参考資料4－3－1

2020 年代半ば頃に向けた電気通信事故の報告・検証制度等の在り方に関する意見募集の結果

令 和 ３ 年 ４ 月　１９ 日
事故報告・検証制度等 TF
事　　務　　局

意見主	提出された意見
個人１	私は ・第一級陸上無線技術士 免許証 ・第一級海上無線通信士 免許証 ・伝送交換主任技術者 資格者証 ・工事担任者（AI・DD 総合種） 資格者証 を所有しております。 まず、電波航法について述べます。船舶・航空機の無線航法システムに対する攻撃や航法装置の故障などの脅威ついて考慮することは重要と考えます。現在、船舶の無線航法はロランＣなどの地上無線航法装置はそのほとんどが廃止され、主に衛星無線航法装置（GNSS）によっていると認識しております。GNSS は海上においても広範囲に利用可能なシステムですが、衛星が利用不能となった場合や受信装置の故障や破損の場合などを勘案すると、予備としてなるべく常時、地上無線航法装置が利用可能であることが望ましいと考えます。ロランＣまたはそれに代わるシステムの運用、NDB の運用などにより船舶ができるだけ衛星・地上両系の無線航法装置を利用可能で確実に自船の位置を知りうるような仕組みが GMDSS をより完全なものとするためにも望ましいものと認識しております。また、ロランＣや NDB などの地上無線航法装置は航空機においても利用可能であり、広く運用中の VOR/DME の欠点を補い、VOR/DME が利用不能となった場合にも予備としても機能するものです。船舶・航空機がその位置を常に正確に把握することは特に万一の遭難や事故・事件などの際には重要となります。遭難や事故・事件の場合の検証の際にも位置情報は肝要な情報であることから地上無線航法と衛星無線航法の両システムが運用され適切に利用されることが重要です。無線航法装置としてはロランＣ、NDB、VOR/DME、GNSS など多彩なタイプ・周波数帯のものが複数利用可能であることが船舶・航空機の安全とインシデント管理のために重要であると考えます。航空機においても GNSS への移行が進むものと認識しておりますが、バックアップとしての VOR/DME の意義は大きいものと考え、VOR/DME は将来的にも運用を継続すべきものと考えます。これらのシステムは陸上無線技術士、第一級総合無線通信士、第一級海上無線通信士、航空無線通信士など各無線従事者により適正に管理されるべきものです。 災害時・有事における無線通信の有効性・可用性の高さについて触れます。通信速度、通信容量、符号誤り率などの点

	において一般に有線は無線より有利です。しかし、災害時・有事において有線は通信設備が毀損されやすく、設備が損傷を受けた場合に迅速な復旧は困難である場合も多いです。無線であれば伝送路は空間であり、無線設備と電源さえ用意できれば直ちに回線を設定し通信を行うことができます。このことについては電波法の非常通信（電波法 52 条）にもある通りです。非常時に限定的にでも直ちに通信を確保するため、有線の回線を設定済みであっても電気通信事業者が必要な統制をとるための無線回線を直ちに設定できるよう予備しておくことは重要と考えます。完全に通信が途絶してしまうと適切な事故報告・検証に至るのも著しく困難となります。 電気通信事業者について述べます。電気通信事業者のサービスレベル維持及びインシデント対策の監督者としても、電気通信主任技術者の役割は重く、重要な立場にあると考えます。電気通信主任技術者は伝送交換設備若しくは線路設備について一定の専門的知識を有しており、電気通信設備の工事、維持及び運用の監督責任者という立場であるため、電気通信事故の報告の際にも重要な役割を果たす者であると認識しております。通信のサービスレベルを無理なく安全に維持するためにも、十分な数の電気通信主任技術者が事業者において活躍することが必要です。電気通信主任技術者の選任は兼任や外部委託も認められておりますが、極力、兼任や外部委託は避けて適正な立場・数の電気通信主任技術者が確保されることが重要と考えます。電気通信事故の報告・検証を適切な権限とスコープの元で行うためにも必要と認識しております。 電気通信主任技術者は、伝送交換主任技術者、線路主任技術者ともにセキュリティ管理及びセキュリティ関連法規が国家試験においても必ず問われており、セキュリティに対する意識及び知識を有していると考えられます。また、端末設備側の監督資格である工事担任者においても情報セキュリティに関する技術が必須であり、通信に従事する者がなるべく多くこれらの資格を取得することが望ましいと考えます。現在ある質の高い国家資格の制度を活用することは有用で効率的なものと考えます。これら国家資格を取得することは専門知識と自らの職務に対する責任感を確固たるものにする一助となると考えます。 伝送交換主任技術者は伝送交換設備の工事、維持及び運用の監督者ですが、無線従事者のような具体的な操作範囲がありません。無線設備は伝送交換設備の一部ですので、無線従事者免許などと併せて取得するのがより効果的と考えます。通信システムのより具体を知ることは適切な電気通信事故の報告・検証に有用と思われます。また、TEMPEST 対策（電

	磁波セキュリティ）も重要であり、電磁波・無線技術をよく知ることはセキュリティ上も必要です。電波・無線技術で最高水準の第一級陸上無線技術士国家試験などにおいてはTEMPESTなどに関する問題の出題も有意義ではないかと考えます。 2020年代半ば頃にかけては特にHF帯の電波伝搬に大きな変化が予測されております。電波伝搬の変化による不意な通信事故の発生の防止及び通信事故が電波伝搬の変化による可能性であることを失念するために起こる事故原因検証の遅滞を防ぐべく、必要な周知をする必要があります。VLF～HF（スポラディックE層を考慮する場合にはVHF）帯について異常伝搬など含め影響を考慮する必要があろうと思われます。 電気通信は非常に領域が広いため、通信事故の際、報告・検証が難しいこともあります。電気通信事業者は電気通信主任技術者に加え、無線従事者やコンピュータネットワーク、情報セキュリティの専門家など広い専門性を持った人材を擁することにより、全体で事故を切り分け、責任の所在は明確にすることが必要です。電気通信においてもそういった意味でのダイバーシティの推進が重要になってきております。
株式会社ジュピターテレコム	【１「自然災害」や「サイバー攻撃」等のリスクの深刻化・自然災害を発生要因とする事故の報告・検証】 第１回　事故報告・検証制度等タスクフォースの資料1-2-2　電気通信事故の報告・検証制度等に関する現状と課題（議論のたたき台）P66にある通り、大規模な自然災害による障害発生時には、管轄の総合通信局へ被害状況等の報告を行うこととなっていますが、通信と放送に関して報告手法が異なっています。具体的には電気通信事業は総務省の「非常時情報伝達ネットワークシステム」のWebサイトを通じて行っており、当社の様な有線放送事業者は、放送に関するものは主に電子メールにて所管の総合通信局に報告をしております。報告手法のみならず様式も同じではなく、当社の様に同じ有線伝送路で通信と放送を一体としてサービス提供する事業者にとって、大規模な自然災害時の例えば電柱倒壊や伝送路の断線などによる影響は双方に及びます。特に大規模災害時には、事業者もその復旧や対策に注力しており、事業者の作業を軽減し復旧に専念する意味でも、通信と放送を一元的に報告できるようなシステムや様式としていただく事で、迅速かつ正確な被害状況の報告、把握が行えるものと考えます。 また、大規模な自然災害が発生し電柱倒壊や大規模な停電が発生した場合、当社の局舎側の設備に問題がなくとも途中の伝送路やお客様の居住エリアにおいては影響が出る場合が想定されます。自然災害発生時の被害状況の把握や、発生

