

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
中間報告(案)

～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～

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班
中間報告(案) 目次

I 検討事項	3
II TFの構成	3
III 検討経過	3
IV 検討結果	6
第1章 報告に向けた検討の経緯・進め方	6
1.1 検討の経緯.....	6
1.2 検討の背景・目的	10
第 2 章 安心・安全で信頼できる通信サービス・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	11
2.1 検討の方向性.....	11
2.2 通信事故の報告制度の見直しの在り方	21
2.2.1 はじめに	21
2.2.2 重要インフラ分野に提供される通信サービス・ネットワークに関する報告制度の在り方.....	30
2.2.3 通信事故の兆候(インシデント)に関する報告制度の在り方.....	44
2.2.4 四半期報告事故(簡易様式)の在り方	48
2.2.5 報告システムの在り方	50
2.3 通信事故の検証制度の見直しの在り方.....	55
2.4 自然災害を原因とする通信事故の報告制度等の在り方	65
2.5 サイバー攻撃を原因とする通信事故の報告制度等の在り方	78
第3章 今後の対応	89
3.1 今後の制度整備等に向けて	811
3.2 引続きの検討課題に向けて.....	210
別表1 事故報告・検証制度等タスクフォース 構成員	91

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たところである。

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、「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」について、本年 3 月から同 6 月までにかけて開催した IP ネットワーク設備委員会委員会 事故報告・検証制度等タスクフォース(第1回～第9回。以下、単に「TF」という。)において検討を行った結果を報告として取りまとめたものである。

II TFの構成

IP ネットワーク設備委員会の下に、作業班として、TFを開催して検討を行った。TFの構成は、別表1のとおりである。

III 検討経過

これまで、TF(第1回～第9回)を開催して検討を行い、「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」について、中間報告書を取りまとめた。

(1) TFでの検討

① 第1回会合(令和3年3月 11日)

電気通信事故の報告・検証制度等に関する現状と課題及び今後の進め方について、第 63 回 IP ネットワーク設備委員会(令和 3 年 3 月 5 日)での検討を受けて、意見交換を行った。

② 第2回会合(令和3年3月 29 日)

電気通信事故の報告・検証制度等に関する検討課題等について、関係事業者からヒアリングを行った。

③ 第3回会合(令和3年4月12日)

電気通信事故の報告・検証制度等に関する検討課題等について、関係事業者からヒアリングを行った。

④ 第4回会合(令和3年4月19日)

電気通信事故の報告・検証制度等に関する検討課題等について、関係事業者団体からヒアリングを行った。

⑤ 第5回会合(令和3年4月26日)

電気通信事故の報告・検証制度等に関する検討課題等について、有識者及び関係事業者からヒアリングを行った。

⑥ 第6回会合(令和3年5月14日)

電気通信事故の報告・検証制度等に関する検討課題等について、関係事業者からヒアリングを行うとともに、事故報告・検証制度等の在り方に関する論点整理を行った。

また、TF におけるこれまでの検討状況について、IP ネットワーク設備委員会に報告することとした。

⑦ 第7回会合(令和3年5月25日)

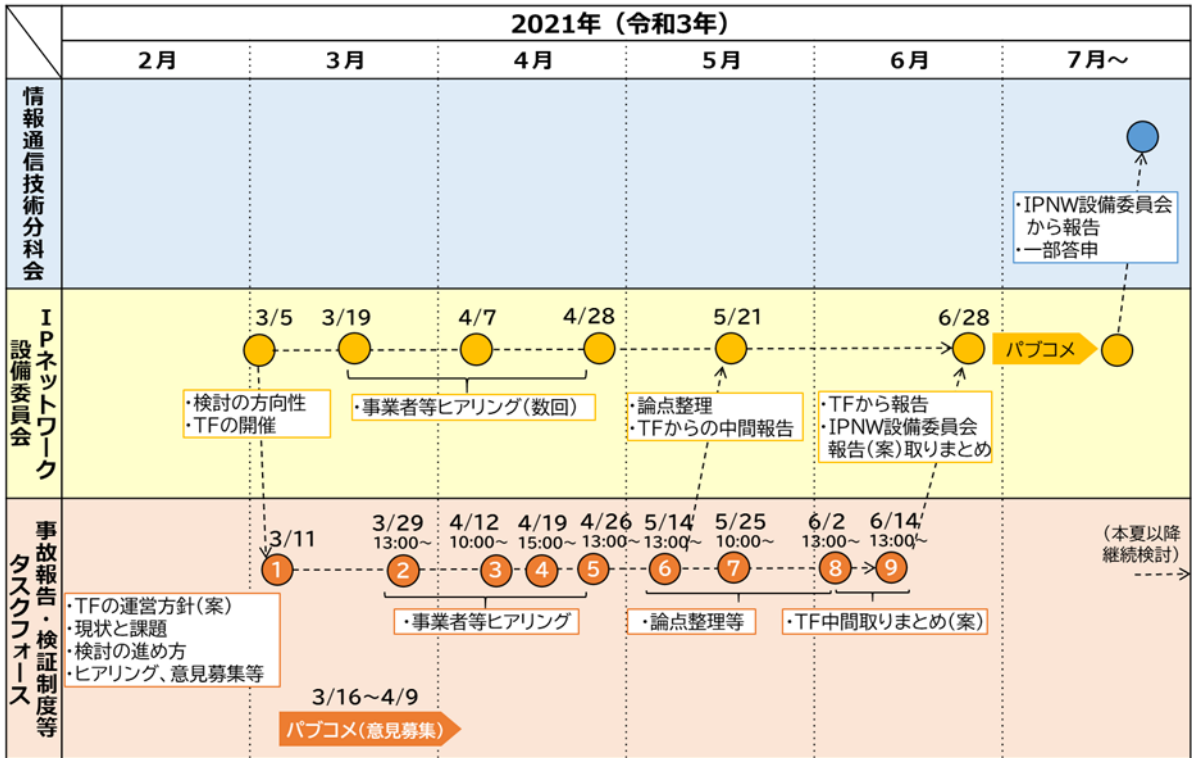
電気通信事故の報告・検証制度等に関する検討課題等について、利用者からヒアリングを行うとともに、第67回 IP ネットワーク設備委員会(令和3年5月21日)での検討を受けて、事故報告・検証制度等の在り方に関する論点整理を行った。

⑧ 第8回会合(令和3年6月2日)

TF におけるこれまでの検討結果を取りまとめた、事故報告・検証制度等タスクフォース中間報告(素案)について検討を行った。

⑨ 第9回会合(令和3年6月14日)

TF におけるこれまでの検討結果を取りまとめた、事故報告・検証制度等タスクフォース中間報告(案)について検討を行い、TF 中間報告を IP ネットワーク設備委員会に報告することとした。



【図 0.1】 TF における検討スケジュール

- 1. 第2回会合**
 - 2021年3月29日(月) 13:00~15:00【非公開】
 - ①日本電信電話(株)、東日本電信電話(株)、西日本電信電話(株)、②KDDI(株)、③ソフトバンク(株)、④楽天モバイル(株)
- 2. 第3回会合**
 - 2021年4月12日(月) 10:00~12:00【非公開】
 - ①日本電信電話(株)、(株)NTTドコモ、エヌ・ティ・ティ・コミュニケーションズ(株)、②ケーブルテレビ(株)、③スカパーJSAT(株)、④ヤフー(株)
- 3. 第4回会合**
 - 2021年4月19日(月) 15:00~17:00
 - ①(一社)電気通信事業者協会、②(一社)テレコムサービス協会、③(一社)日本ケーブルテレビ連盟
④(一社)日本インターネットプロバイダー協会、⑤(一社)ICT-ISAC
- 4. 第5回会合**
 - 2021年4月26日(月) 13:00~15:00 ※インターネットトラフィック流通効率化検討協議会
 - ①指田 朝久・立教大学大学院21世紀社会デザイン研究科客員教授、②CONNECT ※
③押立 貴志・法政大学大学院公共政策研究科講師(事故調査論)、④(株)NTTデータ
- 5. 第6回会合**
 - 2021年5月14日(金) 13:00~15:00【非公開】
 - ①アマゾンウェブサービスジャパン(株)、②(株)エヌ・ティ・ティネオメイト
- 6. 第7回会合**
 - 2021年5月25日(火) 10:00~【非公開】
 - ①千葉県

【図 0.2】 TF におけるヒアリング対象事業者等

IV 検討結果

第1章 報告に向けた検討の経緯・進め方

1.1 検討の経緯

IP ネットワーク設備委員会報告「電気通信事故等に関する事項」(2009年7月)及び「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」報告書(総務省2013年10月)を踏まえ、通信事故の第三者検証等のための機関として、2015年5月より「電気通信事故検証会議」が開催されている。

上記会議において、2020年4月から7月までの間、2015年以降5年間における平成時代の総括とともに、令和時代における新たな環境やリスクの変化を踏まえ、今後の通信事故の報告及び検証の在り方について検討が行われた。

以上の結果、「令和元年度電気通信事故に関する検証報告」(総務省2020年9月)において、ニュー・ノーマルに対応したデジタル強靱化社会には、より安心・安全で信頼できる情報通信ネットワークの確保が必要不可欠であり、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等、マルチステークホルダー連携によるガバナンスの在り方に関する議論を深める必要性が提言された。

- 通信事故の大規模化・長時間化やその内容・原因等の多様化・複雑化を踏まえ、通信事業者から報告された通信事故について、外部の専門的知見を活用しつつ検証を行うことにより、通信事故の発生に係る各段階で必要な措置が適切に確保される環境を整備するとともに、通信事故の再発防止を図る。
- 「IPネットワーク設備委員会」報告(2009年7月)及び「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(2013年10月)等を踏まえ、電気通信事業部長主催の会議として、2015年5月に設置。

- ▶ 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。(以下、50音順。令和3年5月現在)
 - 相田 仁 (東京大学副学長・大学院工学系研究科 教授)【座長】
 - 阿部 俊二 (国立情報学研究所アーキテクチャ科学研究系 准教授)
 - 内田 真人 (早稲田大学基幹理工学部情報理工学科 教授)【座長代理】
 - 加藤 玲子 ((独)国民生活センター相談情報部相談第2課 課長)
 - 森島 直人 (EYアドバイザリー・アンド・コンサルティング株式会社 シニアマネージャー)
 - 矢入 郁子 (上智大学理工学部情報理工学科 准教授)
- ▶ 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。



【図 1.1.1】「電気通信事故検証会議」の概要

- 「電気通信事故検証会議」において、同会議の設置以降 5 年間における**平成時代の総括**とともに、令和時代における新たな動向を踏まえ、**今後の電気通信事故の報告及び検証の在り方**について検討。
- ニュー・ノーマルに対応したデジタル強靱化社会には、**より安心・安全で信頼できる情報通信ネットワークの確保が必要不可欠**。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等**、**マルチステークホルダー連携によるガバナンスの在り方**に関する議論を深める必要性を提言。

自然災害を起因とする 障害や事故に関する 報告等の在り方

- 豪雨、台風、地震等による大規模な自然災害が頻発化等。「令和元年房総半島台風（台風15号）」等、**甚大被害をもたらす災害が毎年発生**。
- 自然災害による事故は、出水期に係る**第2四半期及び第3四半期**に例年共通して多くが報告。また、年々、**件数自体も増加傾向**。
- 激甚化等する自然災害により、**通信障害も広域化・長期化**。被災地の通信環境の確保は、被災地における**生活改善や復旧活動等に益々重要**。
- 自然災害による事故等の報告及びその分析・検証等の在り方について、**より有効・迅速な復旧等の対策を総合的に推進する観点で検討が必要**。

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 事故報告等の在り方

- 令和元年度より、「**送信型対電気通信設備サイバー攻撃**」による事故が報告対象。**氷山の一角**に過ぎないと考えられるが、8件が報告。
- 電気通信分野は、**他の重要インフラ分野からの依存度**が高まっており、かつ、比較的短時間の障害でもその影響が大きくなる恐れ。
- 来夏に開催予定の**東京オリンピックパラリンピック競技大会**を控える中、**情報共有の質・量の改善等、PDCAの実効性の強化**が必要。
- 他の重要インフラ分野を先導する観点から、**サイバーセキュリティ対策と連携した情報通信ネットワークの安全・信頼性の向上について検討が必要**。

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

- グローバル化に伴い、**外国法人等が提供する電気通信サービス等の国内における利用の拡大**。今後、これらに対する法執行の実効性強化が課題。
- **新型コロナウイルス感染防止**のため、**BtoBも含むテレワーク等遠隔・非接触サービスを支える電気通信サービス**に求められる役割・期待が一層向上。
- **ソフトウェア化や仮想化・クラウド等**のイノベーション、**海外事業者等も含めたマルチステークホルダー連携による情報通信ネットワークの構築等**が進展。
- **事故報告等によるガバナンス**につき環境変化・リスク多様化等に対応した**安心・安全で信頼できる情報通信ネットワークの確保の観点から検討が必要**。

【図 1.1.2】令和時代の事故報告等の在り方

(出典:「令和元年度電気通信事故に関する検証報告」概要(2020年9月))

上記検証報告については、第 61 回 IP ネットワーク設備委員会(2020年9月18日)において、総務省より報告が行われ、次のような意見があった。

- インターネット障害には、意図的でない故障と悪意のある人による故障があり、後者の場合、セキュリティ問題になる。単なる障害の場合も、セキュリティ問題の場合も、過去の教訓等のフォローアップということで、悠長だと感じる。セキュリティに関わる事故が起こった場合、事業者だけで解決できるのかという課題があると思う。事故の対応について相談できるプロフェッショナル集団のような組織が求められる。
- 経路情報の問題が起きたという事故があったが、経路情報が意図的に操作されるとナショナルセキュリティに発展する怖さがあるので、やはりプロ集団が必要ではないかと思う。
- サイバーセキュリティ関係の事故かどうかという分類ができたのが今年なので、これまでどれだけそういった事故があったか、あまり明確ではない。ただ、5年前の時点では、意図しない、つまらないヒューマンエラーによる事故が結構な数あったので、そういった事故をなくすために、作業をする際はあらかじめ手順を作って確認しながら行うなどの方針を示し、それはグッドプラクティス、ベース

トプラクティスとして成果を上げてきたと思う。しかし、5年経ってみると、取り巻く環境がかなり変わってきている。

そこで、以上を踏まえ、第63回IPネットワーク設備委員会(2021年3月5日)において、「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」について集中的に検討を行うための作業班として、TFを開催することが承認された。その際、次のような意見があった。

