復旧対応手順を作成すること。

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。

【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. (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を想定。

(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。	◎	◎	◎	◎	◎*

・経路情報の設定後に、トラヒックの疎通に係る異常等が発生した場合の対応について、教育・訓練を実施すること。

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。

【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. (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を想定。

(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。	◎	◎	◎	◎	◎

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に係る対策と解説（その１）

・不要又は不正な経路情報の送受信を防ぐために有効な機能を設けること。

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た上で、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。

【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)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を想定。

(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。	◎	◎	◎	－	－

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に係る対策と解説（その２）

・経路情報の瞬間的かつ急激な増加を考慮した設計とすること。

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。

【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)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を想定。

(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	－	－

・将来の経路情報の増加を考慮した設計とすること。

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、ルーター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を想定。

(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。	◎	◎	◎	◎	◎

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に係る対策と解説

・事故又は障害発生時に迅速な原因分析や状況把握等のため、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。

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など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。

【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＞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を想定。

(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。	◎	◎	◎	○	○

・契約関係等がある事業者(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。

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。

【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＞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を想定。

(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。	◎	◎	◎	○	○

ネットワーク構成と利用者周知に係る対策と解説

・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こと等により、信頼性の向上を図ること。

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。

【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)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を想定。

(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。	―	―	―	○	○

・インターネットにつながりにくい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。

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。

【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＞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を想定。

(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電気通信事故報告制度に係るその他の検討

電気通信事故報告制度に係るその他の検討

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、そうしたサイバー攻撃を原因とする事故について、「第三者要因」の事故や「その他」の発生原因の事故として報告されているものの、当該報告の発生原因の分類としてサイバー攻撃を規定していないため、発生原因がサイバー攻撃であることが明確に示されない。

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。

※1　発生原因の詳細は関連規定を参照。

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」※2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。

※2　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。次頁参照。
（「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」のうち、新たに加えられた電気通信事業法第116条の2第1項第1号より抜粋。）。

技術検討作業班構成員（検討事項(3)関係）

	氏　名	主 要 現 職
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
	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
	高橋　　範	株式会社ソラコム　事業開発マネージャー
	西川　嘉之	UQコミュニケーションズ株式会社　渉外部　部長
	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 （第32回～） 小林　真寿美 （～第31回）	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
	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
	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