	後の早期の復旧においては、通信事業者の提供するサービスの利用場所での復電や、サービス提供に使用している幹線を架空する電柱の復旧見込みの情報も必要となります。電柱の倒壊状況や、復電の見込などの情報を電力事業者などから共有いただける仕組みやシステムが構築されれば、復旧対応要員の配置が効率的に行え、早期復旧につながることが期待できると考えます。現状ではこうした情報を得ることは容易ではないため、今後の事業者間の情報共有の仕組みに関する検討を要望致します。 【３「インターネット関連サービス」や「ブロードバンドサービス」 等の電気通信サービスの「ユニバーサル化」・データ伝送（ベストエフォートサービス）の品質低下に関する報告基準】 第１回　事故報告・検証制度等タスクフォースの資料 1-2-2　電気通信事故の報告・検証制度等に関する現状と課題（議論のたたき台）P63 には、「固定ブロードバンドサービスの品質測定手法の確立に関するサブＷＧ」が 2021 年度末目途の確立を目指している固定 BB の品質測定手法の確立を前提に今夏頃以降に検討する予定との趣旨の記載がございます。現在、品質測定手法について検討がなされていますが、そもそもインターネットがベストエフォートであるサービスであることから、測定方法の適切性や公平性などについて様々な意見が出ていると承知しており、検討要の段階と認識しております。例えば、測定個所に関しては全ての利用者の個別の状況を把握する事は現実的ではなく、サンプル的に取得される情報をもとに全体のサービスを判断することになりますが、特に固定通信の場合には携帯電話と異なり同一箇所で異なる事業者のデータを取ることが困難であること、お客様の宅内・棟内での状況が異なるなどの点が指摘されております。したがって、まずは事故報告基準に適用することができるのか、適用することが適切なのかといった視点から、慎重な検討がなされることを要望致します。 【４情報通信ネットワークの「産業・社会基盤化」・行政・医療等重要インフラ向けサービスに関する報告基準・テレワーク・遠隔学習等向けサービスに関する報告基準】 産業・社会基盤化されているシステムやアプリケーションに対する事故報告・検証制度を検討することは、電気通信分野の安全・信頼性対策のための事故報告・検証制度の趣旨から鑑みてその必要性について疑いはありません。他方、行政・医療向けとして専用線を用いているような場合は別として、一般的に通常提供されるインターネットサービス（アクセス回線の提供並びに ISP としてのサービス）においては、通信事業者はお客様がどのような用途で使われているかを知るすべはなく、また通信の秘密との関係で、お客様の利用される具体的なサービスを同意なく接続先を把握することもできません。 従って、いわゆる B to C 向けサービスにおいては、ここで掲げられているような目的（テレワーク、遠隔学習等）に

	関しての報告義務を課されたとしても、実態上報告は困難です。対象範囲をB to BやB to Gに限定し、お客様側の同意を前提にする等、制度的な裏付けを整備していただくことが障害状況の把握においては必要と考えます。 【５情報通信ネットワークの構築・管理運用の「高度化・ マルチステークホルダー化」・SNSによる障害の早期認知や共有等利用者によるガバナンス】 SNSを活用した、複数ネットワークに跨がって発生するインターネット障害の把握手法については、第１回　事故報告・検証制度等タスクフォースの資料1-2-2　電気通信事故の報告・検証制度等に関する現状と課題（議論のたたき台）P43にある「令和元年度インターネット障害の把握に関する調査研究」の結果をベースに検討がなされると考えております。事業者の規模や地域性によって、発信されている障害情報に関する件数が異なる事、ベストエフォートのサービスにおいては発信者の受け止め方や主観も入り得ることから、調査研究結果を踏まえ更なる精度の向上も必要ではないかと考えます。 また、情報を集約し管理運用を行う機関についても言及がなされていますが、各通信事業者の障害に関する情報を取り扱うことから、その情報の適正性の判断はもとより、得られた情報の扱い（特に特定の事業者に対して不利となるような提供の仕方など）については、公平中立であることが求められると考えます。国以外の組織がこれを行うにあたっては、守秘義務等についても併せて検討することが必要と考えます。
個人２	自然災害やサイバー攻撃だけにとどまらず、物理的に電気設備やアンテナ等への破壊工作等をどのように防ぐか、万が一破壊された場合の補完体制は二重三重に準備されているかなども重要です。 また、そのような攻撃や「事故（に見せかけた攻撃）」が発生した場合、どこに穴が出るか（警備が手薄になるのはどこか等）も観察されます。そのような場合にも、弱点を把握されないよう、万全の準備をお願いします。
個人３	(6)その他の検討課題（社会全体として安心・安全を追求するべきか） ■ 要旨 現代は VUCA （Volatility：変動性, Uncertainty：不確実性, Complexity：複雑性, Ambiguity：曖昧性 の頭文字からなる造語）という言葉で表されるような不安定な時代です。この時代の大きな流れに逆行して社会全体として安心・安全を追求するのは無理があるので、VUCA を前提として社会全体としてリスクマネジメントできるような制度設計に