- 通信事故の報告制度において、インターネット関連サービス、特に新しいクラウド系についても検討することは、非常に重要。電気通信設備の構成やそのサービスが非常に複雑化している中、クラウドに係る事故、例えばGメールのサービス停止等、これまでの通信設備の範囲外のことも消費者の生活に影響を及ぼすようになっている。ただ、それらに対して事前に網をかけて制度や基準を作ることは非常に難しいので、実際に発生した事故から原因を切り分けていくところから、制度を作っていくという形が望ましい。
- PDCAでは対応できなくなってきたことを前提に、OODAを意識した制度設計にしなければならない。PDCAの場合は、システム全体を把握できている前提でガバナンスコードを作っているが、特に自然災害は予期できないことが起きるとのこと、また、人災の場合も、攻撃でもなく、意図的でもなく、実装上の技術的な問題点が、OSS、マルチステークホルダー、サプライチェーンの中で発生するということになってくると、これはガバナンスコードとしての企業の中での管理に関係してくる。事故調査をした結果として、対策としてガバナンスコードの話が当然出てくるだろうが、このあたりの整理が必要。
- プロダクトとサービスが全部国際的につながっていることを強く意識する必要がある。その意味では、国際機関、例えばインターネットでいうとIGF、ITU、ISO等でこの問題をどうトレーシングしていくか、国際的なルールの中で担保しておかなければ、事故調査自体が非常に難しく、対処できなくなってしまう。
- 電気通信事故検証会議における5年間の検証の中で、事故のほとんどはヒューマンエラーや設備の不備が原因ではあるものの、国際問題のために、あるところから先が一切事故の原因追及や検証ができないという事象もいくつかあった。検証できないというのは、事故検証会議としてある意味敗北的な部分もあると思っており、今後、外国企業が情報開示を拒否した場合、何とか少しでも開示していただけるような仕組みを考えていかなければならない。ただ、日本企業が外国企業に対して、事故の際に総務省に情報開示しなければならないという項目を提示した場合、契約料が高くなってしまいう等の問題が起こりうるので、うまい落としどころを探さなければならない。

- 原因究明に至らなかった極端な例としては、メーカーも事象を再現できず、宇宙線によるソフトエラーではないかというレポートが上がってきたこともある。あるところから先、本当の意味での原因究明が難しい可能性があることも考慮して、どのようにシステムを組めばよいのか、いざそういったことが起きたらどのように対応すればよいのか、知恵をつけていくことになるかと思う。
- サイバーセキュリティ、仮想化、マルチステークホルダー化等、情報通信ネットワークを取り巻く近年の環境変化に伴うリスクへの対応が一層重要になってきており、今後も情報通信ネットワークの安全性や信頼性を確保する上で、従来の事故報告・検証制度の在り方について、先ほど、PDCAではなくOODAがキーワードになってきている、そもそも検証のための条件が満足できないこともある、といったご指摘があったが、そういった観点によるアップデートが必要。

また、第67回IPネットワーク設備委員会(2021年5月21日)において、TFにおける検討状況について報告を行った。その際、次のような意見があった。

- OODAループを入れていただいたが、これは大事。
- 総務省と事業者の関係は大体ここで定義されているが、このプロセスをちゃんと動かすためには、事業者内でのガバナンスコードとして、安全・安心、監査機能として同コードの中に埋め込んでいかなければならない。そして、それをやる人に対する立場をコーポレートガバナンスとして上げることが実装上とても必要。今のコーポレートガバナンスコード的には監査等委員会に移行している会社もすごく増えている。

1.2 検討の背景・目的

我が国では、フィジカル空間とサイバー空間が高度に融合・一体化する CPS (Cyber Physical System) により経済発展と社会的課題の解決を両立する人間中心の社会「Society5.0」を目指している。そのような中、with/after コロナ時代における「新たな日常」に対応した強靱な経済・社会を構築するためには、CPS が益々重要となっている。また、「デジタル社会」の形成に関する検討が急速に進められ、本年5月、デジタル社会形成基本法及びデジタル庁設置法等のデジタル改革関連法が成立した。

以上を実現するためには、サイバー空間を構成する中核であるとともに、サイバー空間とフィジカル空間とを繋ぐ通信サービスの継続的・安定的かつ確実な提供という価値が一層求められ、その基盤として、安心・安全で信頼できる情報通信ネットワークを確保することが必要不可欠となっている。

この点、情報通信ネットワークを取り巻く環境について、近年、①自然災害やサイバー攻撃等の発生自体が不可避なグローバルリスクの深刻化、②外国企業等による通信事業者やサービスの多様化、③with/after コロナに伴い益々浸透している遠隔・非接触サービスに不可欠なブロードバンドサービスやインターネット関連サービス等の通信サービスのユニバーサル化、④5G 本格展開等による他の重要インフラとの相互依存の深まり等の情報通信ネットワークの産業・社会基盤化、そして、⑤仮想化・ソフトウェア化等による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等の変化が発生している。

新たな環境変化に伴い、通信事故の発生により生命・身体・財産に直接的な影響を与えるリスクも増大するなど、通信分野における安全・信頼性対策が取組むリスクが多様化・複雑化している。これらのリスクに適切に対応するためには、通信事業者による自主的な取組のみならず、関係する他の事業者、個人や法人等の利用者等のマルチステークホルダー間の連携・協力によるガバナンスを通じて、通信事故の防止や被害の拡大防止等に社会全体で取組むことが必要となっている。

そこで、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として、安心・安全で信頼できる情報通信ネットワークが確保されるよう、2020 年代半ば頃に向けた、①事故報告・検証制度、②情報通信ネットワーク安全・信頼性基準等の在り方について検討を行うための作業班として、「事故報告・検証制度等タスクフォース」が開催されることとなった。

第 2 章 安心・安全で信頼できる通信サービス・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

2.1 検討の方向性

(1)現状・課題

通信サービス・ネットワークにおける電気通信設備に関する安全・信頼性対策(以下、単に「通信サービス・ネットワークの安全・信頼性対策」という。)については、通信サービスの円滑な(確実かつ安定的な)提供を確保するとともに、その利用者(一般消費者、通信事業者を含む法人利用者)の利益を保護することを目的としている。

以上の目的を実現するにあたっては、イノベーションの進展等の環境変化に適時適切に対応するため、提供する通信サービスやその基盤となる通信ネットワークの構成・設備等の特性を熟知する通信事業者による主体的な取組が有効・重要であり、通信事業者の自主的な取組(自律的・継続的な PDCA サイクル)に委ねることが基本となっている。

他方、電気通信回線設備の設置の有無や提供する通信サービスの社会的影響力(生命・身体・財産との関連性、利用者数の規模、料金徴収の有無、サービスの同時・双方向性、サービスの代替性の程度等)の観点から、通信事故等による影響が大きい通信事業者(回線設備設置事業者等、有料で利用者 100 万以上の通信サービスを提供する回線設備非設置事業者)については、自主的な取組に全てを委ねるのは適当ではないことから、通信事業者による自律的・継続的な PDCA サイクルが適時適切に確保・促進されるため、その取組を下支えする枠組みとして、総務省において、技術基準や管理規程等の制度が整備・強化されてきている。

【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(総務省2013年10月31日) (抄)】



【図 2.1.1】安全・信頼性対策に関する基本的な枠組み

(出典:「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」報告書(総務省 2013 年 10 月))

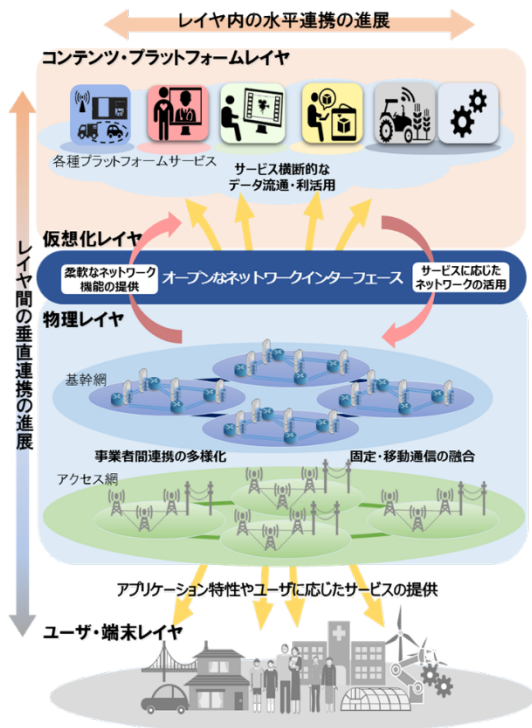
中でも、通信事故の報告・検証制度については、全ての通信事業者(2021年4月現在、約2万2千者)が対象になっている。そして、実際に発生した通信事故の報告・分析・評価等を通じ、通信サービス・ネットワークの安全・信頼性対策について、総務省が改めて検証し、再発防止等に向けた関係者の取組を継続的に充実・強化するために不可欠なPDCAサイクルの要となっている。

電気通信事業者 (登録及び届出)		(2021年4月1日現在)
回線設置 (基礎的役務含む) 約450社		有料かつ大規模 回線非設置 4社
		回線非設置(左記以外)約2.15万社
監督責任	電気通信設備統括管理者	●経営レベルの事業用電気通信設備の統括管理 電気通信事業者が経営陣で実務経験のある者から選任、事故防止対策に主体的に関与。 【法第44条の3等、電気通信事業法施行規則(省令)】
	電気通信主任技術者	●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者を選任して事業用電気通信設備を監督。電気通信主任技術者に登録講習機関による講習を受けさせる義務。【法第45条等、電気通信主任技術者規則(省令)】
	工事担任者	●端末設備等の接続の工事を実施等 資格者が利用者の端末設備等の接続の工事を実施・実地監督。 【法第71条・第74条等、工事担任者規則(省令)】
強制基準	技術基準	●電気通信事業者の事業用電気通信設備の技術基準 予備機器、停電対策、耐震対策、防護措置、通話品質等を規定。 【法第41条・第42条等、事業用電気通信設備規則(省令)】 ●利用者の端末設備等の接続の技術基準 安全性、電氣的条件、責任の分界、セキュリティ対策等を規定。登録認定機関等が技術基準適合認定等を実施。登録修理業者は修理された端末機器の技術基準適合性を確保義務。 【法第52条・第86条等、端末設備等規則(省令)、技術基準適合認定等に関する規則(省令)】
	管理規程	●事業用電気通信設備の管理に係る事業者毎の特性に応じた自主基準 部門横断的な設備管理の方針、電気通信主任技術者等の職務、組織内外の連携、事故対応等を定める義務。 【法第44条等、電気通信事業法施行規則(省令)】
推奨基準	安全・信頼性基準	●情報通信ネットワーク全体の安全・信頼性対策に関する基本的・総合的な指標を整理した推奨基準(ガイドライン) 設備等に関する「設備等基準」と、設計・施工・運用等に関する「管理基準」に区分、大規模インターネット障害対策、ソフトウェア信頼性向上、災害対策、事故状況の情報公開等を規定。自営情報通信ネットワークやユーザーネットワークも対象。 【情報通信ネットワーク安全・信頼性基準(告示)】
報告義務等	事故報告 事故検証	●一定の基準を超える規模の電気通信事故が発生した場合に報告 重大事故:事故発生後の速やかな連絡、事故発生後30日以内における詳細(概要、原因、対応状況、再発防止策等)を報告 四半期報告事故:四半期ごとに、事故の概要を報告 【法第28条、電気通信事業用施行規則(省令)、電気通信事業報告規則(省令)】 ●重大事故等に関する第三者検証 【電気通信事故検証会議】

【図 2.1.2】安全・信頼性対策に関する制度

そこで、上記 PDCA サイクルを取り巻く環境として、近年、次の変化が進展することに伴い、当該サイクルが取組むリスクが多様化・複雑化しており、2020年代半ば頃に向けた通信事故の報告・検証制度の在り方について、検討が必要となっている。

- 1) 自然災害やサイバー攻撃等の発生自体が不可避なグローバルリスクの深刻化
- 2) 外国企業等による通信事業者やサービスの多様化
- 3) with/after コロナに伴い益々浸透している遠隔・非接触サービスに不可欠なブロードバンドサービスやインターネット関連サービス等の通信サービスのユニバーサル化
- 4) 5G 本格展開等による他の重要インフラとの相互依存の深まり等の情報通信ネットワークの産業・社会基盤化
- 5) 仮想化・ソフトウェア化等による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



- ① **自然災害やサイバー攻撃等のリスクの深刻化**
 - 例 ● 自然災害を発生要因とする事故の報告・検証
 - サイバーセキュリティ対策と連携した事故報告・検証
- ② **外国企業等による通信事業者や通信サービスの多様化**
 - 例 ● 外国法人等に対する法執行の実効性強化の適用対象となる具体的なサービスを踏まえた事故報告等
- 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通信サービスのユニバーサル化**
 - 例 ● 「インターネット関連サービス」等に関する報告基準
 - 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
- ④ **通信ネットワークの産業・社会基盤化**
 - 例 ● テレワーク・遠隔学習等向けサービスに関する報告基準
 - 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
- ⑤ **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**
 - 例 ● 事故や被害の原因究明調査等によるサプライチェーン対策
 - 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

【図 2.1.3】 通信事故の報告・検証制度を取巻く環境・リスクの変化と検討事項

なお、通信分野を含む重要インフラ防護の基本的枠組みに関する「重要インフラの情報セキュリティ対策に係る第4次行動計画」（2020年1月サイバーセキュリティ戦略本部改定等。以下、「行動計画」という。）によると、重要インフラ事業者等における行動規範については、自主的に見直しの必要性を判断して改善できる PDCA サイクル自体は浸透しつつあるが、C（確認）と A（是正）の取組については、いまだに十分に定着しているとは言えず、行動様式として根付いているとは認められない状況であり、その定着が課題であるとされている。

行動計画では、通信分野について、各重要インフラ分野における情報通信技術の活用が進展し、また各分野間の相互依存関係が増大する中、他分野からの依存度が高く、かつ、比較的短時間の障害であってもその影響が大きくなるおそれのある分野とされている。そのため、主要な事業者等を中心として、相対的に高度な対策が自主的に進められており、引続き先導的取組を更に強化・推進し、他分野等に広めていくことが期待されている。

(2)考え方

①通信事業者による主導的役割の必要性

デジタル社会の実現のためには、その中枢基盤として、サイバー空間とフィジカル空間を繋ぐ神経網である通信サービス・ネットワークが安心・安全で信頼され、円滑に(安定的かつ確実に)提供されることが不可欠である。そのため、通信サービス・ネットワークの安全・信頼性対策が極めて重要になると考えられる。

この点、本年 5 月に成立したデジタル社会形成基本法においては、基本理念として「国民が安全で安心して暮らせる社会の実現」(第 7 条)が規定されるとともに、デジタル社会の形成は民間が主導的役割を担うという原則の下、国等は民間の知見を積極的に活用して、環境整備を中心とした施策を行うとされ、例えば、サイバーセキュリティの確保や通信ネットワークの災害対策など国民が安心して高度情報通信ネットワークを利用できるようにするために必要な措置を講じる旨が規定されている。

