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　事故報告・検証制度等タスクフォース（第１回）

議事要旨

１　日時

令和３年３月11日（木）10時00分～12時00分

２　場所

Web開催

３　出席者（敬称略）

（１）タスクフォース構成員

内田　真人（主任）、石田　幸枝、井ノ口　宗成、落合　孝文、熊取谷　研司、高口鉄平、実積　寿也、蔦　大輔、中尾　彰宏、林　秀弥、引地　信寛、深村　有史、福智　道一、向山　友也、吉岡　克成

（２）オブザーバ

日本電信電話株式会社、東日本電信電話株式会社、西日本電信電話株式会社、NTTコミュニケーションズ株式会社、株式会社NTTドコモ、KDDI株式会社、ソフトバンク株式会社、楽天モバイル株式会社、ケーブルテレビ株式会社、スカパーJSAT株式会社、電気通信サービス向上推進協議会、田中　絵麻（明治大学/IPネットワーク設備委員会委員）、押立　貴志（法政大学大学院）、内閣サイバーセキュリティセンター、内閣府（防災担当）ほか

（３）総務省

恩賀　一（安全・信頼性対策室長）、村上　理一（安全・信頼性対策室課長補佐）、西室　洋介（電気通信技術システム課課長補佐）、中溝　和孝（サイバーセキュリティ統括官室参事官（総括担当））

４　議事

（１）開会

・内田主任より、３月５日に開催されたＩＰネットワーク設備委員会において、本タス

クフォースの設置を承認され、安心・安全で信頼できる情報通信ネットワークの確保のための事故報告・検証制度等の在り方に関する検討を始める旨、及びWeb会議による開催の旨説明があった。

（２）議事

（２－１）事故報告・検証制度等タスクフォースの運営方針（案）について

・事務局（西室課長補佐）より、資料１－１－１に基づき、本タスクフォースの運営方針等について説明があった。

・内田主任より、林構成員が主任代理に指名された。

（２－２）事故報告・検証制度等に関する現状と課題等について

・事務局（恩賀室長）より、資料１－２－１に基づき、３月５日に開催されたＩＰネットワーク設備委員会における本タスクフォースに関する主な意見について説明があった。

・事務局（恩賀室長）より、資料１－２－２に基づき、電気通信事故の報告・検証制度等に関する現状と課題について説明があった。

・説明終了後、各構成員から電気通信事故の報告・検証制度等に関する現状と課題等について意見が述べられた。主な意見は以下のとおり。

○技術の進化とともに実現できるサービスのレベルは変化していくため、その時代に合った事故報告・検証の在り方を常に見直していくべき。

○電気通信事業法が誕生してから３５年が経ち、ネットワークの根本は同じでもその機能は大きく変化している。ソフトウェア化・クラウド化により、消費者だけでなく事業者自身も原因がわからない事故が起こることなど、当時は想定していなかったのではないか。制度の見直しは常に行っていかなければならない。

○情報通信を取り巻く環境が多様化し、時代に応じた事故報告・検証制度は必要。事業者にとってもウィン・ウィンとなるような仕組みについて建設的な議論が重要である。

○デジタル時代、サイバーフィジカルでのインフラはどういうものかという議論の中で通信が一つの重要な柱になる。社会的なインフラとしての必要性がより一層高まる中、事故に関する情報については、政策形成に必要な情報収集、事故の対処や利用者保護等のため

に必要となり、利用者保護はtoCだけではなくtoBも重要である。例えば、医療、金融や交通等では、通信を使えるということを前提に可用性の確保等々を行うこともあるため、こういった点も踏まえ、情報収集や開示のタイミングをどうするかというのは様々な活動の基礎になる。これらを合理的に、過度な負担にならないような形で実施することが重要である。

○事故の報告や検証については、海外では災害時において進んでいるＡＡＲ（After Action Review）の考え方も参考に、責任追及を目的とするのではなく、何がボトルネックで発生したのか、改善点はどこか等を振り返り、同じことを繰り返さないようにすることが重要である。