	するべきです。 ■ 本文 「電気通信事故の報告・検証制度等 に関する現状と課題（議論のたたき台)」p8 には、事故報告・検証制度等 TF の目的として、安心・安全で信頼できる情報通信ネットワークの確保が掲げられています。また、同資料 p4　検討課題（案）C) に「電気通信事故の 未然防止や被害の拡大防止等に社会全体で取組むことが今後益々必要になってきているのではないか」という記載があり、社会全体として安心･安全を追求するのが基本方針案と理解しています。現代は VUCA（Volatility：変動性, Uncertainty：不確実性, Complexity：複雑性, Ambiguity：曖昧性 の頭文字からなる造語）という言葉で表されるような不安定な時代です。情報や物も国境を超えて瞬時に流通するようになりました。このような時代の大きな流れに逆行して、日本は社会全体として安心・安全を追求するべきなのでしょうか。また、安心・安全を追求し続けることは可能なのでしょうか。むしろ社会全体として VUCA を認識し、VUCA を前提として、VUCA に適応して適切にリスクマネジメントするような方向性にするべきと考えています。 日本企業の改善の文化は、変化の緩やかな時代においては日本の製品やサービスの信頼性向上に大きく寄与してきました。しかし時代は変わり、VUCA の時代においては競争の土俵そのものが変わる不連続な変化が頻繁に起こります。スマートフォンの登場のような破壊的イノベーションが起これば、漸進的な改善活動は水の泡となります。技術のトレンドの移り変わりも激しく、様々なプラットフォームサービスを組み合わせて短期間でサービス開発できるようになりました。このような時代にあっては、漸進的な改善活動は必ずしも正解とは言えず、これまでの事故報告・原因究明・再発防止を前提とした事故報告・検証制度は抜本的に見直した方がよいと考えています。 現在の事故報告・検証制度に代わるものとしては国際的な足並みも揃える必要があると思いますが、変化に追従してルールを作るアプローチではなく、変化を前提としたものにするべきです。例えば第三者による通信網や SNS 等の監視による早期の障害認知、その影響の大きさに応じて行政が事業者や消費者にアクションを取るというような OODA ループ的な対応が考えられます。規律については、都度生まれる技術や事業毎に細かいルールを作ってもすぐに時代遅れになるので、技術や事業形態が変化しても変わらない原理原則を示し、具体的に何をどこまでやるかという判断は各事業者に委ねるプリンシプル・ベースの規制を取り入れていくのがよいと考えています。障害発生時の事業者間の情報連携

	や事故の再発防止のための情報共有は、民間が主体のスキームを作りつつ行政がそれを支援する形が望ましいと考えています。もし、こうした制度にした場合、行政の事業者に関する関与が恣意的になるという懸念があり、どう公平性を担保していくかが課題と考えています。 消費者としては通信事業者に障害が起こることをある程度想定するべきです。自宅の有線回線に障害が起きてもスマートフォンを使えば必要最小限の通信はできます。携帯電話は必要に応じてデュアル SIM 端末等でマルチキャリア化すれば、通信事業者の障害の影響を受けなくても済みますし、Wi-Fi に切り替えることも可能かもしれません。クラウドに関しては事業者が設備のあるリージョンを公開しており、別リージョン間で冗長化することもできます。必要であればマルチクラウドで冗長化することもできます。メールや LINE ようなアプリケーションサービスについても無料で使えるものも含め代替手段は多数あり、例えば LINE が使えないなら電話や Facebook Messenger を使うなど、多少の不便は感じても困ることはほぼありません。このように利用者側が適切にリスクマネジメントするのが VUCA に適応した消費者だと考えます。現在は一家に一台の固定電話しかなかった時代と違い、消費者には通信事業者や通信サービスの多様な選択肢があります。消費者視点でみても個々の通信事業者の信頼性は以前ほど重要ではないと思われます。 　私たちは地震や台風などの災害そのものの発生を防ごうとは考えません。地震や台風などの災害が発生するのを避けられないものとして、備蓄などの対策をとります。同じように通信についても停止は避けられないものとして、致命的な問題にならないように対策を取るべきと考えています。 このようなアプローチをとれば消費者の負担が増えるのは事実ですが、VUCA の時代では通信事業者の障害を無くすことは不可能です。障害を想定していなければ、障害発生時に困るのは消費者自身です。安心・安全を追求して規律を強めても重大事故をゼロにすることはできません。そればかりかイノベーションを阻害し、日本の産業そのものを衰退させ、結局は国民生活の質の低下を招きます。変化に適応していくのは簡単なことではないですが、社会全体として VUCA に適応していくことが国の発展、国民生活の向上につながると考えています。
個人４	(1)「自然災害」や「サイバー攻撃」等のリスクの深刻化について 「自然災害」や「サイバー攻撃」等により事故が発生した場合は、原因が明確であるから、事故の報告のみで明らかな問題が無い限り検証は不要ではないだろうかと思う。復旧に官民の連携協力体制が整えられるのはよいと思う。

	(3)「インターネット関連サービス」や「ブロードバンドサービス」等の電気通信サービスの「ユニバーサル化」について 「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５版)」 https://www.soumu.go.jp/main_content/000666214.pdf P9 (5) (2)のアについて、総和が 2Gbps を超える状態であれば、影響利用者数が 3 万人以上というのは現状にそぐわないと思う。 また、ベストエフォートサービスには品質低下の状態を許してもいいと思う。利用者が品質と価格からサービスが選べるとよい。高品質なものしか許されなければ高いサービスしか存在しなくなってしまう。選択肢がある方がよいと思う。 (4)情報通信ネットワークの「産業・社会基盤化」について インターネットは行政・医療・テレワーク・遠隔学習すべてに対するインフラになるので個別に報告基準を決めるのは不要ではないか。社会基盤として大きな基準があるべきだと思う。 (5)情報通信ネットワークの構築・管理運用の「高度化・マルチステークホルダー化」について ステークホルダーが複数あるにせよ、利用者にはサービスが使えない状態にあった・使えない状態にあることをわかるようにしてほしい。 利用しているサービスの情報を知るために他の SNS のアカウントを取得しなければ情報を閲覧できないのはよくないと思う。
（　公社）日本消費生活アドバイザー・	新型コロナウイルス感染症拡大防止で提唱された新しい生活様式により、リモートワーク、インターネットを介した取引や交流を行う消費者が増えています。インターネットが重要なインフラになった現代、たとえ 30 分でも繋がらなくなると不安になります。電気通信事故の報告・検証を行い、PDCA サイクルによる防止策を講じる施策は、消費者にとって頼もしいものです。消費者の目線で報告・検証制度について意見を述べさせていただきました。 １　検討事項１について