以上を踏まえると、デジタル社会を支える中枢基盤である通信分野においては、イノベーションの進展が著しい中、通信事業者間のサービス競争も激しく、市場環境変化のスピードが速いこと等から、引続き、民間である通信事業者が主導的役割を担うことが必要と考えられる。

(国民が安全で安心して暮らせる社会の実現)

第7条 デジタル社会の形成は、**高度情報通信ネットワークの利用**及び情報通信技術を用いた情報の活用により、**大規模な災害の発生、感染症のまん延その他の国民の生命、身体又は財産に重大な被害が生じ、又は生ずるおそれがある事態に迅速かつ適確に対応することにより、被害の発生を防止又は軽減が図られ、もって国民が安全で安心して暮らせる社会の実現に寄与するものでなければならない。**

(国及び地方公共団体と民間との役割分担)

第9条 デジタル社会の形成に当たっては、**民間が主導的役割を担うことを原則とし、国及び地方公共団体は、民間の知見を積極的に活用しながら、公正な競争の促進、規制の見直し等デジタル社会の形成を阻害する要因の解消その他の民間の活力が十分に発揮されるための環境整備並びに公共サービス(公共サービス基本法(平成21年法律第40号)第2条に規定する公共サービスをいう。第29条において同じ。)**における国民の利便性の向上並びに行政運営の簡素化、効率化及び透明性の向上のための**環境整備を中心とした施策を行うものとする。**

(国及び地方公共団体の責務)

第13条 **国は、前章に定めるデジタル社会の形成についての基本理念(以下「基本理念」という。)にのっとり、デジタル社会の形成に関する施策を策定し、及び実施する責務を有する。**

(事業者の責務)

第16条 **事業者は、基本理念にのっとり、その事業活動に関し、自ら積極的にデジタル社会の形成の推進に努めるとともに、国又は地方公共団体が実施するデジタル社会の形成に関する施策に協力するよう努めるものとする。**

(サイバーセキュリティの確保等)

第33条 **デジタル社会の形成に関する施策の策定に当たっては、サイバーセキュリティ(サイバーセキュリティ基本法(平成26年法律第104号)第2に規定するサイバーセキュリティをいう。第37条第2項第14号において同じ。)の確保、情報通信技術を用いた犯罪の防止、情報通信技術を用いた本人確認の信頼性の確保、情報の改変の防止、高度情報通信ネットワークの災害対策、個人情報保護その他の国民が安心して高度情報通信ネットワークの利用及び情報通信技術を用いた情報の活用を行うことができるようにするために必要な措置が講じられなければならない。**

【図 2.1.4】 デジタル社会形成基本法(2021年5月19日法律第35号)

②リスクマネジメント・OODA ループ的な対応の重要性

前述したように、環境変化に伴い、通信サービス・ネットワークの安全・信頼性対策が取組むリスクの多様化・複雑化が進展する中、通信事業者が主導的役割を担うにあたり、自らが提供する通信サービスやその基盤となる通信ネットワークの構成・設備等の特性を熟知することが益々困難になってきている。そのため、それらに影響を及ぼすリスクの特定・分析等による最適化を図る「リスクマネジメント」に取り組むことが一層必要になってきている。

リスクマネジメントについては、通信サービス・ネットワークの安全・信頼性対策の関係者間における共通的な考え方や用語等を踏まえた取組が重要である。この点、行動計画及び同計画に基づく「重要インフラにおける機能保証に基づくリスクアセスメント手引書(第1版)」(2019年5月同本部重要インフラ専門調査会改定等。以下、「手引書」という。)においても、リスクマネジメントの重要性についての認識は広まりつつあるとされている一方、リスクマネジメントの考え方や実施方法が十分に定着しているとは言いがたい状況であるとしている。

この点、行動計画によると、「リスクマネジメント」については、次の通りとされている。

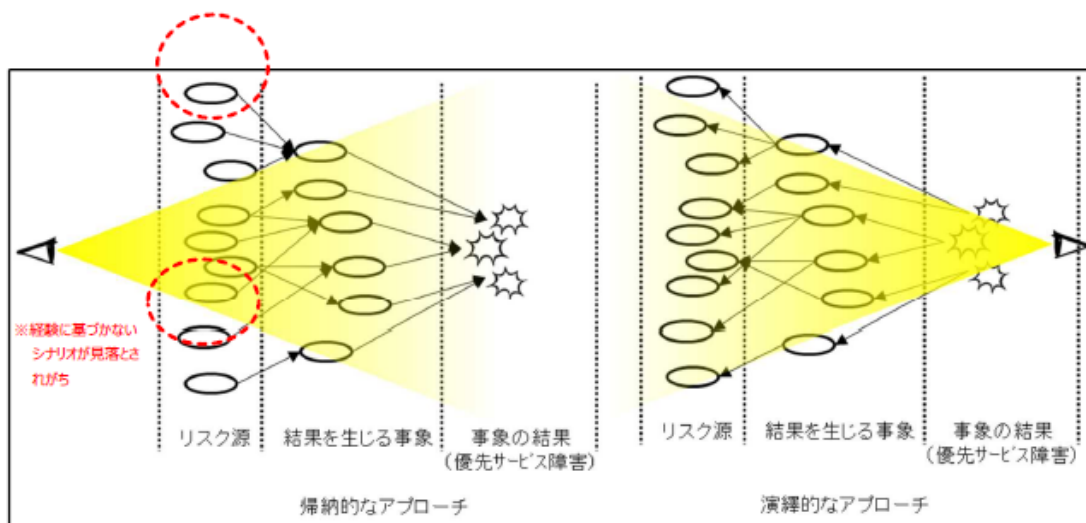
- 情報通信技術の活用の進展に伴い、サイバー攻撃や情報システムの不具合に起因する個人情報の漏えいやサービス提供の中断による経済的損失等の事例が頻繁に報告されており、実社会への被害が深刻化している。未公開の脆弱性を狙ったゼロデイ攻撃のような高度化したサイバー攻撃や内部不正に関しては、もはや「未然に防ぎきることは不可能である」ということを認識する必要がある。
- こうした状況において、重要インフラ事業者等にあっては、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、リスクアセスメントの結果を踏まえたリスク対応を戦略的に講じることが必須の要件となっており、機能保証の観点からは、サイバー攻撃等に遭遇した場合であっても、重要インフラサービスを安全かつ継続的に提供できるように、リスクアセスメントの結果を踏まえた適切な対処態勢が整備されることも必要である。また、こうした活動全体(リスクマネジメント)が継続的かつ有効に機能するための仕組みを構築することも重要である。
- リスクマネジメントは、各重要インフラ事業者等がそれぞれにおいて主体的に実施するものである。一方で、各関係主体間において共通的なリスクマネジメントの考え方や用語による情報共有及び議論がなされない状態では、本行動計画における各種取組が、各重要インフラ事業者等のリスクマネジメントにおいて効果的に生かすことができない可能性がある。

このため、手引書では、国際標準規格「ISO31000」及び同規格に基づく国内規格

「JIS Q31000」における考え方や用語等に準拠しつつ、機能保証の考え方に基づくリスクアセスメントの方針として、重要インフラ事業者等における経営戦略上の「目的」を「社会経済システムの中で果たすべき役割・機能を発揮するために必要なサービスの提供を維持・継続すること」とし、「リスク」として、当該「目的に対する不確かさの影響」のうち「負の影響:好ましくない結果をもたらすリスク)に限定している。

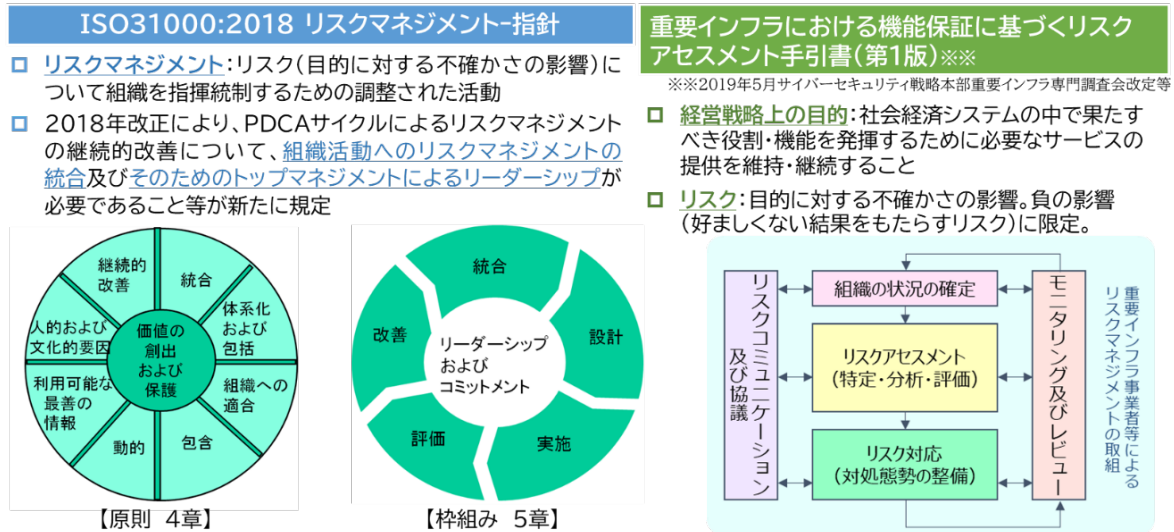
また、リスクアセスメントのアプローチとして、「演繹的なリスクアセスメント」が基本であるとしている。具体的には、「発生確率の低い事象から目を背けた(発生した場合には危機的状況につながる可能性がある事象であっても、過去に経験していない、又は発生確率が低いためにリスクとして想定しなかった)ことにより、その事象の結果が想定外となって大きな混乱を招くこととなった東日本大震災での教訓」を踏まえ、「影響する事象の結果からリスク源までを演繹的に特定・分析・評価」するアプローチを基本としつつ、多くの重要インフラ事業者等で実施されているイベントツリー分析等の帰納的なアプローチとの組合せによる効率的な作業への配慮等も示している。

	帰納的なアプローチ	演繹的なアプローチ
概要	リスク源を想定し、そのリスク源から派生する様々な事象及び事象の結果がどうなるかを明らかにする手法 (イメージ) $\mathcal{R} \times \mathcal{E} \rightarrow \mathcal{Q}$	事象の結果を想定し、その結果に至る様々な事象及びリスク源を明らかにする手法 (イメージ) $\mathcal{Q} \leftarrow \mathcal{E} \times \mathcal{R}$
主な手法	イベントツリー分析	フォールトツリー分析
メリット	個別のシナリオ分析に優れており、各シナリオに応じた対処事項についての有効な知見を得ることができる	事象の結果に関するシナリオを演繹的に分析することにより、網羅的に全容を知ることができる
デメリット	リスク源を網羅することが難しい	提供するサービスや業務の構成が複雑な場合、分析結果の組合せが爆発的に増加し、作業負荷が多くなる



【図 2.1.5】 リスクアセスメントのアプローチ
(出典:「重要インフラにおける機能保証に基づくリスクアセスメント手引書(第1版)」)

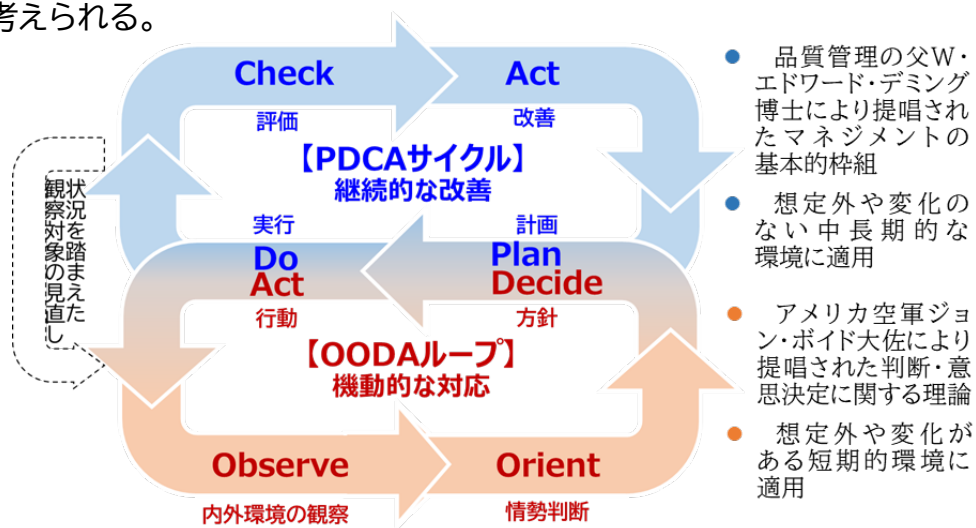
今後は、通信サービス・ネットワークの安全・信頼性対策においても、基本的に、以上の考え方等を踏まえて取組むことが重要になっている。なお、ISO31000 については、2018 年に改正され、PDCA サイクルによるリスクマネジメントの継続的改善について、組織活動へのリスクマネジメントの統合及びそのためのトップマネジメントによるリーダーシップの必要性等が新たに規定されている。



【出典】指田朝久(立教大学大学院21世紀社会デザイン研究科客員教授等)「リスクマネジメントと危機管理～想定内と想定外:原点に戻って考える～」(2020年4月26日事故報告・検証制度等TF第5回)等

【図 2.1.6】通信分野の安全・信頼性対策における「リスクマネジメント」の考え方

また、未然に防ぎきることは不可能である状況等不測の事態においては、「OODA ループ」的な対応も重要である。OODA とは、Observe(内外環境の観察)、Orient(方向付け・情勢判断)、Decide(方針・意思決定)、Act(行動)の略であり、判断・意思決定に関する理論として、想定外や変化がある短期的環境に適用される考え方である。この考え方については、特に、Observe 及び Orient の観点から PDCA サイクルを補強するものと考えられる。



【出典】(株)日本総合研究所・経営コラム「“VUCAの時代”のビジョンデザインと未来年表」(2018年09月14日 粟田恵吾)やチャット・リチャーズ著等「OODA LOOP」(東洋経済新報社)等を参考として事務局作成