○事故報告・検証制度は犯人捜しが目的ではないことを明確にすべき。インターネットのように、失敗を重ねて改善していくというサービスについては、事故が起こった際は、失敗の原因を明確にし、それに対してパッチを当てていくことが重要。

○失敗の経験を生かすという意味でも、事故検証の結果をきちんと公開し、社会全体の知恵、ノウハウにしていくことが大事。そのアウトプットが事業者自身のビジネスモデルの中に位置づけられ、利潤最大化、社会貢献につながるようにする必要があり、事業者にとって利用しやすい制度にするべき。

○情報共有には２つ手段がある。１つ目が任意の情報提供であり、検証会議に近い。２つ目は義務を課して報告頂き、その形で情報共有するもので事故報告制度になる。前者は、何で情報提供してもらうのか、インセンティブが非常に大事であり、報告させること自体が目的というのはよくない。情報提供をすると提供者にどういういいことがあるのかをできる限り設計していく必要がある。後者は過度な負担になってはいけない。サイバーセキュリティの文脈で情報共有は結構活発にされているが、多くの体制があり、関係者が情報共有に疲れている状況も若干生じている。事故報告制度は、それ自体は大事だが、何のために報告するのかという目的をはっきりすることと、情報共有疲れにならないよう、過度な負担にならないようにするということも大事。

○起こってしまった事故の背景を理解するためには、事業者がどういう対応を行い、その結果、しょうがなく事故は起こるが、その背景の情報として、技術の問題なのか運用の問題なのか等、事故の背景を把握し、次の事故を未然に防ぐ方策をとることが、健全な在り方である。

○総務省において進めているＡＩを活用した障害検知プロジェクトがあるが、こういった

ものを通信事業者も使えるようになれば、より迅速に障害検知ができる可能性がある。障害検知技術の進化も見据えた上で、事故検証や事故を未然に防ぐ施策を考えていく必要がある。

○自然災害やサイバー攻撃は予期できない、いわゆる想定外のため、ＯＯＤＡループを取り入れていくということに賛成。ＯＯＤＡループでは観察が必要だが、そのためには事業者間、他業種とも情報共有することが必要になる。幅広く情報を収集するためには、報告する事業者の負担が大きくならないよう配慮が必要。報告すると面倒だということになると、報告自体が上がってこなくなってしまう恐れがある。

○事故の報告が面倒くさいということもあるため、事業者が事故を報告した場合、それをヒアリングして、ある一定の方向性にまとめてくれるような中立な機関を設立するのも一つの案である。

○複数の事業者の契約関係の問題等が背景にあった重大事故があった。一般消費者は通常つながると思っているので、つながらないという問題はかなり問題になってくる。また、ＩｏＴ化により様々なものがネットワークに接続されることで、責任の所在が分からない事故が起きてくる。現在重大事故に該当しない事故についても、早期に情報を集め、それをどのように発信していくか考える必要がある。

○通信の先にどのようなサービスが繋がっているのか、その通信に対する利用者の依存度等の質の問題についても、クリティカルなインフラとしての観点から、事故の重大性を評価等できるとよい。

○テクニカルには同じ事故でも、その事故によりどのようなサービスに影響が出たかにより、社会的影響は大きく異なる。ＢtoＢtoＸの「Ｘ」の部分など、事故の先にあるサービスまで視野を広げて事故報告・検証制度の在り方を考えなければならない。

○インターネットに接続しづらい障害等、把握そのものが難しい障害についても事故報告の対象として見ていく必要がある。

○通信品質が低下してその上のアプリが使えなくなることが、昔で言う電話が繋がらないことと同じ意味を持つようになりつつある。繋がってはいるものの、十分な性能を発揮しない状況についても、同様に対応する必要が出てきている。

○「重要な」事故か否かの判断に、是非利用者の感覚を入れたい。品質低下によりアプリが使えなくなるケースでは、通信事業者からすれば通信は繋がっているという判断だが、重要なのは、最終利用者がサービスを利用できるかどうかであり、利用実態に即した判断が