コンサルタント・相談員協会 ICT 委員会	通信事故は、自然災害とサイバー攻撃等によるものがあります。重大事故として同列に報告検証せずに、別々のジャンルに分けて報告することを提案します。 （意見） 自然災害による通信事故は、停電、災害の影響による施設の破損、荒天等の影響によるため、事故の地理的範囲、原因は誰でも容易に理解でき、発生から時間の経過で被害は逓減する類のものです。 それに対し、サイバー攻撃などが原因の通信事故は、事故の発現が原因の発生時期と異なることが多い傾向です。また、サイバー攻撃は海外からの攻撃が主で、「事故の兆候→重大事故発生の恐れのある事態→重大事故」となるため、通信事故がはっきりと目に見えるようになるまでタイムラグがあり、原因究明にも時間がかかります。 そのような点からもサイバー攻撃による通信事故と自然災害による通信事故とは別の検証方法にすべきと考えます。 ２　検討事項 2 無料サービス等を提供する海外事業者等の回線非設置事業者の報告義務を実効性のあるものにするとともに、報告義務のインターバルを四半期より短く、少なくとも 2 か月ごとにすることを提案します。 また、報告義務の対象外となる業務委託企業（特に海外の企業）に起因する通信事故であっても、事故が発生して一般利用者に影響を及ぼした事故の場合は、報告義務を課すようにすることを提案します。 (意見) 通信事故の報告対象事業者の範囲が、回線設置業者、ユニバーサルサービスを提供する事業者、有料で利用者 100 万以上のサービスを提供する回線非設置事業者のみならず、無料サービス等を提供する海外事業者等の回線非設置事業者を含めた全ての通信事業者（約 2 万 1 千）が対象になっている点はとても良いと考えます。しかし、現実に、四半期事故報告では海外の事業者にどこまで実効性を担保できているのか、疑問です。 また、これだけ通信技術の進歩の早い分野で、報告が四半期ごと、それから検証、施策に反映となると非常に遅いと感じます。重大事故に準じ 30 日以内の報告書提出が理想と思いますが、少なくとも 2 か月以内の報告にすべきです。 海外企業との連携や業務委託で通信事故が起こるリスクも高まっています。クラウドサービスなどの業務委託先がサイバー攻撃を受ける場合もあり、それが最終的には消費者の通信障害を発生させるリスクとなっています。 その場合は報告義務の対象外になる場合もままあるので、委託元で事故原因が起こっても報告義務となるよう報告要件の再検討を希望します。そのためにも、監督官庁としては国境をまたいだ連携をし、法執行を含めた解決方法の基本

	方針を構築してください。 ３　検討事項３ 　データ伝送はベストエフォートの考え方とは理解していますが、回線卸事業者等の甘い見通しが原因の接続できない等の通信事故を防ぐため、監督官庁として、事業者指導につながるきめ細やかな検証を要望します。 （意見） 　クラウドSIMサービスで繋がらないという重大事故が起きました。消費者相談の現場でも、広告に書かれた表示と異なり思うように接続できないから解約したい等の、それに関連した相談がありました。コロナ禍でビデオ会議システム、ビデオ電話、動画配信サービスなど高速大容量のデータ通信利用者が増加し、今後ますますトラフィックがひっ迫すると予想されます。この例のような通信事故は未然に防げる可能性があるものですので、企業のガバナンス向上に資するよう、特に力を入れて、通信事故の検証を願います。 ４　検討事項４ 　行政サービス、医療等重要インフラ向けサービスに関する報告基準作成に賛成します。注目を集めている自動車の自動運転システムについても重要インフラ向けサービスとして報告基準作成に加えることを希望します。 （意見） 　医療分野では電子カルテ、保険証のマイナンバーカード利用など電子化を促進させていますが、医療従事者が患者の情報にアクセスできないと命に係る重大事故になります。自動運転システムも行政の住民サービスも同様です。これらの分野は特に、重要インフラ向けサービスとして、重大事故報告、四半期報告事故の義務要件とは別の基準を作成し、少数事故（例えば１病院だけの事故）であっても速やかに報告するようにすべきと考えます。 ５　検討事項５ 　業界団体を中心に緻密な情報通信ネットワークの構築を促す報告・検討を要望します。 （意見） 　マルチステークホルダー化で、通信事故の原因究明が困難になっていると感じます。 　OS のアップデート等により一部のアプリや端末で、重大事故までには至らない通信切断事故が頻繁に起きていると

	感じています。身の回りを見ると、「通信が切断しており、スマホ決済が現在利用できません」との張り紙の出ている小売店、飲食店を目にするようになっています。スマホなど使用する端末の全てのアプリにおいて接続が切断される訳ではないので、消費者も事故の原因がわからず困る状況に陥ります。 　通信の秘密の問題があることは理解しますが、SNS 等で飛び交う事故情報等のキーワードを AI で拾い、アプリ提供元や通信会社への問合せ等を迅速にして総合的に事故を分析できるよう、情報通信ネットワークの高度なシステムの構築を希望します。 　キャッシュレス決済を政府が促進していますが、決済トラブルなどはたとえ事故の発生範囲が狭くても、消費者にとって重大事故です。 ６　その他 　通信事故が起きた場合、利用者に迅速に情報が伝わるよう、情報配信の方法を、通信会社などと構築するよう希望します。自然災害も通信状況の情報が必要ですが、貴課が検討事項に書かれているどの事象であっても、どこで何が起きているのか迅速な情報は、通信事故に遭った利用者が次善策等をとるために重要な情報です。 以上
楽天モバイル株式会社	【⑥その他の検討課題（上記①～⑤以外）】 　現在の事故報告制度は、事業者の保有する設備の故障、および役務の提供に支障を及ぼす恐れのある情報漏洩を広範に対象としております。これにより、少なくとも事故発生による利用者への影響が大きい通信事業者においてはその自主的な取組により、様々な環境変化に対応できる自律的・継続的な PDCA サイクルが既に確保されていると考えております。 　当社も登録電気通信事業者として、国民生活、社会経済活動や危機管理等のために不可欠なインフラを提供することで Society5.0 の実現を下支えすべく、今後も安心・安全で信頼できる情報通信ネットワークの確保に努めてまいります。
一般社	【⑤情報通信ネットワークの構築・管理運用の「高度化・マルチステークホルダー化」】