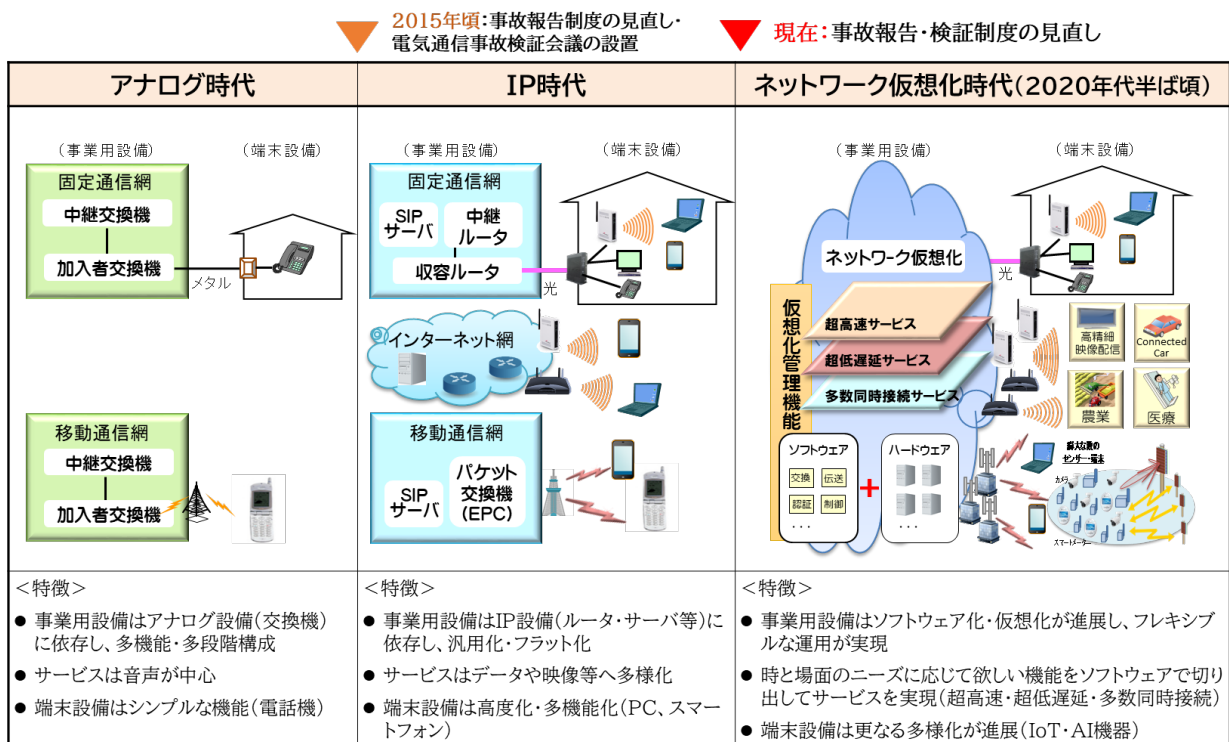
【図 2.1.7】OODA ループによる PDCA サイクルの補強

(3)検討の方向性

通信サービス・ネットワークの安全・信頼性対策に関する PDCA サイクルについては、通信事業者における適切な対応、総務省における施策の立案や他通信事業者への水平展開等による継続的改善を図るため、車の両輪として、①OODA ループ的な対応に関する重大事故の報告制度、②電気通信事故検証会議による重大事故等の検証制度から構築されている。

この点、上記 PDCA サイクルが取扱うリスクが、VUCA (Volatility: 変動性, Uncertainty: 不確実性, Complexity: 複雑性, Ambiguity: 曖昧性)といわれる環境変化により、量的・質的に変化するとともに、マルチステークホルダー(通信事業者、ベンダやメーカ等関係事業者、個人や法人等利用者や公的機関等の安心・安全で信頼できる通信サービス・ネットワークを確保するための課題解決における関係者。以下、同じ。)に拡散している。そのため、前述の OODA ループ及びリスクマネジメントの考え方を踏まえ、上記 PDCA サイクルを見直すことが求められている。

従って、2020年代半ば頃に向けて、デジタル社会における通信事故の防止や被害の拡大防止等という目的を達成するため、総務省においては、そのリーダーシップにより、マルチステークホルダーとの連携・協力を通じた統合を推進し、通信事業者が引続き主導的な役割を担うことができる環境を整備することが必要である。

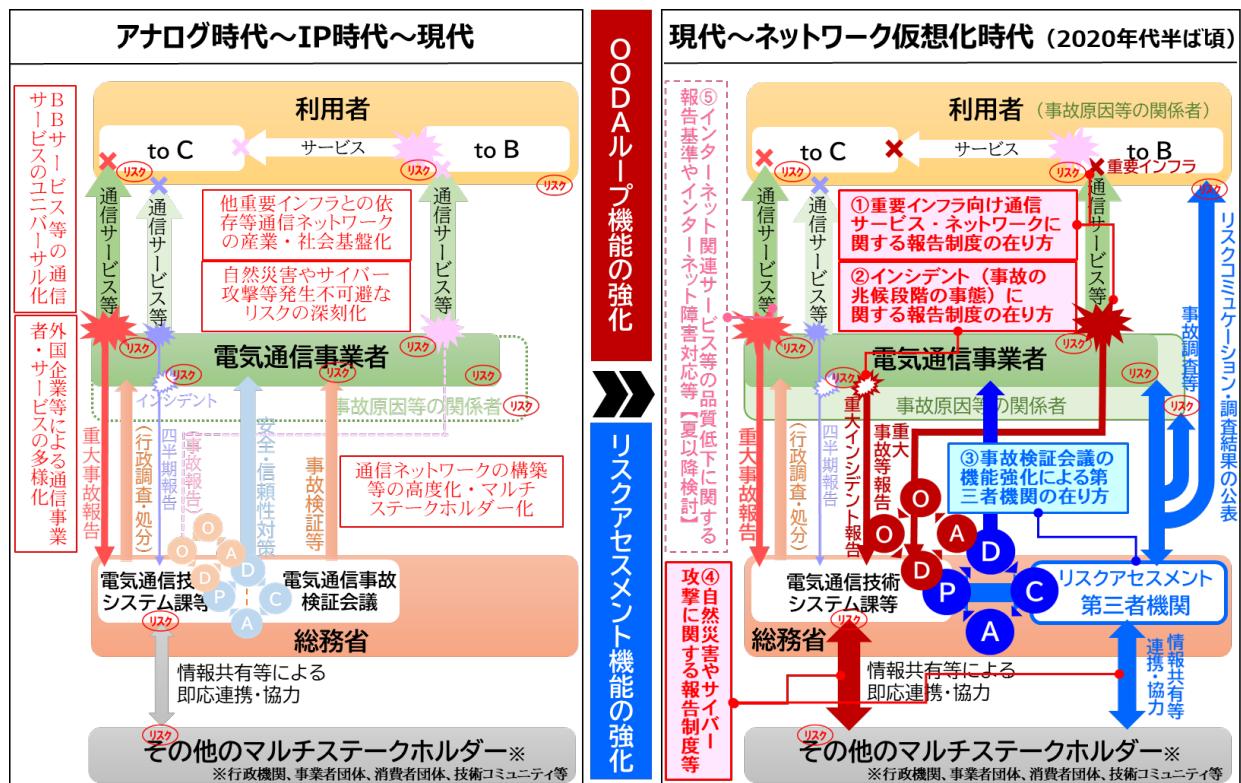


【出典】平成31年4月26日IPネットワーク設備委員会第二次報告概要(「IoTの普及に対応した電気通信設備に係る技術的条件」)を事務局で一部修正

【図 2.1.7】 2020 年代半ば頃における通信サービス・ネットワーク(イメージ)

具体的には、①重大なリスクの Observe(内外環境の観察)及び Orient(方向付け・情勢判断)による OODA ループ機能の強化、②重大なリスクに関するリスクアセスメント機能の強化の観点から、次の点を検討することが必要である。

- 1) BtoB/GtoX(通信事業者to法人利用者/行政機関to一般利用者等。以下同じ。)型の通信サービス・ネットワークのうち、通信分野との相互依存が深まりつつある重要インフラ分野に提供される場合等の通信事故に関する報告制度の在り方
- 2) リスクが顕在化したアクシデントではなく、その兆候段階の事態であるインシデントに関する報告制度の在り方
- 3) 事故調査を通じた演繹的なアプローチ等の電気通信事故検証会議の機能強化による第三者機関の在り方

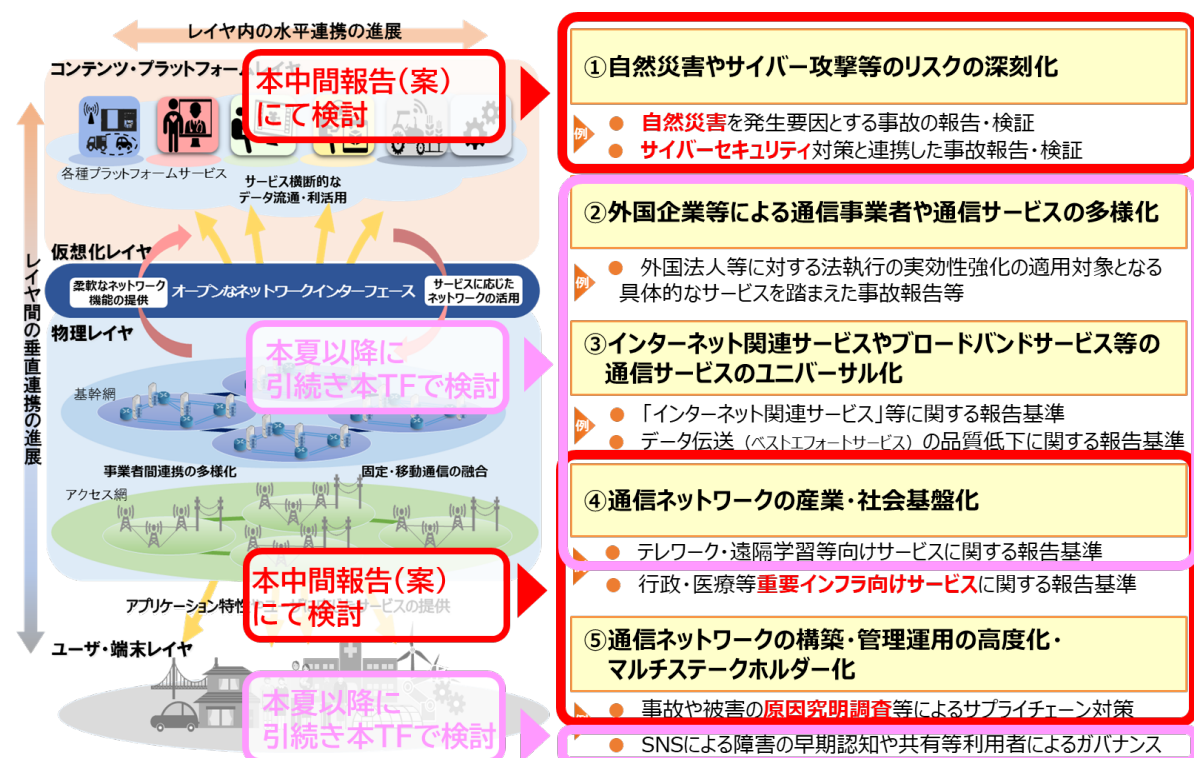


【図 2.1.8】通信事故の報告・検証制度の見直しに関する基本的な方向性

なお、BtoC(通信事業者 to 一般利用者。以下同じ。)型の通信サービス・ネットワークに関する通信事故の報告制度の在り方については、2021年4月より施行された「電気通信事業法及び日本電信電話株式会社等に関する法律の一部を改正する法律」(令和2年法律第30号。以下、「改正電気通信事業法」という。)に基づく外国企業等からの通信事業者等に関する届出等の状況、「ブロードバンド基盤の在り方に関する研究会」(総務省において2020年4月より開催)によるブロードバンドサービスのユニバーサルサービス化や「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ワーキング

グループ」(総務省において 2020 年 12 月より開催)による同サービスの品質計測手法の検討状況等を踏まえつつ、テレワーク・遠隔学習等向けのインターネット関連サービスやデータ伝送サービス(ベストエフォートサービス)の品質低下に関する通信事故の報告基準の在り方や、SNS の活用等によるインターネットにつながりづらい障害への対応の在り方等とともに、本TFにおいて本夏以降に引続き検討することが適当である。

また、通信事故の報告・検証制度の見直しを行うにあたっては、不可抗力である自然災害、意図的なサイバー攻撃やヒューマンエラー等他要因におけるリスクの相違、中小規模事業者を含む通信事業者における報告等の負担や、基本的な価値観を共有する国々等との国際連携の可能性等に配慮することが必要である。



【図 2.1.9】 事故報告・検証制度を取巻く環境・リスクの変化と検討事項

2.2 通信事故の報告制度の見直しの在り方

2.2.1 はじめに

(1) 報告制度の概要

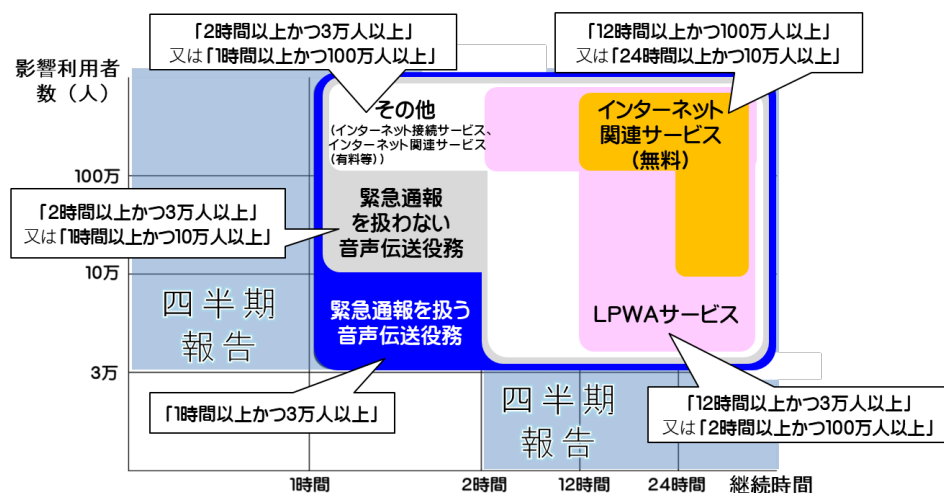
通信事故の報告制度においては、重大事故等の報告を契機として、総務省と通信事業者等との即応連携等の OODA ループ的な対応により、通信サービス・ネットワークの円滑な(確実かつ安定的な)提供の確保と利用者利益の保護を図っている。また、電気通信事故検証会議と相俟って、重大事故等の分析・評価等を通じ、通信事故の事前防止や応急対応等の対策を検証し、再発防止や被害軽減等に向けた施策を充実・改善するために不可欠な安全・信頼性対策に関する PDCA サイクルの要となっている。

「重大事故」報告制度	「四半期報告事故」報告制度
<ul style="list-style-type: none"> ■ 根拠：電気通信事業法第28条 ■ 開始：1985年4月（電気通信事業法の制定・施行）～ ■ 目的：一定規模以上の事故は、社会的影響力が大きいため、速やかに報告させ、迅速な復旧対応を促すとともに、その後の詳細な報告を踏まえ、実態把握・原因分析等を行い、必要に応じ適切な指導、助言、命令等の再発防止のための適切な措置を講ずることが可能。 	<ul style="list-style-type: none"> ■ 根拠：電気通信事業法第166条 ■ 開始：2008年4月～ ■ 目的：「重大事故」に該当しない小規模・短時間の事故の中に、将来の大規模・長時間等の事故に発展する要因を含む事故が内在していると考えられることから、事故発生状況の統計分析等を通じマクロ的に把握し、必要な政策等に適切に反映。