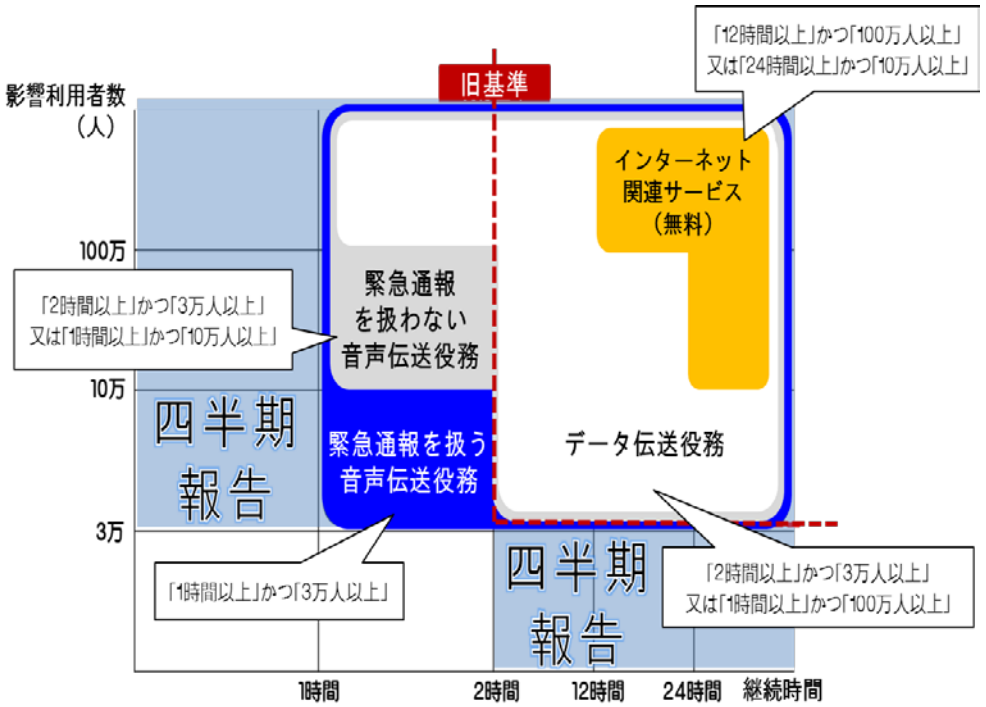
参考資料

（検討課題①）電気通信事故の報告基準について

法令上、**総務省への報告義務**のある**電気通信事故**（電気通信設備の故障により電気通信役務の提供を停止又は品質を低下させた事故）は、次の二つに大別。

① **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

② **重大な事故**：継続時間及び影響利用者数が①「**緊急通報を扱う音声伝送役務**」、②「**緊急通報を扱わない音声伝送役務**」、③「**インターネット関連サービス（無料）**」、④「**データ伝送役務**」の**4区分毎に設定した基準を超える事故**
→ 事故発生後30日以内に報告



○電気通信役務の提供を停止又は品質を低下させた事故で、次の表の基準に該当するもの

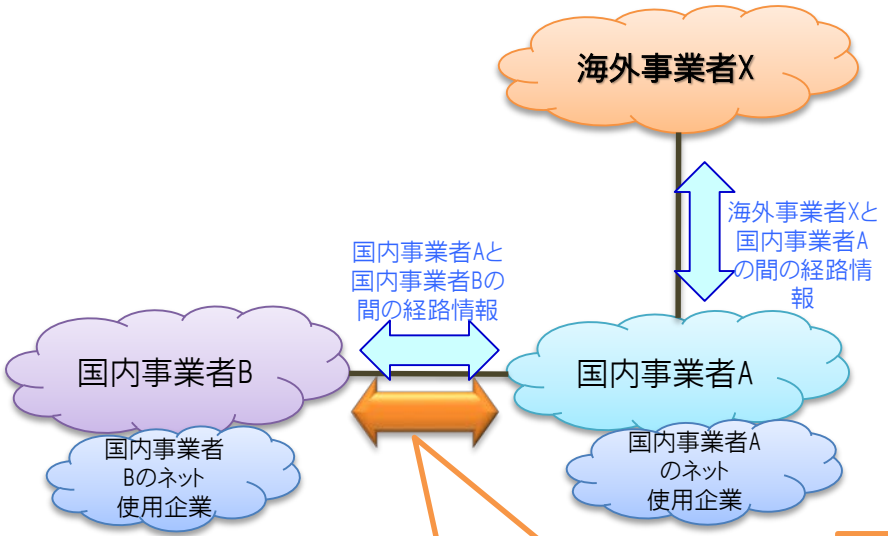
電気通信役務の区分	時間	利用者の数
一　緊急通報を取り扱う音声伝送役務	1時間	3万
二　緊急通報を取り扱わない音声伝送役務	2時間	3万
	1時間	10万
三　利用者から電気通信役務の提供の対価として料金の支払いを受けないインターネット関連サービス（音声伝送役務を除く。）	24時間	10万
	12時間	100万
四　一の項から三の項までに掲げる電気通信役務以外の電気通信役務	2時間	3万
	1時間	100万

○電気通信事業者が設置した衛星、海底ケーブルその他これに準ずる重要な電気通信設備の故障により、当該電気通信設備を利用する全ての通信の疎通が2時間以上不能となる事故