団法人日本インターネットプロバイダー協会	昨今のISPは接続などにより自社でネットワークを構築するのではなく、NTT東西の光卸やNGNにおけるVNEの利用、インターネット接続のためのネットワークの構築及び運用を他のISPに委ねるローミングサービスの活用により、インターネット接続にかかる交換設備を所有せず、他事業者からサービスとして提供を受ける割合が増えつつあります。そのような現状を踏まえると、利用者に対しサービスを提供する電気通信事業者と上記のサービスを電気通信事業者に対し提供する事業者との間での、事故や障害についての情報連携の在り方が重要であると考えます。 また、昨今はインターネット接続サービスの提供にあたって認証サービスと同様にほぼ必須であるDNSのサービスを提供するサーバーやメールサーバーなど、電気通信サービスの提供に関わる設備も自社ではなく、他事業者のクラウドサービス上に設置される傾向にあり、電気通信事業者とクラウド事業者との 情報連携も同様に重要であると考えます。 【⑥その他の検討課題】 新型コロナの拡大に伴う在宅時間増等によりインターネットトラフィックは急増し、今後もデジタル活用が進展し、トラフィックはさらに増加する事が想定される中、インターネットの混雑緩和及び地域格差のない通信品質確保が一層求められています。このような状況の中で現場レベルの責任者、および技術者の負荷は増えており、それらの者に対して新たな報告の新設などが過度の負担にならないことも求められると考えます。 また、現在の重大な事故の定義では、無料サービスの場合、「100万人以上かつ12時間以上」「10万人以上かつ24時間以上」という基準しか存在しません。 しかしながら、無料サービスでも実際には社会的影響や他事業者サービスへの影響が大きいサービスが存在している状況です。(例えば、yahoo！メールやGmail、GoogleのPublic DNSなど）こういった観点から、無料サービスの大規模事業者を対象にした新たな基準追加の必要性の検討も重要であると考えます。
アジアインターネット日本	１．総論・要旨 アジアインターネット日本連盟(AICJ)は、国際的にインターネットビジネスを展開する企業の連盟として2013年９月に設立され、インターネットにおける自由で公正な情報の流通を促進するために活動しています。 今般、総務省において、情報通信ネットワークを取り巻く環境変化に鑑み、そのような環境変化にふさわしい電気通信

連盟	事故の報告・検証制度等の在り方を検討されることに賛同し、また、電気通信役務提供に関わる民間事業者から意見を提供する機会を設けていただくことに感謝いたします。 2020 年代半ば頃に向けた電気通信事故の報告・検証制度等の在り方に関する意見募集の対象文書（以下、本文書」といいます）にお示しいただいているとおり、Society5.0 の進展や with/after コロナの状況にあって、インターネット関連サービスは多様化し、国内外の電気通信役務関連事業者は増大し、自然災害やサイバー攻撃によるリスクが深刻化・複雑化しており、電気通信役務提供を取り巻く環境は、大きく変化しています。このような状況を正面から捉えて、民間事業者がイノベーションを起こしながら合理的かつ迅速な事業展開をできるようにし、もって日本企業がグローバルでの競争力を確保しつつ、課題解決につながる事故報告・検証制度を検討していただくことを支持いたします。 ２．電気通信事故の報告制度について（意見対象の検討事項：③②関連） 本文書６頁には、現行の事故報告制度におけるサービス毎の閾値が記載されています。現行の報告制度は 2013 年に開催した「多様化・複雑化する電気通信事故の防止の在り方に関する検討会」における議論を経て決定されたものと理解しております。しかしながら、総論で記載した電気通信役務提供を取り巻く大きな環境変化と目指すべき方向性に鑑みれば、各サービスの閾値の設定については、全ての電気通信事業者及び役務提供に関わる関係事業者にとって、一義的に明確であり、分かりやすく、合理的なものにアップデートいただくことを支持いたします。 そのための検討に際しては、国際的な状況も考慮して、日本のみがユニーク又は大幅に低い閾値を採用している点については、必要性や合理性、そして実効性の観点も踏まえつつご検討いただきたいと考えます。例えば、EU や米国（ただし、米国の場合の報告対象は、PSTN 網を使う電話や VoIP 等の電気通信サービスのみに限定）を含む諸外国では、「ユーザー時間」（「影響利用者数」と「継続時間数」を掛け合わせて計算する）の考え方を採用しております。電気通信事業者のみならず広域かつ多様な関係事業者が関わってくることから、一義的明確性の観点から、日本においても以下のとおりのユーザー時間の基準の採用を勘案いただくことが望ましいと考えます。 現行の考え方：「影響利用者数●人以上」かつ「継続時間数●時間以上」 変更案：「ユーザー時間」（「影響利用者数」×「継続時間数」）≧ ● 現状、「ユーザー時間」に換算してサービス毎の閾値を計算すると、現行のルールでは、一つのカテゴリにおいて「ユー

ザー時間」が大きく異なる基準が２つずつ存在していることになります。例えば、インターネット関連サービス（無料）については、「1200 万ユーザー時間又は 240 万ユーザー時間」となって２つのユーザー時間には大きな差があり、インターネット関連サービス（有料）については、「6 万ユーザー時間又は 100 万ユーザー時間」となって、同様に大きな差があるユーザー時間が存在します（下表のとおり）。

電気通信役務の区分	時間	利用者の数	ユーザー時間換算
一 緊急通報を取り扱う音声伝送役務	1 時間	3 万	30,000
二 緊急通報を取り扱わない音声伝送役務	2 時間	3 万	60,000
三 セルラーLPWA を使用する携帯電話及び電気通信事業報告規則第一条第二項第十八号に規定するアンライセンス LPWA サービス	1 時間	10 万	100,000
四 利用者から電気通信役務の提供の対価としての料金の支払いを受けないインターネット関連サービス（一の項から三の項までに掲げる電気通信役務を除く。）	24 時間	10 万	2400,000
	12 時間	100 万	12,000,000
五 一の項から四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	60,000
	1 時間	100 万	1,000,000