求められる。

○これまで重大事故は、影響時間や、事業者から直接見える影響利用者数の基準で決まっていたが、これは事業者目線に偏った基準になっている。重大事故の基準を見直す上で、利用者目線は不可欠である。例えば、欧州の欧州電気通信コード指令における事故報告制度は、利用者目線となっている。

○最終エンドユーザへの影響を考えることが重要である一方、ＢtoＢtoＸのミドルＢには通信障害の報告に関する責任がないか、又は間接的な責任しかない。この会社にどの程度の報告義務を課すべきか難しい問題で、自主的に報告していただくのが望ましい。

○行政も関わりつつ、ステークホルダー間で連携して障害を把握する仕組み等、ソフトな事故検証の在り方も今後は考えていく必要がある。

○Ｓｏｃｉｅｔｙ５．０において、フィジカル空間のセンサーの膨大な情報がサイバー空間に集積されるようになり、事業者の情報収集や報告の作業が大きな負担になると考えられる。事業者側の負担を軽減するためのシステム構築も必要。さらに、報告されたデータを匿名化した上で、研究者等も含めたステークホルダーで情報共有できるシステムになれば、様々な知恵を持ち寄って柔軟な事故対応方策をとることができる。

○２０１７年に大規模なインターネット障害が発生したが、インターネットに接続しづらい障害について、どうやって把握するか、どうやって再発防止するのか、ＢＧＰにおける大規模障害における障害の範囲をどれだけ極小化できるか、本障害で実際起きた二次・三次的なトラブルもどうやったら防げるのか等が課題となるが、事業者間連携や情報の迅速な交換が大事。Peering in Japanというグループがあるが、そこでのSlackが一番情報の流通が早く、それらのベストプラクティスの共有等も有効。

○サイバー攻撃には様々な形態があり、たとえば近年、身代金型のサイバー攻撃がある。こういった攻撃があるという情報共有として、業種をまたいだＩＳＡＣ間での連携で相談等がくる場合がある。

○ＲｅｇＴｅｃｈやＳｕｐＴｅｃｈなど、ＡＩ等の活用により、ＳＮＳの情報含め様々なオルタナティブな情報を収集し、規制対応の合理化・高度化が可能になると思われる。

○インターネット接続がしづらい障害といった把握そのものが難しい障害も、重要なインフラであるため、見ていく必要がある。ただ、こういう障害が起こったときは、ルールに従って事故報告すること自体が目的ではなく、障害を積み重ね、なるべく事故や障害が起きないようにすることが目的。そのため、一事業者と行政がただやり取りするという報告

の在り方だけではなく、事業者間でウィン・ウィン関係が築けるのであれば、連携して障害を把握する仕組み、そこに行政が関わりステークホルダー間で協力できるようなソフトな検証の在り方も今後は考えていく必要がある。

○ＳＮＳのコメント等、利用者の意見をうまく利用することで、社会全体でコストを分担しながら事故報告・検証制度を動かしていく観点が大事。

○ＳＮＳにおける利用者の投稿情報により障害の発生状況を把握するなど、利用者目線の事故対応の在り方は重要。

○ＯＯＤＡループについて、攻撃なり事故というのが継続してくる場合というのは、観測システム等で観測することにより、報告が上がってこなくても自動的に何かが分かるという形で、ＩＣＴ－ＩＳＡＣでもシステムに取り組んでいる

○ＳＮＳを用いた情報収集は、研究でも一定の有効性が示されているが、事業者が独力でシステム構築し運用するのは難しい。特定事業者に限らず、広く情報収集を行い、ステークホルダーで適切に情報共有できる共通のシステムやサービスについて、産学官連携等様々な形が考えられる。

○インシデントという言葉の定義について、読み手等によって捉え方が異なるため、用語の説明等を明確にするのがよい。ＩＳＯではセキュリティ上好ましくない事象といった広い意味だが、現場レベル、ＣＳＩＲＴ等では通常、すでにインシデント自体が重要な事故と認識されている。