（検討課題②）昨年8月に発生した大規模なインターネット接続障害

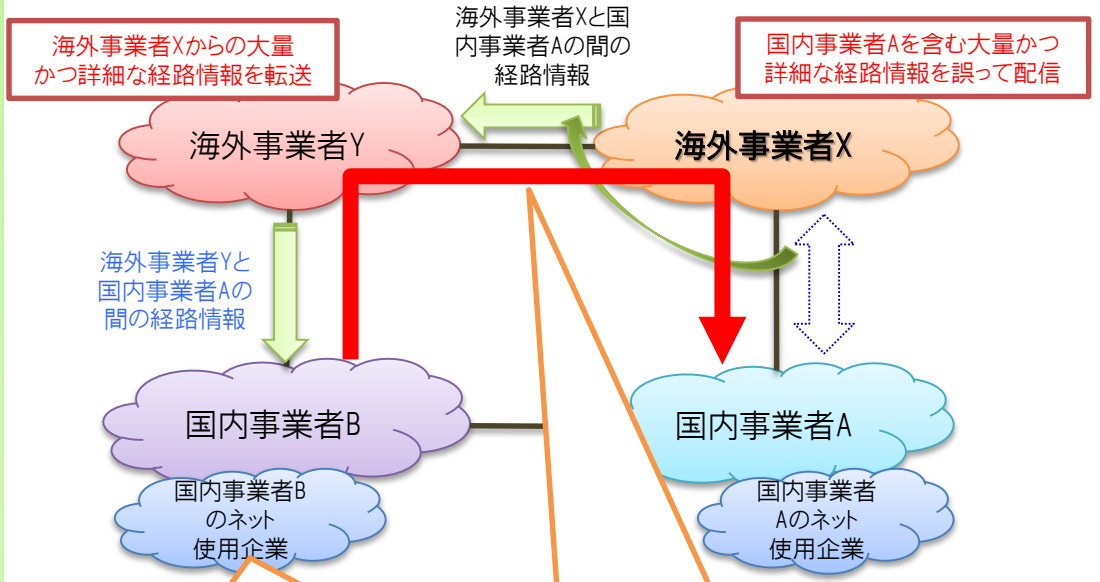
- 昨年8月25日、海外事業者Xが行う通信経路設定の誤りが原因となり、我が国の電気通信事業者（国内事業者A、国内事業者B）の一部の回線や設備に過大な負荷がかかったことにより、インターネットに障害が発生

本来の通信経路



国内事業者Aと国内事業者B間の通信は、経路情報に従い最短の国内ルートを通過

今回の障害時の通信経路



大量の経路情報を処理しきれず、法人ユーザー収容ネットワークで一部不安定事象発生
（ルータの再起動により解消）

国内事業者Aと国内事業者B間の通信は、経路情報に従い海外事業者（海外事業者X及び海外事業者Y）のネットワークに回り込むルートを通過
⇒通信に遅延が発生
（海外事業者Xが修正したことにより解消）

本事象の発生原因は、ネットワーク技術者レベルでの情報交換を通じて、推定はできたが、判断がつかなかったため、利用者への情報提供に苦慮

（検討課題②）経路情報の誤りによるインターネット障害の発生状況

発生年月	発生場所	発生事象
2017年11月	米国、カナダ、ブラジル、アルゼンチン、アラブ首長国連邦	米国のTier1事業者であるLevel3 Communicationsが、本来配信する予定でなかった数千もの詳細な経路情報を誤設定により契約事業者に配信したことにより、米国大手ISPであるComcast、カナダ大手ISPであるBell Canadaや、大手コンテンツプロバイダであるNetflix宛ての通信がLevel3 Communicationsを回り込むこととなり、ComcastやBell Canadaだけではなく、ブラジル、アルゼンチン、アラブ首長国連邦のISPに約90分のインターネットの遅延が発生。 【出典:Dyn (Doug Madory) "Widespread impact caused by Level 3 BGP route leak" Nov7,2017
2015年6月	マレーシア	マレーシアのISPであるTelekom Malaysiaが、Level3 Communicationsに約17万9千もの経路情報を配信したが、当該経路情報はTelekom Malaysiaを回り込む経路となってしまったため、世界中で約2時間インターネット接続の遅延が発生。 【出典:BGP MON "Massive route leak causes Internet slowdown" Jun12, 2015】
2014年8月	米国及びカナダの一部地域	大手ISPのルータのグローバルルーティングテーブルに15,000件の新しい経路情報が追加されたことにより、ルータのメモリ容量が不足し、ルータの処理遅延が発生。 これにより、インターネット通信が不安定となり、一部のサイトが全く読み込まれない事象が発生。 【出典:ZDNet Japan「米国全土でインターネットサービスの途絶が発生-BGPルーティングテーブルの巨大化で」Aug15,2014】
2012年8月	カナダ	カナダのISPであるDery Telecom IncがVIDEOTRONから配信された10万超のASパスの長い経路情報をBellに配信し、Bell(あるいはDery Telecom)のフィルタが最適に稼働しなかったことにより、ピア接続しているインドのTataをはじめとする事業者にそのまま配信され、BellやTataのインターネット接続に障害が発生。 【出典:BGP MON "A BGP leak made in Canada" Aug8, 2012】
2012年2月	オーストラリア	オーストラリアの大手ISPであるTelstraとトランジット契約をしているDodoが、設定誤りによりTelstraへの経路をインド経由する設定としてしまい、約30分インターネットに接続しづらい状況が発生。 【出典:BGP MON "How the Internet in Australia went down under" Feb27, 2012】
2009年2月	チェコ	チェコのISPがルータのバグあるいは設定不良により、同じAS番号を多く連結された不適切なAS Pathを配信したことにより、一部の処理能力の低いルータが機能停止。 これにより、一部のISPにおいて約1時間インターネットが接続できなくなった。(Long AS Path事件) 【出典:(独)情報処理推進機構 情報セキュリティ技術動向調査(2009年上期)】