これまでの主な見直し等

- 【2004年4月】重大事故の報告基準：第一/二種区分廃止に伴う事業毎（加入者系、中継系、二種事業者）の基準撤廃、全事業者一律の基準を適用
- 【2008年4月】「品質の低下」の追加：ネットワークIP化に伴う「つながりにくい」というサービスレベルの著しい低下等「品質の低下」を報告対象に追加
- 【2010年4月】報告の効率・迅速化等：重大事故の報告様式整備、四半期報告事故の報告様式における選択式導入、報告不要の軽微な事故の指定等
- 【2010年9月】ガイドラインの策定：報告を要する事故の範囲の目安を定め、通信事業者にとって関係法令を遵守するための指針として、「ガイドライン」を策定
- 【2015年4月】重大事故の報告基準：全事業者（サービス）一律からサービスの重要度に応じた「サービス区分別」の基準への報告基準の見直し、事故報告の第三者検証の仕組みとして「電気通信事故検証会議」の設置等を実施

- 通信事業者において、電気通信事業法^{*}に基づき、総務大臣に対する報告を要する電気通信事故（電気通信設備の故障による電気通信役務の提供の停止又は品質の低下等）は、次の2つに大別。
 - ① 重大な事故：1）サービス毎の影響利用者数・継続時間の基準（下図参照）に該当するもの、又は、
2）重要電気通信設備（衛星・海底ケーブル等）の故障により、全ての通信の疎通が2時間以上不能のもの
（→ 事故後、速やかに一報、30日以内に報告書を提出）
 - ② 四半期報告事故：1）影響利用者数3万人以上又は継続時間2時間以上（電気通信設備以外の設備の故障により電気通信役務の提供に支障を来した事故を含む）、又は、
2）電気通信役務の提供に支障を及ぼす恐れのある電気通信設備に関する情報の漏えい（インシデント）
※電気通信事業法28条・166条、同法施行規則58条、電気通信事業報告規則7条の3
（→ 四半期ごとに報告）



【図 2.2.1】通信事故の報告制度の概要

そして、回線設備設置事業者や有料で利用者 100 万以上のサービスを提供する回線設備非設置事業者等のみならず、無料サービス等を提供する海外事業者等の回線設備非設置事業者も含めた全ての通信事業者(2021 年 4 月現在、約 2 万 2 千者)が対象となっている。

この点、現行の報告制度においては、通信設備の故障による通信サービス・ネットワークの提供停止又は品質低下を対象として、リスクによる影響が顕在化した「アクシデント」、そして、アクシデントの兆候段階の事態である「インシデント」について、同じ「通信事故」として定義し、それらの報告を通信事業者に求めている。

以上のうち、重大なリスクによる影響が顕在化したアクシデントのみが「重大事故」と定義され、総務省と通信事業者等による即応連携等の OODA ループ的な対応の対象となっている。

従って、リスクの量的・質的な変化及びマルチステークホルダーへの拡散に対応するため、OODA ループ機能を強化する観点から、その対象となる重大事故の範囲やインシデントに関する報告の在り方等、報告制度について量的・質的にも見直す必要がある。

(2)「重大事故」の報告制度に関する現状・課題

通信事故の報告制度のうち重大事故については、電気通信事業法の制定・施行(1985年4月)当時より、同法第28条で規定されている¹。これは、通信事業者が、社会経済活動に必要な通信サービスを提供する公共性の高い事業を行っており、その継続的・安定的なサービス提供が求められるため、利用者の利益を保護する必要があるという趣旨である。

以上において、特に、一定規模以上の通信事故については、その社会的影響力が大きいと考えられるため、「重大事故」として速やかに総務省に報告し、迅速な復旧対応を促すとともに、その後の詳細報告を踏まえ、その実態を把握するとともに原因分析等を行い、必要に応じ、事故当事者である通信事業者に対し、適切な指導、助言又は立入調査(同法第166条)や技術基準適合命令(同法第43条)等の行政処分により、再発防止のための適切な措置を講ずることが可能となっている。

また、以上の重大事故の報告をせず、又は虚偽の報告をした通信事業者については、罰則(30万円以下の罰金。同法第188条)の適用対象になり得る。また、重大事故等の通信事故により通信サービスの提供に支障が生じている場合、通信事業者がその支障を除去するために必要な修理その他の措置を速やかに行わないときは、業務改善命令(同法第29条)の対象にもなり得る。

なお、以上により報告された重大事故については、通信事故の当事者である通信事業者の任意の協力により、電気通信事故検証会議で検証されている。この際、通信事故の概要や検証結果等については、同会議の報告書において、「検証は、事故の責任を問うために行うものではない」ことが明記されつつ、公開されている。

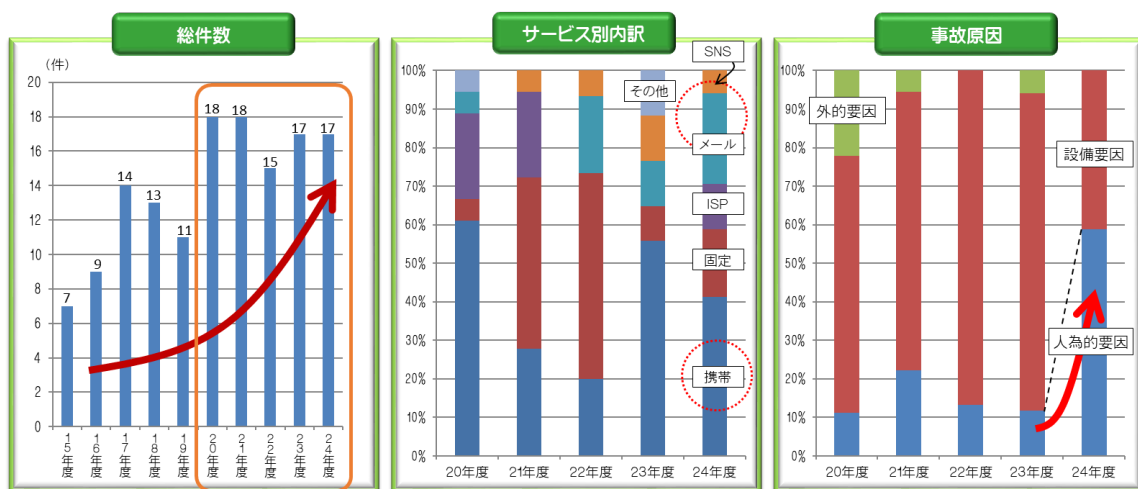
以上の報告対象となる重大事故に該当するか否かの基準について、2014年度までは、電気通信事業法制定時における日本電信電話公社の固定電話を前提とし、通信サービスの種類に関係なく一律で、「影響利用者数3万人以上」かつ「継続時間数2時間以上」とされていた。これは、当時の加入者交換機の平均収容加入者数や故障修理時間等を考慮して設定されたものである。

上記基準による重大事故については、2008年度から2012年度で毎年15件以上の報告が行われている。特に、2013年度は、LTEに係る通信事故等により同年8月時

¹ 電気通信事業法第28条において、「業務の停止等の報告」として、「電気通信事業者は、第八条第二項の規定により電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えいその他総務省令で定める重大な事故が生じたときは、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告しなければならない。」と規定されている。本TFの検討対象である「重大事故」については、以上のうち「その他総務省令で定める重大な事故」であり、「第八条第二項の規定により電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えい」は含まれていない。以下同じ。

点で8件発生するなど、その10年前となる2003年度の年間件数(7件)を超過した。また、2011年度以降、携帯電話関連の通信事故が多発したため、総務省において、2012年より「携帯電話通信障害対策連絡会」を開催し、携帯事業者間で事故原因や対策等の情報共有が実施された。その後、事故発生事業者の多様化等により、2014年、同連絡会を「電気通信事故対策連絡会」に改組し、携帯事業者以外の固定系通信事業者、ISP、ケーブルテレビ及びインターネット関連サービス事業者が新たに参加した。

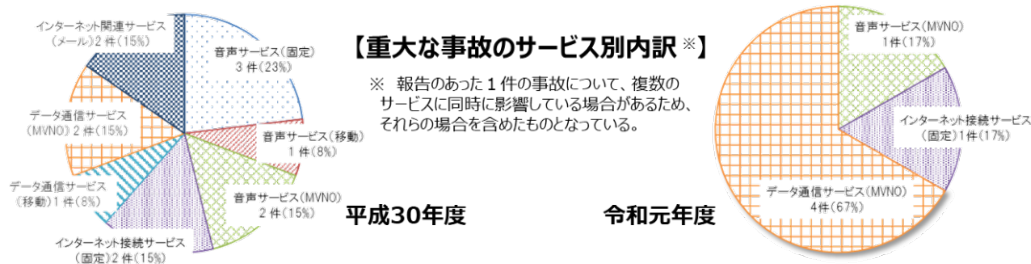
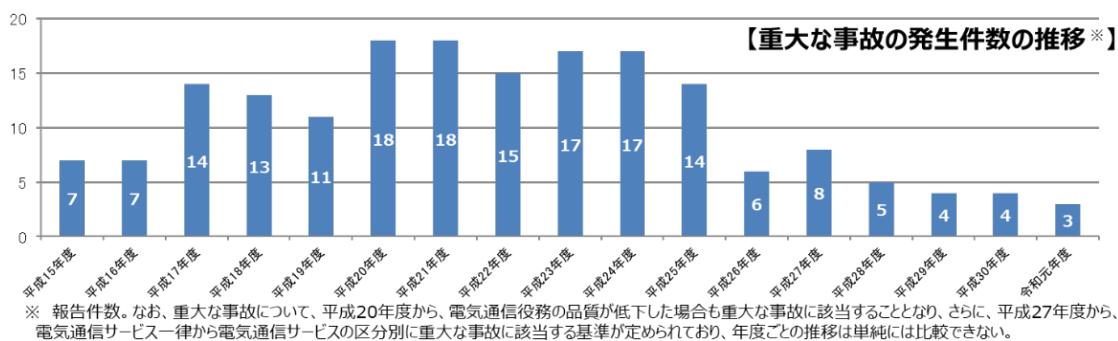
- 総件数について、2011(平成23)年度は17件、2012(平成24)年度も17件の重大事故※が発生。それらを含む5年間の件数は、ほぼ横ばいの状況。
- サービス別内訳について、スマートフォンの急速な普及等に伴い、携帯電話関係の事故割合が大(携帯関係のうち、40%はスマホ利用者のみに影響する事故(2011年度))。また、プラットフォームサービスの進展に伴い、SNS・メール(ポータルサイト事業者等が提供)の事故割合が約30%(2012年度)となり、固定通信より大。
- 事故原因について、従来は設備要因が太宗を占めていたが、2012年度は人為的要因が50%超を占める状況。



【図 2.2.2】 重大事故の発生件数(2008~2012 年度)

その後、2015年度において、通信事業者や通信サービスの多様化・高度化等の進展を踏まえ、通信事故が利用者に与える影響が通信サービスの重要度や社会的影響力に応じて異なり、原因や再発防止策等の検討・報告を義務付ける必要性も異なることから、重大事故に関する基準が通信サービス区分別に改正された。これにより、改正後の基準において、2015年度から2019年度の5年間で平均5件の重大事故が発生している。なお、この改正と併せて、同年度から電気通信事故検証会議が開催されている。

最近では、重大事故について、2019年度に発生したものは3件となり、2015年度以降で最少となっている。また、2020年度は4件となっている。これらについては、回線設備非設置事業者のうちいわゆる届出通信事業者による割合が従来よりも大きくなるとともに、データ通信サービスやクラウド型メールサービスにおけるMVNO等のBtoBtoX(通信事業者to事業利用者to一般利用者等)型のサービスや新たな技術に関するものとなり、国内外の多様な事業者の連携によるサービスという特徴が見られる。

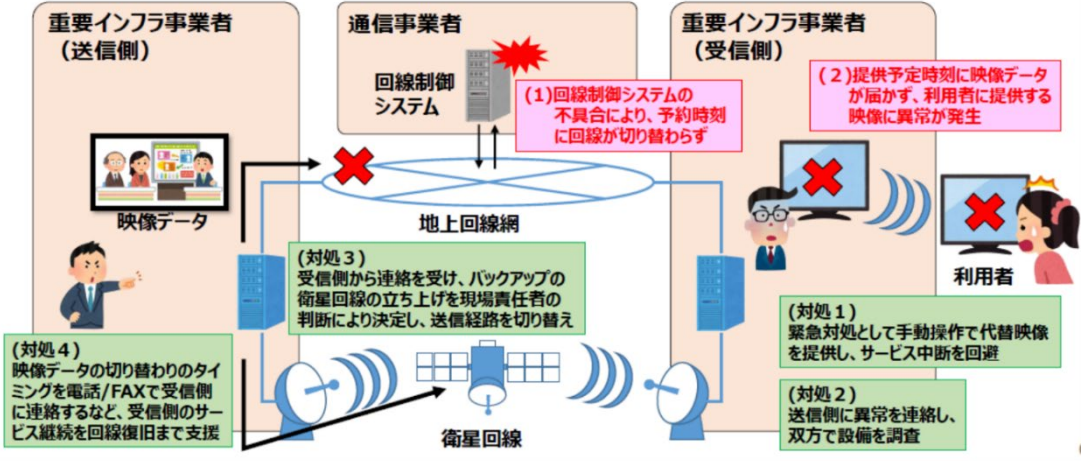


【図 2.2.3】 重大事故の発生件数(2019 年度まで)

この点、BtoB/GtoX 型の通信サービスのうち LPWA サービスについては、1)通信頻度として数時間おきの低頻度で通信を行うものがあること、2)相当数のセンサー端末等を接続するものであること、3)遠隔検針・設備の状態監視・交通監視・環境計測・スマートハウス等の状態監視が主な用途であること等により、個々のセンサー端末等の通信が停止する事態が同サービス利用者に大きな影響を与えるとは考えにくく、また、同サービスの普及に伴いセンサー端末等が膨大な数になっていく中で、アクセス回線毎の管理により同サービス提供事業者側の負担も増え、同サービスの発展性等を阻害する懸念もある。そのため、重大事故か否かに関する基準における影響利用者数については、個々のセンサー端末等へのアクセス回線の数ではなく、基本的には、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数単位でカウントすることとされている。