このため、現状では一義的に明確で分かりやすいとは言いづらいこともあり、何故大きく異なる閾値が同一カテゴリで、数値に大きな差がある状態で複数存在するのか、ということについて理解が得られないなど、事業者において調整に困難を伴う実態も生じております。

情報通信ネットワークが広域かつ複雑に関連していることから、通信事故等に際しては、国内外の企業を含む数多くの事業者の連携が必須となっている中、基準を見直し、全ての関連する事業者にとって合理的に理解しやすい基準の整備

	が望まれます。 加えて、同時に、いたずらに短い電気通信役務の停止や少ない影響人数等で多数の報告が必要となることも政策目的に合致せず、また事業者の実務上の負担の観点からも現実的ではないことにも留意が必要です。このことから、影響利用者数や継続時間数を設定する現行の考え方も合理的に維持すべき部分は維持すべきであり、その観点からは、今回の事故報告・検証制度の検討に際しては、「ユーザー時間」の考え方を勘案し、同じカテゴリ内では（「ユーザー時間」を勘案したことによりいたずらに低くならない）閾値を一つに定めることを通じて合理化していただくことで、電気通信事業法のもと活躍する企業における迅速な課題解決に資するばかりでなく、合理的かつ迅速な報告という政策目的にも資することにつながるものと考え、見直しによる整備を要望いたします。 ３．イノベーションの進展等に伴う事故報告等の在り方について（意見対象の検討事項：②関連） 本文書２頁では「電気通信事故の報告及び原因究明等の検証等を通じたPDCAによる リスクマネジメント」について触れられており、今回の事故報告・検証制度の検討では、①電気通信の途絶に関する情報収集　②電気通信に関する事故の責任の明確化及び同様の事故発生の防止　の両方が、事故報告の目的として求められているものと理解しています。しかしながら、現在の国際的な通信インフラを用いて世界中で電気通信役務の提供が行われる状況では、特にインターネットサービスでは、自己が管理する施設で事故が発生する場合だけでなく、自己が管理する施設に接続する他者が管理する施設で事故が発生する場合にも、電気通信が途絶する事象が生じることになります。そのため、本文書２頁で事故報告が「氷山の一角に過ぎない」と表現されているように、責任を負う事業者からの事故報告に依存していては、電気通信の事故の全貌を確認することは難しい場合もあります。 従って、電気通信の途絶に関する情報収集を重要視するのであれば、同一の事故について複数の報告がなされることを受け入れ、事故報告と事故の責任とを切り離して検討いただくことが望ましいと考えます。 一方で、電気通信に関する事故の責任の明確化及び同様の事故発生の防止に重きを置くのであれば、電気通信に関する事故の責任を負うべき範囲は、予見可能性・回避可能性の観点から、自己が管理する施設で事故が発生した場合に限定していただきたいと考えます。インターネットサービスにおいては、プロバイダーが管理する施設（例：サーバ）の故障等によりサービスの提供ができなかった場合はプロバイダーの責任となり、プロバイダーによる事故報告の対象とする一方、プロバイダーが管理していない電気通信網の故障・事故等により電気通信が途絶したことが原因でサービスの提供ができなかった場合は、プロバイダーの責任とならず事故報告の対象とならない、という整理が望まれます。

	時宜を得た検討に感謝申し上げますとともに、AICJ としても貢献して参ります。
在日米国商工会議所	【全般】 貴省の今般の意見募集におけるご指摘のとおり、絶え間ない急速な技術進化とインフラ整備に伴って、内外企業によるグローバル規模でのサービスの多様化、ステークホルダーの増大、リスクの複雑化等、電気通信役務提供を取り巻く環境は大きく変化している状況です。このような環境の変化を踏まえ、電気通信事故の報告・検証制度等の在り方の検討の機会を設けていただいたことに感謝申し上げます。 【3 頁　外国法人等に対する法執行の実効性の強化やイノベーションの進展等に伴う事故報告等の在り方】 在日米国商工会議所（ACCJ）は、貴省がガイドラインを改訂し、インターネットサービスの場合には、事故報告義務は、プロバイダが自らの行為によって特定の障害が発生したことを認識している場合に限定される旨明確にすることを要望します。 例えば、自然災害や社外の人間が原因でサービスが停止した場合には、その停止は積極的な報告義務から除外されるべきだと考えます。 プロバイダが障害を引き起こしたかどうかにかかわらず報告が求められる場合、貴省は、異なるプロバイダから同じ事故に関する複数の重複した報告を受けることとなると考えられます。 これは、貴省にとって事務処理上の負担となるだけでなく、貴省が障害の原因となっていないプロバイダからの報告を受けることとなり、必ずしもその原因を特定したり障害を修復したりすることにつながらないと考えます。 これは、インターネットを利用したメッセージングサービスの場合には、特に考慮すべき点です。メッセージングサービスは、通常、サービスの提供に利用されるインターネットアクセスインフラを所有または管理していないためです。

	例えば、携帯電話の電波塔がダウンしたり、インターネットへのアクセスができなくなったりして、ユーザーがメッセージングアプリを利用できなくなった場合、その原因や障害を解消するために講じた措置を総務省に報告する立場にあるのは、メッセージングアプリのプロバイダではなく、通信事業者やインターネットアクセスプロバイダであると考えられます。 メッセージングアプリのプロバイダは、原因を特定できない可能性があり、また、いずれにしても、利用者のインターネットサービスを回復させることはできないため、このような状況での報告は、貴省にとって有用な情報を提供することにはならないと思われます。 特に、報告書の提出を求められる可能性のあるプロバイダが世界中におよび、その数が潜在的に多いことを考えると、世界の産業界にかかる負担は、障害の影響を受けたがその原因となってはいないプロバイダからの報告書の有用性とは不釣り合いであると思われます。 検討事項を示した貴省の資料にも記載されているように、多様なサービスが数多く存在し、各企業、業界、サービスごとに特徴があります。報告においては、報告内容やどのメディア・ツールで報告するかなどについて、サービスごとに柔軟性または裁量が追加的に認められるべきであると考えます。特に BtoBtoX の場合においては、「影響を受けたユーザー」を計算することは、規制当局、ユーザー、消費者、サービス・プロバイダのいずれにとっても利益にはなりません。 【３頁 外国法人等に対する法執行の実効性の強化やイノベーションの進展等に伴う事故報告等の在り方】 事故報告の在り方について、事故報告の趣旨が、①電気通信の途絶に関する情報収集にあるのか、②電気通信に関する事故の責任を明確にして将来同様の事故が発生しないようにすることにあるのかを、明確にすべきであると考えます。 資料を拝見する限りでは、上記①と上記②を同時に求めていると解されます。しかし、現在の国際的な通信インフラを用いて世界中で電気通信役務の提供が行われる状況では、特にインターネットサービスでは、自己が管理する施設で事故が発生する場合だけでなく、自己が管理する施設に接続する他者が管理する施設で事故が発生する場合にも、電気通