（検討課題②）電気通信事故検証会議の開催

「事故が大規模化・長時間化し、その内容・原因等が多様化・複雑化する中で、その検証作業も複雑化・高度化している状況にあるため、事故報告の検証は、外部の専門的知見を活用しつつ、透明性の高い形で行われることがこれまで以上に重要となっている。」【「多様化・複雑化する電気通信事故の防止の在り方について」報告書（平成25年とりまとめ）】

電気通信事故検証会議の設置（平成27年5月～）

○ 通信工学、ソフトウェア工学、システム監査、消費者問題の有識者で構成。（任期中の構成員氏名を非公表とするとともに、守秘義務を課している。）

○ 会議及び議事録は非公開（議事要旨、配付資料等は原則公開。ただし、当事者又は第三者の権利、利益や公共の利益を害するおそれがある場合は議事要旨又は配付資料の全部又は一部を非公開とすることができる。）

重大な事故報告

四半期事故の報告

電気通信事業者・総務省の実施対策の評価
⇒ **毎年度年次報告書をとりまとめ**

事故発生事業者へのフィードバック

業界内共有
フォローアップ調査

ガイドライン等へ反映

（検討課題②）大規模なインターネット接続障害から得られた教訓

昨年10月から11月に、電気通信事故検証会議において発生した事象や対応状況を検証し、その結果得られた教訓が以下の4つの観点から整理された。

人為的ミスの未然防止

- 経路情報の設定においても、人為的ミスを防ぐための事前・事後のチェック体制の充実が必要
- 万一誤設定してしまった場合でも、設定が反映される前に自動的に検証し、アラームなどで知らせるような仕組みが有効

誤送信された膨大かつ詳細な経路情報の受信防止及び不要な経路情報の送信防止

- リミッターによる大量な経路情報を受信しない設定や、フィルターによる不要な経路情報を送受信しない設定が有効

→ **「情報通信ネットワーク安全・信頼性基準」等に規定することが適当**

障害に関する情報の電気通信事業者間での共有

- 複数の電気通信事業者に影響のあるインターネット障害の対応において、ネットワーク技術者間のメーリングリスト（JANOG）等による情報交換や、ICT-ISACの「経路奉行」の取組による検知結果の共有といった取組みが一定程度行われているが、事案の詳細を迅速かつ正確に把握し、短時間での収束を図るには、より緊密に電気通信事業者間で連携した情報共有体制の整備が必要
- 電気通信事業者と総務省が連携することで、より効果的な情報共有と的確な対応策の検討が可能となると考えられ、総務省が情報共有の結節点となることも有効

利用者周知

- 複数の電気通信事業者に影響のあるインターネット障害の対応においては、利用者周知の観点からも、電気通信事業者間の連携、電気通信事業者間と総務省の連携強化により、迅速な情報収集ができる体制が必要

→ **総務省への障害報告の在り方を含め、障害に関する情報共有体制の整備を行うことが適当**

（検討課題②）本事案に係る電気通信事故の該当性

電気通信事故の定義

○電気通信設備の故障により、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させた事故（電気通信事業法施行規則58条）

※　インターネット接続サービスは、継続時間が2時間以上かつ影響利用者数が3万以上の場合に「重大な事故」に該当

（参考）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

○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、「役務の提供の停止」とする。

※　ベストエフォートサービスの場合は、品質の低下の定義が確立していない。

事業者への確認結果

利用者とのリンク又はセッションは切れていなかった

電気通信事故には該当しない

（検討課題②）
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（抜粋）

➢ 総務省は、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取りまとめられた「対応の方向性（案）」について、昨年12月27日から本年1月18日まで意見募集を実施。意見募集の結果等を踏まえ、本検討会において「対応の方向性」が以下のとおり取りまとめられた。