他方、同じ BtoB/GtoX 型の通信サービス・ネットワークにおいて、通信事業者が他の重要インフラ分野の事業者(放送事業者)に提供する通信サービスの障害により、当該事業者が重要インフラサービスとして提供する予定の映像を予定時刻に送受信できず、その利用者に提供できなくなった事案(2018 年度)があった。これについては、影響利用者数及び継続時間ともに、重大事故及び後述する四半期報告事故に該当せず、通信事故としての報告は行われていない。

- 重要インフラ事業者間で映像データの送受信に使用している回線が、予約日時に切り替わらず、接続障害が発生し、受信側の重要インフラ事業者では予定の映像を利用者に提供できなくなった。
- 回線が切り替わらなかった原因は、回線を提供している通信事業者の回線制御システムの不具合。
- 通信事業者の回線網は冗長化されているため、回線起因の障害は当該重要インフラ事業者では前例が無かったが、「サービス（映像の提供）の継続を最優先に行動」という共通の対応方針の下、衛星回線経由のルートに切り替え、迅速に復旧。



【出典】「重要インフラにおける補完調査について（2018年度）」（2019年4月内閣官房内閣サイバーセキュリティセンター（NISC））
<https://www.nisc.go.jp/conference/cs/ciip/dai18/pdf/18shiryoku06.pdf>

【図 2.2.4】重要インフラ事業者間での映像データ送受信の中断に関する障害

更に、重要インフラ分野の事業者等である地方自治体向けのクラウドサービス(IaaS)の障害について、50 超の地方自治体等における約 450 のシステムに障害が発生し、職員のメール送受信の不可等により地方自治体の事務や住民サービスの提供に影響がでた事案(2019 年度)があった。これは、影響利用者数について重大事故に該当しなかったものの、四半期報告事故として報告されている。

※自治体からの報告及び日本電子計算へのヒアリングベース

- 12月4日（水）に発生した自治体向けIaaSサービスである「Jip-Base」の障害により影響を受けた自治体数は以下のとおり。

	回体数
県	1
市区町村	46
公立図書館	1
一部事務組合	5
計	53 (全 453システム)

- 「Jip-Base」に搭載された各システムの復旧経過は、以下のとおり。

・12/15時点	稼働中（暫定含む）システム数	315/453システム
	データが見つからない割合	15% (OSベース)
・12/18時点	稼働中（暫定含む）システム数	346/453システム
	データが見つからない割合	8% (OSベース)
・1/7 時点	稼働中（暫定含む）システム数	442/453システム
	データが見つからない割合	0.5% (OSベース)
・1/21 時点	稼働中（暫定含む）システム数	450/453システム
	データが見つからない割合	0.5% (OSベース)

- 本事案により自治体事務や住民サービスに下記のような影響があった。

- ・要介護認定の新規認定や更新等ができない。
- ・住民票・印鑑登録証明書など各種証明書の発行ができない。
- ・自治体職員のメールの送受信ができない。
- ・自治体のHPが閲覧不可となる。

【出典】「Jip-Base」事案に係る有識者会議での議論について（総務省自治行政局地域力創造グループ地域情報政策室）（総務省からの地方公共団体向けIaaSサービスの障害事案を踏まえた、クラウドサービスの提供に係る対応要請について）（令和2年6月2日（一社）ASP・SaaS・AI・IoT クラウド産業協会）
<https://www.aspicjapan.org/nintel/pdf/news/200602.pdf>

【図 2.2.5】「Jip-Base」障害の自治体への影響と復旧状況について

(3)「四半期報告事故」の報告制度に関する現状・課題

四半期報告事故については、電気通信事業法第 166 条に基づき、2008 年 4 月より制度化されたものである。重大事故に該当しない小規模・短時間の事故の中には、将来の大規模・長時間等の事故に発展する要因を含む事故が内在していると考えられることから、通信事故の発生状況等の統計分析を通じてマクロ的に把握し、必要な安全・信頼性対策に関する政策等に適切に反映することが目的である。

詳細様式によるものと簡易様式によるものの2種類がある。なお、以上の報告をせず、又は虚偽の報告をした通信事業者については、罰則(罰金 30 万円以下。同法第 188 条)の対象となる。

まず、詳細様式による報告については、2011 年度の約 9000 件をピークに減少し、2019 年度は約 6300 件となり、近年は安定的に推移している。

【令和元年度に報告された電気通信事故】

(括弧内は前年度(平成30年度)の数値)

	報告事業者数	報告件数
重大な事故	5社※1 (6社※1)	3件 (4件)
四半期報告事故		
詳細な様式による報告※3	111社 (132社)	6,301件※2 (6,180件※2)
簡易な様式による報告※4	24社 (27社)	58,211件 (62,240件)

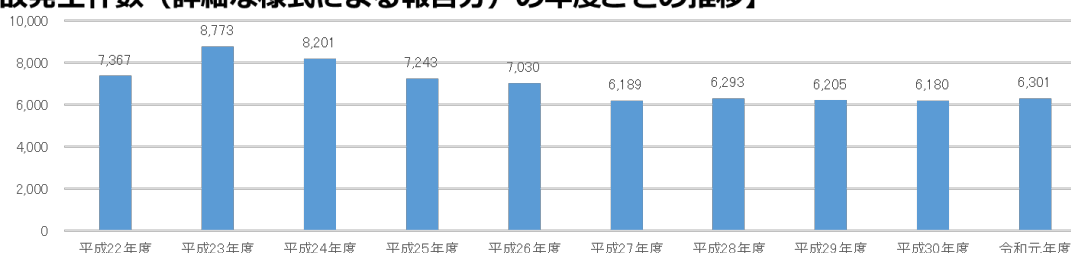
※1 卸役務に関する事故については、報告事業者数として卸提供元事業者及び卸提供先事業者の両方が含まれているため、報告事業者数が報告件数よりも多くなっている。

※2 卸役務に関する事故については、当該事故における卸提供元事業者及び卸提供先事業者の両方からの報告件数が含まれている。

※3 重大な事故については、施行規則様式第50の3に加え、電気通信事業報告規則様式第27により報告することとされているため、詳細な様式による報告に含まれている。

※4 ①無線基地局、②局設置遠隔収容装置又はき線点遠隔収容装置及び③デジタル加入者回線アクセス多重化装置の故障による事故については、簡易な様式による報告が認められている。

【事故発生件数(詳細な様式による報告分)の年度ごとの推移】※5



※5 四半期報告事故について、平成22年度より、報告内容の統一化・明確化等を図るため、新たな詳細な様式への変更等が行われている。また、重大な事故について、電気通信サービスの多様化・高度化・複雑化等に伴い、それまでのサービス一律の報告基準(影響利用者数3万以上かつ継続時間2時間以上)から見直しが行われ、平成27年度からはサービス区分別の基準に基づき報告が行われている。

【図 2.2.6】通信事故の報告件数(令和元年度)

同報告においては、次の事故(アクシデント)及び事故の兆候段階の事態(インシデント)が対象となっている。

- 1) 電気通信設備の故障による通信サービスの提供停止又は品質低下
- 2) 通信サービスに直接的な影響はないが、利用者に大きな影響を及ぼす電気通信設備以外の設備(利用者登録システム、工事関連システムや社内の業務管理用シ

ステム等)の故障により通信サービスの提供に支障を来した事故

- 3) 利用者に影響が及んでないが、電気通信設備に関する情報(電気通信設備であるサーバのログイン ID やパスワード等)の漏えいにより通信サービスの提供に支障を及ぼすおそれがある事態(インシデント)

近年、以上について、上記 1)としては、前述した大規模・長時間の障害となった地方自治体向けクラウドサービス(IaaS)の事故(2019 年 12 月発生)、上記2)として、顧客管理システムや工事関連システムの障害による通信サービスの提供に支障を来した事故(2021 年 5 月公表等)、上記3)として、サイバー攻撃を起因とした電気通信設備に関する情報の漏えいの可能性のある事案(2020 年 5 月公表等)など、将来の大規模・長時間等の事故に発展する要因を含むものが含まれている。

この点、詳細様式における報告内容について、例えば、影響利用者数に重要インフラ事業者が含まれているかどうか、電気通信設備に関する情報の漏えいの原因としてサイバー攻撃によるものか否かや、大規模自然災害を原因とする通信事故について気象庁が名称を定める顕著な災害を起こした自然現象(例えば、「令和元年房総半島台風」等)と関係するものか否かなど、通信事故の発生状況等の統計分析を通じたマクロ的な把握により、必要な政策等を検討するにあたっての報告事項が不明確となってきている。

次に、簡易様式による報告については、次の電気通信設備の故障による事故(アクシデント)及び事故の兆候段階の事態(インシデント)が対象となっている。これらは、当該設備の故障による利用者への影響が全体には及ばず、他の利用者に対する通信サービスの提供は継続可能であることから、通信事故の発生件数のみの簡易な報告とされ、近年は 6 万件前後で推移している。

- 1) 移動通信における無線基地局(携帯電話基地局等)
- 2) リモートターミナル(局設置遠隔収容装置又はき線点遠隔収容装置)
- 3) DSLAM(デジタル加入者回線アクセス多重化装置)

なお、以上のうち、上記1)の携帯電話基地局の故障については、隣接局による応急的なエリア補完により通信サービスの提供が継続され、利用者に直接的な影響が及んでいないインシデントが発生した場合も対象となっている。なお、一部の携帯事業者においては、利用者に直接的な影響が発生したものの件数だけを報告している場合もある。

(4)報告不要な「軽微事故」

四半期報告事故のうち、重大事故における影響利用者数に関する基準に達する恐れはない機器等設備の故障による事故については、「軽微な事故として総務大臣が別に告示するもの」として、通信事故の報告制度の対象外とされている。

具体的には、利用者の建築物又はこれに類するところに設置する事業用電気通信設備である次のものが対象外とされている。

- 1) 利用者宅内に設置されているターミナルアダプタ、モデムやセットトップボックス等の機器の故障
- 2) 端末系伝送路設備(移動通信における無線基地局等を除く)の故障のうち当該故障の箇所が架空線路の区間であるものとして、電線、電柱、引込線(マンション等の集合住宅への引込線を含む)及び保安器等の加入者系事業者のアクセス回線部分の故障

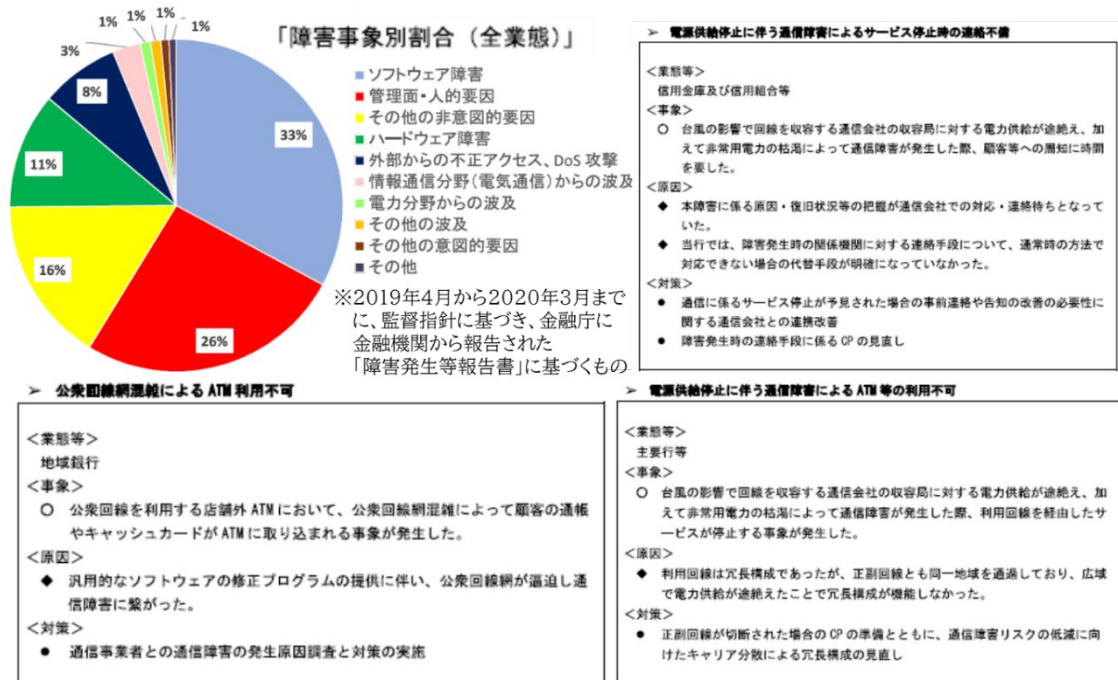
以上は、主に固定通信事業者が設置する電気通信設備であり、これらの故障による通信事故の報告件数は非常に多く、現在でも一日あたり数百件以上のペースで発生している。他方、加入者が限定され、ほとんどが収容者数 500 人未満となっている。また、加入者の周辺に位置している設備であるため、通信事業者等の保守者が常駐しておらず、通信サービスが停止した際の修復に移動時間が必要とされ、2 時間以上かかることが多いという実態がある。更に、故障の要因として、自然故障や厳しい風雪の影響による障害等も多く、通信事業者としても、費用対効果の観点から、機器や系統の多重化等以上の対策をとることが困難となっている。

2.2.2 重要インフラ分野に提供される通信サービス・ネットワークに関する報告制度の在り方

(1)現状・課題

現行の通信事故の報告制度においては、主に BtoC 型の通信サービス・ネットワークに関する重要度や社会的影響力に応じた基準が明確化されているが、BtoB/GtoX 型の通信サービス・ネットワークの通信事故に関する基準は十分に明確化されていない。

以上において、例えば、前述した地方自治体や放送事業者におけるサービス障害の他、金融庁の「金融機関のシステム障害に関する分析レポート」において紹介されている「情報通信分野(電気通信)からの波及」による金融システム障害等、重要インフラ分野に影響を及ぼす通信事故が発生している。



【図 2.2.7】 情報通信分野(電気通信)からの波及による金融システム障害の例
(出典:「金融機関のシステム障害に関する分析レポート」(2020年6月金融庁))

また、重要インフラ分野の中でも、他分野からの依存度が高く、かつ、比較的短時間の障害であってもその影響が大きくなるおそれのある通信分野においては、近年、通信サービス・ネットワークの提供にあたり、「クラウドサービス」²が利用されている。

この点、クラウドサービスについては、その普及に伴い、様々な分野において依存関

² 「事業者によって定義されたインターフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの」(「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(2018年6月各府省情報化統括責任者(CIO)連絡会議決定))をいう。以下、同じ。

係が深まっており、サービス等の責任主体が最終的な利用者から見えづらくなっているという指摘もある中、前述した地方自治体向けのクラウドサービス(IaaS)における通信事故の他、クラウドサービスの障害により、事業利用者や行政機関によるサービスの提供に影響を及ぼす事案が近年頻発している。