	信が途絶する事象が生じることになります。 事故報告が氷山の一角に過ぎないと表現されているように、責任を負う事業者からの事故報告に依存していては、電気通信の事故の全貌を確認することは難しいと考えます。 従って、電気通信の事故情報を確認できるようにすることを重要視するのであれば、同一の事故について複数の報告がなされても構わないので、事故報告と事故の責任とを切り離すことを検討されるべきであると考えます。 【３頁 外国法人等に対する法執行の実効性の強化やイノベーションの進展等に伴う事故報告等の在り方】 事故報告の趣旨について、電気通信に関する事故の責任と将来同様の事故が発生しないようにすることに重きを置くのであれば、電気通信に関する事故の責任を負うべき範囲は、予見可能性・回避可能性の観点から、自己が管理する施設で事故が発生した場合に限定されるべきです。 従って、インターネットサービスでは、プロバイダが管理する施設（例：サーバ）の故障等により、サービスの提供ができなかった場合はプロバイダの責任となり、プロバイダによる事故報告の対象となるが、プロバイダが管理していない電気通信網の故障・事故等により電気通信が途絶し、サービスの提供ができなかった場合はプロバイダの責任とならず、事故報告の対象でないことを明確にすべきです。 【6 頁　電気通信事故の報告制度の概要】 ６頁には事故報告に関する現行の閾値が記載されています。これは 2013 年に開催された「多様化・複雑化する電気通信事故の防止の在り方に関する検討会」における議論を経て、現在のものとなっていると認識しています。しかしながら、今般の意見募集対象に記載されているとおり、電気通信事故を取り巻く環境は大きく変化しており、また、国内外のステークホルダーが増大していることを考えれば、閾値の考え方については、全てのステークホルダーにとって、より明朗かつ分かりやすいものに変更し、採用していただくことを要望します。 より具体的には、閾値について、EU や米国（ただし、米国の場合の報告対象は PSTN 網を使う電話や VoIP 等の電気通信

	サービスのみに限定されている）を含む諸外国で採用されている「ユーザー時間」（「影響利用者数」と「継続時間数」を掛け合わせて計算されるもの）の考え方を採用し、以下のように変更することを提案します。 現行の考え方：「影響利用者数●人以上」かつ「継続時間数●時間以上」 変更案：「ユーザー時間」（「影響利用者数」×「継続時間数」）≧ ● さらに、「ユーザー時間」の考え方のベースに引き直すと、現行の基準では、一つのカテゴリにおいて「ユーザー時間」が大きく異なる基準が２つずつ存在しており（例えば、インターネット関連サービス（無料）について「1200 万ユーザー時間又は 240 万ユーザー時間」、インターネット関連サービス（有料）について「6 万ユーザー時間又は 100 万ユーザー時間」）、かつ、一方の閾値が非常に低くなっています。 ネットワークが広域かつ複雑に広がっていることから、通信事故等に際しては、国内企業とグローバル企業の双方を含んだ数多くのステークホルダーの連携が必須です。そのような状況において、現行ルールの下での１つのカテゴリに大きく異なる２つの「ユーザー時間」の基準があることは、全てのステークホルダーにとって合理的に理解しづらいものと考えます。 以上より、国際的なハーモナイゼーションの利点および閾値の明確性に鑑み、「ユーザー時間」を基準にし、同じカテゴリにおいて１つの閾値を定め、著しく低い閾値を撤廃していただく合理化を要望します。 貴省の事故報告に関するガイドラインにおいては重大な事故について事業者に速やかな報告が求められています。外国事業者においては、接続障害の管理をグローバルに行っていたり、報告で技術面の説明が必要となる場合があるため、報告内容を日本語に翻訳し正確な説明を行うために追加的な時間を要します。そのため、即時の報告についてだけでも、英語による報告を貴省に認めていただくよう要望します。 上記と同様の理由により、重要な資料、ガイドライン、基準等は英語でも公表することが、日本国外にある事業者への執行を確保するための前提条件になると考えます。

株式会社　オプテージ	【①「自然災害」や「サイバー攻撃」等のリスクの深刻化】 サイバーセキュリティ対策における情報共有体制等と連携した事故報告・検証について 　通信ネットワークへのサイバー攻撃のリスクや脆弱性等への対処方法・ノウハウ等については、ベンダー等関係事業者にも依存する部分が多いため、ベンダー等関係事業者からの情報は重要と思います。また、事業者間を跨る通信サービスやクラウドサービスを経由する通信サービスもあり、通信事業者、クラウドサービス提供事業者からの情報も重要と思います。以上のことを踏まえると、ベンダー等の関係事業者や業界団体と情報共有できるシステム・仕組等が構築できれば、業界全体にとって安全・信頼性の向上に繋がり、有益と考えます。 　また、サイバー攻撃に関しては、サービスの不安定や停止に至らない場合や情報共有することによるセキュリティリスク(他の攻撃を誘導する等)等を考えると、各社とも情報開示を行うかどうかの判断が難しく、とはいえ、そのような情報こそが共有情報の根幹とも考えられますので、情報開示のガイドラインとその共有における秘密保持の在り方、特に通信の秘密や個人情報保護との整理も合わせて整備することが必要であると考えます。
個人５	要旨： 総務省は、まずは、ちゃんと、ISP 等の電気通信事業者が、電子メール役務において、電子メールの送受信（送受信双方）が、TLS で保護されるよう、指導等されたい。(現在、通信されている電子メールは、ほとんど漏えいといった状態であるはずである。) 意見全体： ＞全体的に 国民としては、政府行政機関が、口ばかりで全然まともに仕事をしていないと見る。 金融庁は暗号資産の事故において、毎度事業者にどの様な問題があったのかの報告書をちゃんと作成・提出させず、結局市井においてどの様な問題が事業者にあったのか分からないままにしているし（技術者としては本当にありえない程