○基本的な考え方

通信ネットワークに関わる者全体が連携することが肝要。

関係者が連携してインターネットの障害の防止や予防を図るためには以下の対応が必要。

【対応の方向性】①電気通信事業者によるDDoS攻撃等の事前予防
②情報共有と相互連携
③IoT機器等の端末設備のセキュリティ対策

推進の際は通信の秘密やプライバシー等に十分な配慮が必要。また、国民のセキュリティ意識の醸成も必要。

○大規模なインターネット障害発生時の対策

【対策】
- 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

【課題と今後の対応】

ガイドライン等において<u>ルータの設定につき規定</u>するとともに、<u>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</u>を検討。

（検討課題②）電気通信設備の安全・信頼性の確保に関する基準

○　通信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、**安全・信頼性確保に関する制度**を設けている。

強制基準

技術基準

＜事業用電気通信設備の技術基準＞
事業用電気通信設備規則（耐震対策、防火対策、停電対策　等）

＜利用者が接続する端末設備等の接続の技術基準＞
端末設備等規則（安全性、電気的条件、責任の分界　等）

自主基準

管理規程

＜事業者ごとの特性に応じた基準＞
業務管理者の職務、組織内外の連携、事故の報告、記録、措置、周知　等

ガイドライン

安全・信頼性基準

＜努力目標として、全ての電気通信事業者の指標となる基準＞
ソフトウェアの品質検証、事故状況等の情報公開、ネットワーク運用管理（運用基準の設定、委託保守管理）　等

監督責任

統括管理者

＜経営レベルの設備管理＞
経営陣から選任、事故防止対策に主体的に関与

主任技術者

＜事業用電気通信設備の「工事、維持・運用」を監督＞
電気通信事業者が資格証の交付を受けている者から選任

工事担任者

＜端末設備等の「接続に係る工事」の実施等＞
資格者証の交付を受けている者が端末設備等の接続に係る工事を実施又は実地で監督

報告義務

事故報告

＜事故の影響度に応じ、期限内に所定の様式で報告＞
重大な事故…30日以内に、事故の概要、原因、再発防止策等を詳細に報告
四半期事故…四半期ごとに、事故の概要を選択肢式で報告

（検討課題②）情報通信ネットワーク安全・信頼性基準概要

● 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・信頼性に関する推薦基準（ガイドライン）を作成。

安全・信頼性基準

設備等基準・・・ 情報通信ネットワークを構成する設備及び情報通信ネットワークを構成する設備を設置する環境の基準（65項目165対策）

設備基準 47項目116対策	1.一般基準 （15項目65対策）	2.屋外設備 （17項目22対策）	3.屋内設備 （8項目13対策）	4.電源設備 （7項目16対策）
環境基準 18項目50対策	1.センタの建築 （4項目13対策）	2.通信機器室等 （6項目22対策）	3.空気調和設備 （8項目15対策）	

管理基準・・・ 情報通信ネットワークの設計、施工、維持及び運用の管理の基準 （ 43項目174対策）

方針 9項目9対策	1.全体的・部門横断的な設備管理 （3項目3対策）	2.関係法令等の遵守 （1項目1対策）	3.設備の設計・管理 （2項目2対策）	4.情報セキュリティ管理 （3項目3対策）
体制 18項目45対策	1.情報通信ネットワークの管理体制 （2項目8対策）	2.各段階における体制 （16項目37対策）		
方法 16項目120対策	1.平常時の取組 （13項目98対策）	2.事故発生時の取組 （2項目16対策）	3.事故収束後の取組 （1項目6対策）	