○サイバー攻撃に関するインシデントの報告は重要。ただ、インシデントが起こった場合、その原因がサイバー攻撃かどうか、またサイバー攻撃だったとして情報漏洩があったのかどうか等、実務上判断が難しく、調査に時間がかかるケースが多い。例えば、ＧＤＰＲでは７２時間以内の報告を求めているが遵守はかなり厳しい。国内では、昨年の個人情報保護法改正で個人データ漏えいの報告等が義務化されたが、通常確報は３０日以内のところ、サイバー攻撃等が原因の場合は特例でその期限が６０日以内となっている。また、欧州のＮＩＳ指令では、重要インフラの運営者に対して事故報告義務を課しているが、昨年１２月にその改正案も公表されているので、これらを参考にしてほしい。

○故意に行われる事故と自然発生する事故は、現象として似ていても、背景や原因は全く異なる。例えば、重要インフラ施設へのサイバー攻撃は、小規模であっても、攻撃として成功していなくても、予兆としては大きな意味を持つ。集めた情報を分析し、その意味を正確に理解することが大切である。その意味で、攻撃か事故かの判定は非常に重要。

○２０２１年４月より電気通信事業法の域外適用が始まる。海外事業者としては、事故が起こってもホームページ等で国民に知らせれば監督官庁である総務省への報告義務はないのではないかという考え方もあるようだが、国民目線に立つと、国民が依存している外国企業等のサービスに対してもしっかり注視していく必要がある。

○海外のクラウド事業者が原因で引き起こされた通信障害が問題化している。海外事業者と通信事業者との認識は大きく異なり、どのようにその認識を合わせ、お客さまに安全・安心なサービスを提供し続けられるか、非常に難しい問題である。

○最近はオープンソースソフトウェア（ＯＳＳ）を利用したサービスが多くあるが、オープンソースにトラブルやバグがあった場合どのように対処すべきかという問題が足元では起こっている。

○通信の重要性は日増しに高まっている。毎年のように災害が発生しているが、ケーブル事業者は地域密着の総合情報通信メディアであり、災害に対してもより高い信頼性が求められている。この点、日本ケーブルテレビ連盟においては、停電やセキュリティ等の各種対策ごとに目標値を設定し、その達成に向けて各事業者が主体的に取り組んでいけるような安全・信頼性向上に向けたガイドラインの策定を進めている。

○５Ｇと組み合わせたＩｏＴ機器の利用において、利用者と事業者の境界線が曖昧になり、ステークホルダーが増える中、安心・安全な利用等の確保が難しくなりつつある。総務省のＮＯＴＩＣＥによるＩｏＴ機器の脆弱性の注意喚起や、５Ｇに関して、様々なステークホルダーに対するガイドラインの提供等を行っている。

○通信分野におけるサービスの多様化が進み、高い可用性を求められるサービスと利用料が低い分可用性が低いサービス等のサービスの特性に合わせることや、サービス提供が複数事業者の連携によるもの等、サービスの構造の変化や性質の多様化を踏まえた適切なガバナンスモデルが重要である。

○クラウドサービス等、電気通信事業法が基本的に適用されない電気通信事業者の事故報告制度についても考えなければならない。法律をいきなり変えるのは難しいが、ガイドラインに盛り込む等の選択肢はある。

○サービスの品質を理解できるような、啓発やリテラシー教育も重要。利用者側も、不具合があれば報告する、使い方を改善するといった利用者教育等も重要である。

○事故報告の際や事故の責任分界点を定める際に、事業者や利用者含め様々なステークホルダーから様々な不満や意見申し出の要求があると考えられる。特に海外事業者は行政

指導的な対応等に従わないケースもある。事業者への不服申立てや意見に対し、適正手続きを考慮した公平中立的な紛争処理制度も今後検討が必要ではないか。

（２－３）今後の進め方について

・事務局（恩賀室長）より、資料１－３－１、１－３－２及び１－３－３に基づき、今後の検討スケジュール等について説明があった。

（２－４）その他

・事務局（西室課長補佐）より、今後の予定について説明があった。

（３）閉会

・内田主任より、本日の会合を終了する旨説明があった。

以上