「AWSの東京リージョンで障害、気象庁のHPが一時閲覧できず」

(日経クロステック 2021年2月20日より以下抜粋)
米アマゾン・ウェブ・サービス (Amazon Web Services、AWS) が提供するクラウドサービスの東京リージョンでシステム障害が発生していることが2021年2月20日に分かった。
気象庁ではホームページが一時閲覧できなくなった。今回のAWSの障害が原因とみられる。バックアップサイトに切り替えたが、警報などの防災情報コンテンツを正しく表示できない状況が続いている。

「Google大規模障害 一時メールなど使えず」

(日本経済新聞 2020年12月14日より以下抜粋)
米Googleのメールなどのサービスが14日、世界の幅広い地域で一時接続できなくなった。
Googleのサービスは大企業も含め、数十億人が利用しており、一企業のシステムトラブルが世界に混乱を招くリスクも浮き彫りにした。
Googleのメールサービスの利用者は20億人に上る。個人の利用だけでなく、Googleのサーバーを利用してサービスを展開する大企業も多い。

「日本電子計算の自治体クラウドで障害、アップデート中に「想定外の事象が発生」

(日経クロステック 2020年6月1日より以下抜粋)
日本電子計算 (JIP) は2020年6月1日、同社が提供する自治体向けIaaS「Jip-Base」で5月31日未明からシステム障害が発生していたと日経クロステックの取材に対して明らかにした。
Jip-Baseは2019年12月にストレージ機器のファームウェアの不具合が原因となって、50自治体のシステムが一斉にダウンして住民票が発行できなくなり、データの一部を消失するというトラブルが発生した。

「Microsoft「Office365」連日の障害 通信設定に問題」

(日本経済新聞 2019年11月20日より以下抜粋)
クラウドで業務用ソフトを使う米マイクロソフトの「オフィス365」で20日、メールシステムやチャットなどの複数のサービスがつながりにくくなる障害が発生した。同社は利用者の通信が停滞する要因となったとみられる通信設定を特定し、改善したとするが、根本原因は調査中という。同社は公式ツイッターで現段階では復旧したとしている。

【図 2.2.8】 最近のクラウドサービスの障害の例

(出典:「デジタル参照に関する現状と課題」(2021年5月経済産業省))

そして、BtoB/GtoX 型の通信サービス・ネットワークの通信事故として、重要インフラ分野事業者である通信事業者が、外国法人が提供するクラウドサービスを利用して国内に通信サービスを提供するにあたり、当該クラウドサービスの障害が原因となり当該通信サービスの通信事故が発生した事案(2019年度)も発生している。

このような中、令和3年4月の改正電気通信事業法の施行により、外国法人等(外国の法人及び団体並びに外国に住所を有する個人をいう。以下同じ。)が、日本国内にある者に対して電気通信事業を営む場合における電気通信事業法の法執行の実効性が強化されたところ、現行の通信事故の報告制度においては、登録又は届出を要するクラウドサービスの障害が通信事故に該当する場合に関する基準や考え方が明確化されていないところである。

従って、リスクの量的・質的な変化及びマルチステークホルダーへの拡散に対し、OODA ループ機能を強化する観点から、重大事故の範囲やインシデント等、速やかな報告の対象を見直し、BtoB/GtoX 型の通信サービス・ネットワークの中でも、通信分野との相互依存が深まっており、特に重大なリスクと考えられる重要インフラ分野に提供される通信サービス・ネットワークの通信事故やクラウドサービス障害による通信事故について、その基準や考え方を整備することが喫緊の課題となっている。

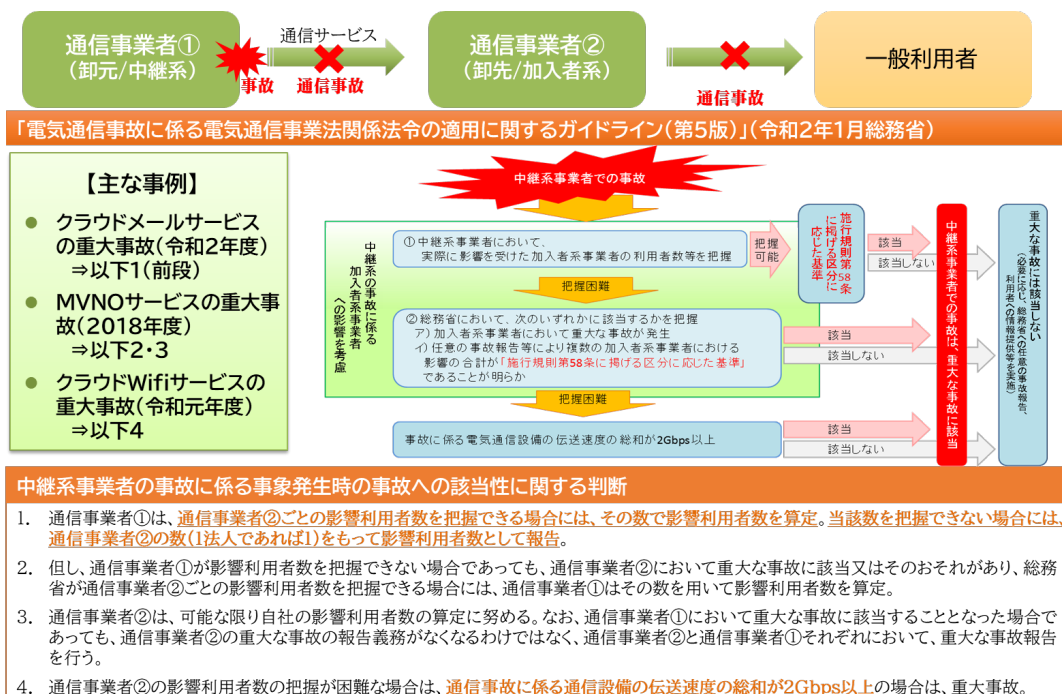
(2)「電気通信事故に係る電気通信事業法関係法令の適用に関するガイドライン」における整理

現行の報告制度において、通信事故による社会的な影響の把握に関する考え方としては、通信事故の継続時間とともに、当該事故による影響を受けた利用者全体(事業利用者及び一般利用者等)を「影響利用者数」として算定している。

以上のうち影響利用者数に関する考え方については、通信事業者による通信サービス・ネットワークの直接の提供先となる事業利用者が重要インフラ分野における事業者(以下、「重要インフラ分野事業者」という。)である場合、又は、当該重要インフラ分野事業者が一般利用者等に対して重要インフラサービス等を提供する場合において、「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)」(令和2年1月総務省。以下、「事故GL」という。)³等により、次の整理となっている。

- 1) 通信事業者(卸元・中継系等)の通信サービス・ネットワークの提供先となる事業利用者たる重要インフラ分野事業者が通信事業者(卸先・加入系等)であり、通信事業者(卸元・中継系等)が提供する通信サービス・ネットワークの利用により、当該重要インフラ分野事業者において通信サービスが提供される場合(例えば、MVNO、クラウドメールサービスやクラウド Wi-Fi サービス等。)

⇒ 影響利用者数として、事故GLにおいて「中継系事業者の事故に係る事象発生時の事故への該当性に関する判断」が規定され、基本的には、「toX」である一般利用者等の数を算定。



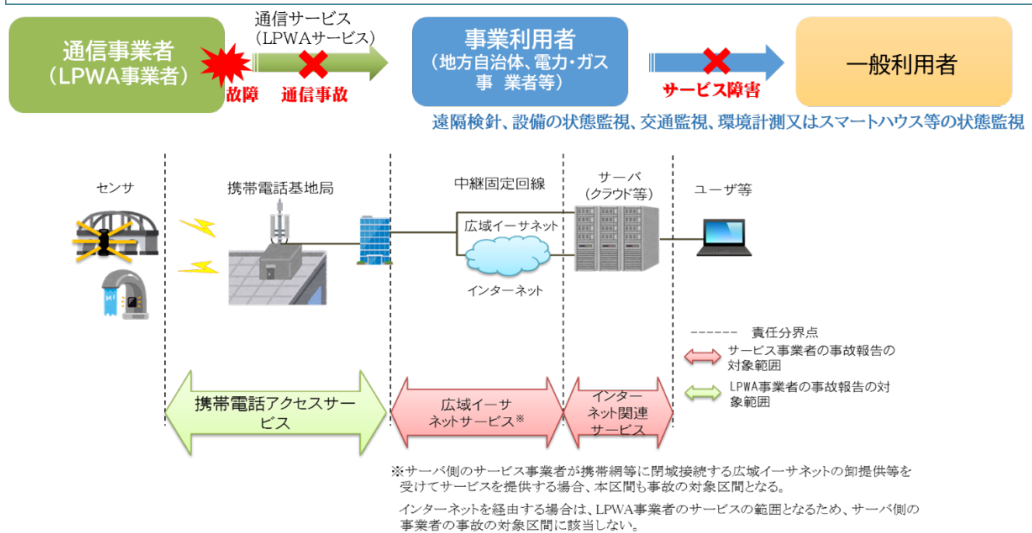
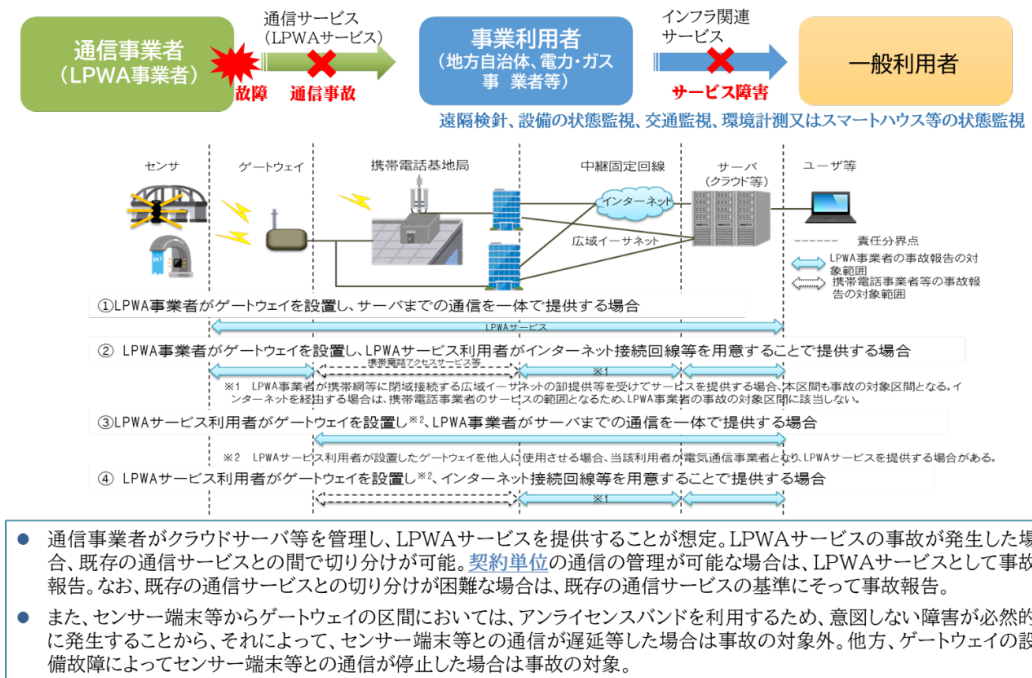
【図 2.2.11】中継系事業者の事故に係る事象発生時の事故への該当性に関する判断

³ 総務省ウェブページ

(https://www.soumu.go.jp/menu/seisaku/ictseisaku/net_anzen/jiko/handan.html) 参照。

2) 通信事業者の通信サービス・ネットワークの提供先となる事業利用者が通信事業者以外の重要インフラ分野事業者(地方自治体、運輸関係事業者や電力・ガス事業者等)であり、当該通信事業者が提供する通信サービス・ネットワークの利用により、当該重要インフラ分野事業者において重要インフラサービス以外の関連サービス(住民の見守り、スマートメータや設備の遠隔検針・状態監視等のサービス)が提供される場合(例えば、LPWA サービス等)

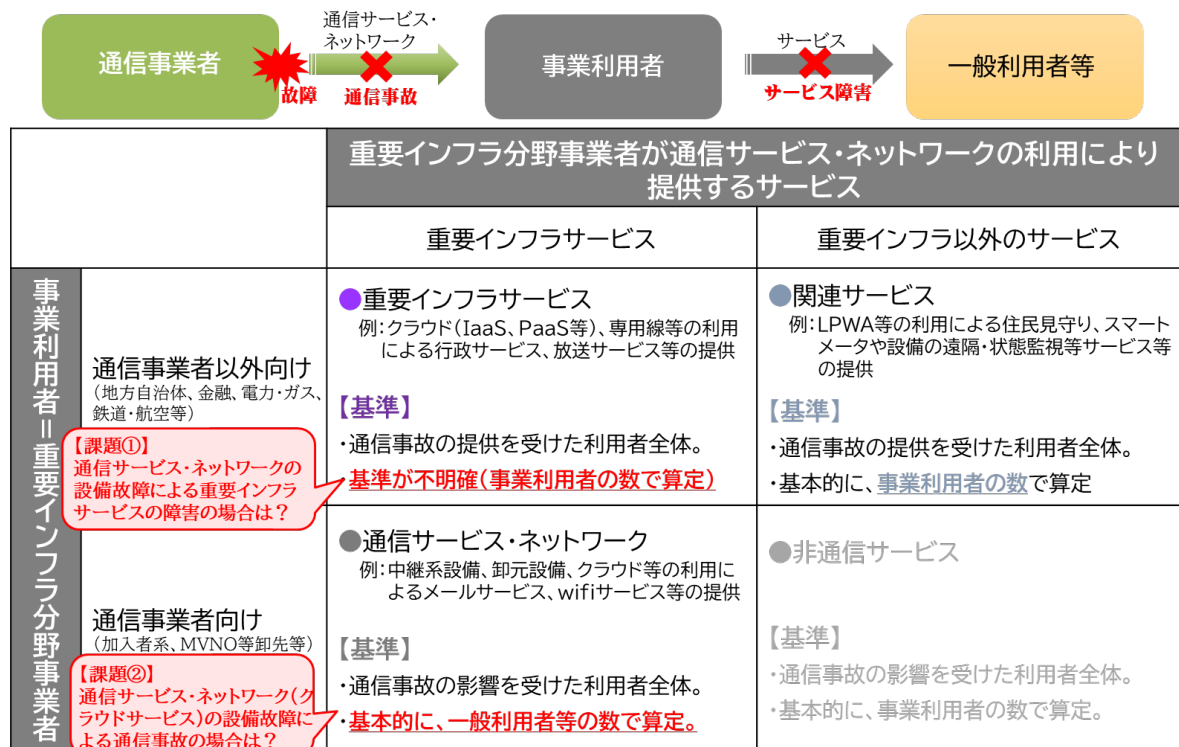
⇒ 影響利用者数として、個々のセンサー等の数と事業利用者への影響が比例しないこと等から、基本的には、「toX」である個々のセンサー数ではなく、同一の目的で利用されるセンサー数を束ねた契約単位の数で算定。