(1) 情報セキュリティポリシーの策定 → 情報セキュリティポリシー策定のための指針

(2) 危機管理計画の策定 → 危機管理計画策定のための指針

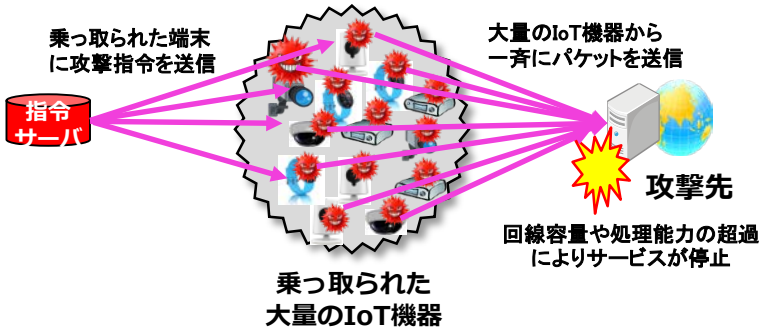
（検討課題③）送信型対電気通信設備サイバー攻撃の範囲について

送信型対電気通信設備サイバー攻撃

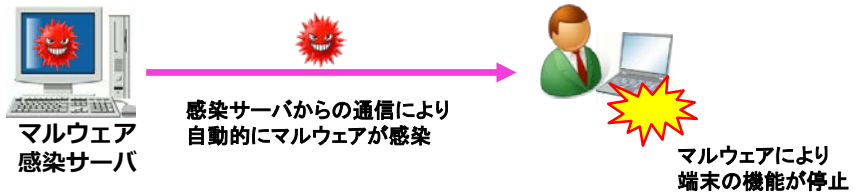
- 「送信型対電気通信設備サイバー攻撃」とは、以下を満たすものをいう。
  - ① **サイバー攻撃**（通常の通信によるトラフィック集中等は含まない。）**のうち、**
  - ② **電気通信設備**（電気通信事業者の電気通信設備及び利用者の端末）**を攻撃の対象とし、**
  - ③ **その機能に障害を与える通信の送信により行われるもの**（受信者の行為が介在することにより障害が発生する場合は該当しない）。
- **また、上記の通信の送信を行う指令を与える通信の送信**（C&Cサーバからの攻撃指令等）**も含まれる。**

該当する例

例①：DDoS攻撃



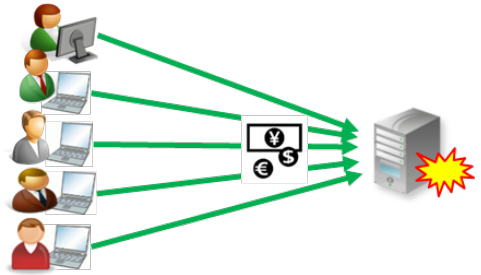
例②：マルウェア感染による機能障害



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。

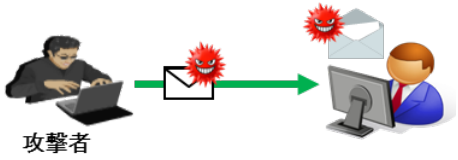


例②：不正アクセス

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。



（検討課題③）関連規定

◆電気通信事業法施行規則（重大事故報告）

➢ 第五十八条　法第二十八条の総務省令で定める重大な事故は、次のとおりとする。

一　次の表の上欄に掲げる電気通信役務の区分に応じ、それぞれ同表の中欄に掲げる時間以上電気通信設備の故障により電気通信役務の全部又は一部（付加的な機能の提供に係るものを除く。）の提供を停止又は品質を低下させた事故（他の電気通信事業者の電気通信設備の故障によるものを含む。）であつて、当該電気通信役務の提供の停止又は品質の低下を受けた利用者の数（総務大臣が当該利用者の数の把握が困難であると認めるものにあつては、総務大臣が別に告示する基準に該当するもの）がそれぞれ同表の下欄に掲げる数以上のもの　（以下略）

➢ 重大な事故の報告書様式（様式第50の3）

注5「発生原因」の欄は当該事故の発生の原因となった電気通信設備又は行為がどのような影響を与えて事故を発生させたのか記載し、大規模化・長時間化した原因についても記載すること。

◆電気通信事業報告規則（四半期毎の事故報告）

➢ 第七条の三　電気通信事業者は、次の各号に該当する事故が発生した場合は、様式第二十七により、毎四半期経過後二月以内に、その発生状況について、書面等により総務大臣に提出しなければならない。ただし、総務大臣が別に告示する事故については、総務大臣が別に定める様式により提出することができる。

一　電気通信設備の故障により電気通信役務の全部又は一部（付加的な機能の提供に係るものを除く。）の提供を停止又は品質を低下させた事故（他の電気通信事業者の電気通信設備の故障によるものを含む。）であつて、次のいずれかに該当するもの　（以下略）

➢ 四半期ごとの事故発生状況の報告書様式（様式第27）

7 「主な発生原因」の欄は、「自然故障」、「ソフトウェア不具合」、「異常トラヒック」、「人為要因」、「他の電気通信事業者の事故による要因（卸電気通信役務を提供する電気通信事業者、接続先の電気通信事業者、その他）」、「停電（通常受けている電力の供給の停止）」、「自然災害」、「火災」、「第三者要因（道路工事による断線、車両による断線、その他）」、「不明」又は「その他」の中から該当するものを記載すること。