	に愚かしいと侮蔑する。フィンテック等言う言葉はカッコイイかもしれないが、本当にやる気の無い能力の低い官庁であると見る。社会全体においての再発対策のために必要な事をしていないのではないか。）（※1）、総務省総合通信基盤局は電気通信事業について本来電気通信事業者になるべき存在について告発やその届出を行う行政指導をせず、また電気通信事業に関係する個人情報保護について関係代数的な認識に基づく個人情報該当回答をしようとしない（何も、例外的事態があるかもしれない、という留保を加える事を否定しているわけではないのであるから、簡単に関係代数的に個人情報該当か否かについて考えて照会への回答等をすればよいと考えるのであるが。）。また、明らかにその保護を行うべきである電子メールについて、各事業者に、素の SMTP メールでの送受信を許容するという様な行政を行っている（送受信される電子メールについては、通常、個人情報（そうでなくても個人識別情報）が付随しているが、また他個人情報や重要な内容を含む事が多いものであり、完全に、保護されるべきもの、という範疇に入るはずのものであるが、法定の電気通信事業者のうち、電子メールの扱いを行っている事業者に、その指導をしないのである。NTT ドコモの扱う利用者の電子メールについて、SMTP プロトコルが TLS で保護されていないようにしている、など、完全にバカかこの行政機関、と国民としては判断せざるを得ないのであるが、そういう状況を、STARTTLS が 1998 年に制定されて以降、20 数年間放置しているのが、我が国の電気通信行政を司る、総務省である（悪人たちが枕を高くして寝られる原因である者達であろう。なお、総務省は、事業者が SMTPoverTLS 及び STARTTLS による電子メール送受信を行っているかどうかについて電気通信役務の提供を受ける利用者に説明する義務についてあるとしていない（それは、電子メール役務に関して、品質や説明すべきその他の事項に該当する事なのではないのか？電気通信に関する役務において何が重要かどうか、分かっているのか？総務省は。）。）。）。 これではとてもまともな電気通信及び電気通信業界の発展を望めないと、今の政府行政機関を見て国民としては感じるのであるが、まずもってまともなセキュリティ対策が行われ（※なお、保護されていない素の SMTP プロトコルでの電子メール送受信など、常時「漏えい」の事態である事を指摘する。SMTP サーバ間と利用者の間、また各 SMTP サーバ間についてもちゃんと保護がなされないと（認証局証明書の取得とその管理など ISP 等においては日常の事なのであるから問題無いはずであるが。）、この「漏えい」の状態は直る事が無いはずであるが（総務省には、まずその様な事態について「漏えい」「せつ用」「知得」を使って説明する作文を行ってほしいものである。）、総務省は、目をちゃんと開けて、世の中を見たらどうなのであろうか？（体中から血が吹き出して死ぬであろうか？データセンター事業者等の善意という混沌的な要素に頼った人治的セキュリティが存在する、という概念は、国民として叩き直しておきたいのであるが。

	通信が技術的に「保護されている」とならない限り、その通信は「保護されていない」と判断するようにしていただけまいか（なお、この判断は、瞬時と言えるレベルで行えるはずである。素の HTTP は保護されていないプロトコルであり、TLS 等を用いた HTTPS は保護されたプロトコルである。その判断が行えるのなら行える様な事であるはずである。さて、20 数年間電子メールの保護を行うよう指導するのを懈怠していたのはどこの行政機関であろうか？当該行政機関はまともなつもりであろうか？）。国民としてはそう考える。））、その上で、セキュリティ保護された対象へのサイバー攻撃についての対応を行うようにされたい。 国は、急ぎ、IoT などでも利用される事の多い電子メールについて、各電気通信事業者に、事業者間での電子メール送受信に用いている SMTP プロトコルを TLS で保護するようにさせ、送受信双方について保護された形での利用が利用者に可能なようにするよう、その保護を行わない事は利用者を危険に晒す事である旨の解釈を公で示し、保護がなされるよう電気通信事業者等の指導等を行うようにされたい（SSH の利用やそういう事を行わずに、IoT だの M2M だのスマートホームだの言ってるのは、もう何が何やら、何だこの子供達は、という感じであるが（事業者も含め、まともな人間なら 30 代で総務省等の権威・善性の虚飾性を知り、その様な認識に至るのではないかと思われる。総合通信基盤局についてその邪悪さの存在を確信するようにのではないかと思われる。）、大人なら、真っ当な、専門分野をその仕事領域とする社会人なら、通信を暗号化（TLS 等は認証の用も為す（なおサーバにおける普及が進めば相互の認証を行える機会も増加する。）。）する必要性についてちゃんと認識し、国民（政府行政は、国民の足を撃たないようにされたい。また、撃たれないようにされたい。今の ICT 政策（※2）はそれを行っている部分がかなりある。）・市民・電気通信の利用者が保護されるようにしていっていただきたい。）。 一応、更に釘を刺しておくと、各種のインシデント報告や行政との連絡、そこでの重要情報のやり取り等も、電子メールを用いて行われるのであるから、まずは、自らの事務がちゃんと行えるようにするためにも、ISP 等の電気通信事業者が、電子メールの送受信（※送受信双方）について、TLS を用いて保護するようにするよう、指導等を行うようにされたい。 意見は以上である。

	※1 暗号資産についてはこの様であるが、勘定方の行政機関の他の一つである財務省外局である国税庁も、ICT 行政においても重要なものである法人番号に関して、行政事務においても様々な場面で用いるものである法人の納税証明書にその記載をしていないというとんでもない堕落した省庁である。…明らかにやる気が無いとしか判断されない。世の中の公正を図る気も、行政機関の便利を図る気も無いと断じられるものである。末端から大臣まで皆がおかしいと判断される。 ※2 近頃、この ICT という言葉もどうなのかという気がしているが（NEC（日本電気株式会社）などが言い始めた事であったかと思われるが。）。ITCT の方が良くないだろうか。