- 通信事業者は、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。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、既存の通信サービス(携帯電話アクセスサービス)の基準に沿って事故報告。
- LPWAサービスの事故が発生した場合において、既存の通信サービス(携帯電話アクセスサービス)との間で切り分けが可能な場合であって、契約単位で通信の管理が可能な場合は、LPWAサービスとしての事故報告

【図 2.2.12】 LPWA サービス(アンライセンス系・セルラー系)の通信事故における影響利用者数

- 3) 通信事業者の通信サービス・ネットワーク(例えば、専用役務、IP-VPN サービスや 5G サービス等)の提供先となる事業利用者が通信事業者以外の重要インフラ分野事業者であり、当該通信事業者が提供する通信サービス・ネットワークの利用により、当該重要インフラ分野事業者において重要インフラサービスが提供される場合(例えば、地方自治体向け IaaS、放送局向け映像伝送サービス等)
- ⇒ 影響利用者数としては、事故GL等において明確な規定がないことから、事業利用者の数を算定。



【図 2.2.13】重要インフラ分野に提供される通信サービス・ネットワークに関する報告制度の現状と課題

以上のように、通信事故による重要インフラ分野への影響については、影響を受けた利用者全体(事業利用者及び一般利用者等)ではなく、事業利用者数のみで算定されている場合がある。そのため、報告基準に満たずに四半期報告事故又は重大事故としての報告がされない場合や、四半期報告事故として報告されたとしても一般利用者等の数に含まれ事業利用者への影響の有無等が不明となっている場合があると考えられる。

従って、通信事故による重要インフラ分野への影響の有無等の情報が量的・質的に不足しており、総務省において、的確な観察(Observe)や迅速な情勢判断(Orient)等による重大事故に対するOODAループ的な対応や、それも含めた総合的な分析・評価等に基づく再発防止や被害軽減等に向けた PDCA サイクルによる継続的な改善が困難に

なっていると考えられる。ひいては、通信事故による重要インフラ分野への影響等について、関係機関との情報共有不足等により、即応連携や再発防止に向けた連携・協力体制の構築・継続・深化が停滞しているおそれもあると考えられる。

そこで、次の事項について検討が必要である。その際、海外(例えば、欧州)における通信事故の報告制度の動向等にも留意することが必要である。

- 通信サービス・ネットワークの通信事故による、重要インフラサービス障害の場合における通信事故の報告制度の在り方【⇒以下、37～40頁にて検討】
- 通信サービスとしてのクラウドサービスの通信事故による、重要インフラサービス障害のうち通信サービス・ネットワークの通信事故の場合における通信事故の報告制度の在り方【⇒以下、41～43頁にて検討】

- 事故報告制度を規定していた枠組指令について、**欧州電子通信コード(E ECC: European Electronic Communication Code)指令により改正され、2020年12月より施行。**
- 新たな事報告制度においては、**対象となる電気通信ネットワーク/サービスとしてOTTサービスへの拡大やセキュリティインシデントの具体化、「重大な影響」に関する要考慮指標の設定や質的基準等**が追加。

枠組指令 (2002/21/EC) 13a条3項

- ▶ 2009年通信改革パッケージの「Better Regulation指令」(2009/140/EC)により追加。**2011年より施行。**
- ▶ **電気通信ネットワーク/サービス(Electronic communication network/service)**。主に、**固定電話/インターネット接続、移動電話/インターネット接続等**の運用に**重大な影響**を及ぼす**セキュリティインシデント(security breaches及びintegrity losses)**について、通信事業者が規制当局に報告する義務等を規定。なお、**対象となるネットワーク/サービス、重大な影響やセキュリティインシデントの詳細は加盟国が独自に設定。**
- ▶ 上記セキュリティインシデントについて、各加盟国が欧州理事会(EC)と欧州ネットワーク・情報セキュリティ庁(ENISA)に対し、その概要を毎年報告する義務を規定。
- ▶ ENISA等への各年報告につき、**相対基準(継続時間1h超かつ影響利用者が15%超・同2h超かつ同10%超等)又は絶対基準(100万ユーザ時間超)**を設定。なお、当面の間、セキュリティインシデントのうち、**integrity losses(電子通信ネットワーク/サービス提供の継続性に影響を及ぼすoutage)**のみが対象。
- ▶ ENISAにて、2012年以降、**年次報告書**を取りまとめ、**2019年に発生したインシデントについて2020年7月に公表。**

詳細は、ENISA「Technical Guideline on Incident Reporting: Technical guidance on the incident reporting in Article 13a ver. 2.1, October 2014」参照

EECC指令 (2018/1972) 40条2項

- ▶ 枠組指令13a条3項を改正。2020年12月21日より施行。
- ▶ 対象となる電気通信ネットワーク/サービスについて、「**番号に依存しない個人間通信(Number-independent Interpersonal Communications)**」サービスとして、**OTTサービス(WhatsApp、Viber、Slack、Gmail、Outlook、Skype-to-Skype等)**も追加。
- ▶ 対象となる**セキュリティインシデント**につき、電子通信ネットワーク/サービスの**セキュリティ(confidentiality、authenticity、integrity、availability)**に**実際の悪影響を及ぼす事象(2本で冗長化された海底ケーブルのうち1本の切断や新発見の脆弱性等も含む)**と具体化。
- ▶ 対象となる「**重大な影響**」につき、加盟国が特に考慮すべき指標(**影響利用者数、継続時間、地理的範囲、電子通信ネットワーク/サービスの機能への影響の程度、経済社会活動への影響**)を規定。
- ▶ 通信事業者は、規制当局等のセキュリティインシデントに関する**主務官庁**に対し、**不当な遅延なく報告**する旨を規定。
- ▶ ENISA等への年次報告につき、**量的基準**(影響利用者数及び継続時間)のみならず、当該基準に該当しない場合の**新たな質的基準(地理的範囲や、重要サービスや重要分野・事業者の継続性等の社会経済等への影響)**を規定。

詳細は、ENISA「SECURITY SUPERVISION UNDER THE EECC, JANUARY 2020」,「Technical Guideline on Incident Reporting under the EECC, March 2021」参照

- NIS指令(2016/1148)において、①「**デジタルインフラ**」等の「**重要インフラ運営者**」、②「**デジタルサービス提供者**」を対象として、その**サービス提供の継続性に重大な影響を及ぼすインシデント報告制度**が規定。
- 2020年12月の**新たな「サイバーセキュリティ戦略」**にて**NIS2指令案**等公表。**EECC指令の報告制度も含めNIS指令を全面改正。**今後、EU理事会等との調整を経て、採択後18ヶ月以内に加盟国で措置予定。

NIS指令 (2016/1148) 14条・16条

- ▶ 2013年2月の「サイバーセキュリティ戦略」において、NIS指令(Directive on security of network and information systems)が提案。**2018年5月より施行。**
- ▶ **重要インフラ運営者(OES)及びデジタルサービス提供者(DSP)**は、**主務官庁やCSIRT**に対し、**不当な遅延なく報告**する義務等を規定。
- ▶ **OES**として、エネルギー、交通、金融、医療、水道、**デジタルインフラ**の7分野を規定。うち、デジタルインフラにつき、**IXP、DNSサービスプロバイダ、TLD名前レジストリ**を規定。
- ▶ **DSP**として、**オンライン市場、オンライン検索エンジン、クラウドサービス**を規定。なお、**零細企業等は対象外。**
- ▶ 対象となる「**重大な影響**」につき、加盟国が特に考慮すべき指標として、**影響利用者数、継続時間及び地理的範囲**を共通に規定。
- ▶ **DSP**については、次も規定。
 - ・「**重大な影響**」の要考慮指標として、**提供サービスの機能への影響及び経済社会活動への影響**も追加。
 - ・「**重大な影響**」のみなし規定(①提供するサービスが500万ユーザ時間超の利用不可、②提供するサービスやデータのCIAの侵害が10万ユーザ時間超、③公共の安全や人命損失等の危険等)
- ▶ **OES**がそのサービス提供にあたり**第三者のDSPに依存する場合**、当該DSPに影響及ぼすインシデントによる重要インフラサービスの継続への**重大な影響**全てについて、**OES**が報告する義務を規定。

詳細は、「Commission Implementing Regulation (EU) 2018/151」参照

NIS2指令案20条

- ▶ OESとDSPの区分を見直し、重要性等に応じ異なる規制枠組みが適用される「**不可欠主体(EE: essential entities)**」と「**重要主体(IE: important entities)**」に見直し。重要インフラの対象を拡大。
- ▶ **EE**として、「**デジタルインフラ**」が規定。NIS指令のOESとしてのデジタルインフラ(**IXP、DNSサービスプロバイダ、TLD名前レジストリ**)、EECC指令の**電気通信ネットワーク/サービス**に加え、新たに、**データセンターサービス、CDN、トラストサービス**、NIS指令のDSPの1つである**クラウドサービス**が対象。
- ▶ **IE**として、「**デジタル提供者**」が規定。NIS指令の**DSP(オンライン市場、オンライン検索)**に加え、新たに、**SNSプラットフォーム**が対象。
- ▶ EE及びIEは、主務官庁やCSIRTに対し、**サービス提供に重大な影響を及ぼすいかなるインシデントを不当な遅延なく報告**する義務(24h以内の速報、求めで中間報告、30日以内の最終報告)を規定。
- ▶ EE及びIEは、主務官庁やCSIRTに対し、**重大なインシデントをもたらす可能性がある**と確認されるいかなる**重大なサイバー脅威を不当な遅延なく報告**する義務を規定。
- ▶ 「**重大**」につき、**当該主体に相当な運用上の混乱又は金銭的損失をもたらす(恐れも)がある場合、相当な物質的又は非物質的な損失により他の自然人・法人に影響を及ぼす(恐れも)がある場合**と規定。
- ▶ 上記インシデント及び**サイバー脅威**等について、各加盟国がENISAに対し、その**概要を毎月報告**する義務を規定。

【図 2.2.14】欧州における通信事故等の報告制度

(3)通信サービス・ネットワークの通信事故による、重要インフラサービス障害の場合における通信事故の報告制度の在り方

①考え方

BtoB/GtoX 型の通信サービス・ネットワークのうち、その提供先となる事業利用者が通信事業者以外の重要インフラ分野事業者であり、かつ、当該重要インフラ分野事業者が一般利用者等に対して重要インフラサービスを提供する場合には、影響利用者数の算定に関する基準や考え方が明確化されていない。

そのため、通信事故を原因とする、重要インフラ分野事業者における重要インフラサービス障害については、現行の報告基準に満たず重大事故や四半期報告事故として報告されない場合や、報告された場合であっても影響利用者数として一般利用者等の数に含まれている場合など、重要インフラ分野に対する通信事故による影響の有無等が「見える化」されていない。

従って、まずは、重要インフラサービス障害により影響を受けた一般利用者等の数が把握可能か否かにかかわらず、通信事故による重要インフラサービス障害の状況を「見える化」するため、少なくとも通信事故の影響を受けた重要インフラ分野事業者の数について、四半期報告事故として報告することが必要と考えられる。

この点、四半期報告事故の場合において、通信事故の影響を受けた重要インフラ分野事業者の数のみならず、通信事故による重要インフラサービス障害の影響を受けた一般利用者等の数も把握可能な場合には、当該数も含めた影響利用者全体の数を報告するという考え方もある。

確かに、通信サービス・ネットワークの産業・社会基盤化等が進展する中、重要インフラ分野事業者が通信サービス・ネットワークを利用して重要インフラサービスを一般利用者等に提供する場合については、それ以外の関連サービスに利用されている LPWA サービスと異なり、通信事故による重要インフラサービス障害が影響は大きいと考えられるため、重要インフラ分野事業者の数のみで算定することは適当ではない。

しかしながら、通信サービス・ネットワークの提供先である重要インフラ分野事業者が通信事業者である場合と異なり、重要インフラサービス障害の影響を受けた一般利用者等の数については、たとえ重要インフラ分野事業者から通信事業者に対して情報共有等がされた場合においても、当該数と当該重要インフラサービス障害による社会的な影響との関係を当該通信事業者が判断等することは困難と考えられる。また、重要インフラ分野事業者に提供される通信サービス・ネットワークが IP-VPN 等の場合、当該重要インフラ分野事業者が当該通信サービス等の利用により重要インフラサービスを提供して

いるか否かについて、通信事業者が把握することが困難という事情もある。

他方で、地方自治体向けのクラウドサービス障害や放送事業者向け映像伝送サービス障害など、通信事故が原因となって重要インフラサービス障害が発生し、その社会的な影響が大きいにもかかわらず、重要インフラ分野事業者の数のみで算定されることにより、重大事故として総務省への速やかな報告が行われなくなることは避ける必要がある。

そこで、重要インフラサービス障害が発生又はその被害が拡大している場合等において、通信事故がその原因であると考えられる場合については、速やかな総務省への報告が円滑かつ公平に行われるようにするため、重要インフラサービス障害の影響を受けた一般利用者等の数とは異なる基準や考え方を明確化することが必要である。

なお、以上の対象となる重要インフラ分野事業者としては、例えば、次の事業者等が考えられる。

1) 「重要社会基盤事業者(サイバーセキュリティ基本法)」等

- 「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者」(サイバーセキュリティ基本法第3条)
- 情報通信、金融、航空、鉄道、電力、政府・行政サービス(地方自治体を含む)、医療等の14分野
- 「重要社会基盤事業者」の事業に類するものとして、農業、林業、漁業、建設業、鉄鋼業、郵便業及び警備業が規定(特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律)

2) 「指定公共機関」

- 自然災害、新型インフルエンザや武力攻撃事態等について、関係機関と相互に連携協力し、対策の的確かつ迅速な実施等の予防・応急・復旧段階で重要な役割を果たす機関
- 災害対策基本法、新型インフルエンザ等対策特別措置法又は武力攻撃事態等対処法(武力攻撃事態等及び存立危機事態における我が国の平和と独立並びに国及び国民の安全の確保に関する法律)に基づき指定

②対応の方向性

まず、重要インフラ分野に提供される通信サービス・ネットワークの通信事故について、「見える化」し、的確な観察(Observe)や、リスクの総合的な分析・評価等を可能とするPDCAサイクルを構築するため、総務省においては、四半期報告事故の報告制度につい

て、所要の制度改正を行うことが適当である。

具体的には、通信事業者において、四半期報告事故が発生した際、当該事故による重要インフラサービス障害の発生の有無にかかわらず、当該事故による直接の影響を受けた事業利用者に重要インフラ分野事業者が含まれる場合は、当該重要インフラ分野事業者の数を報告することとすることが適当である。

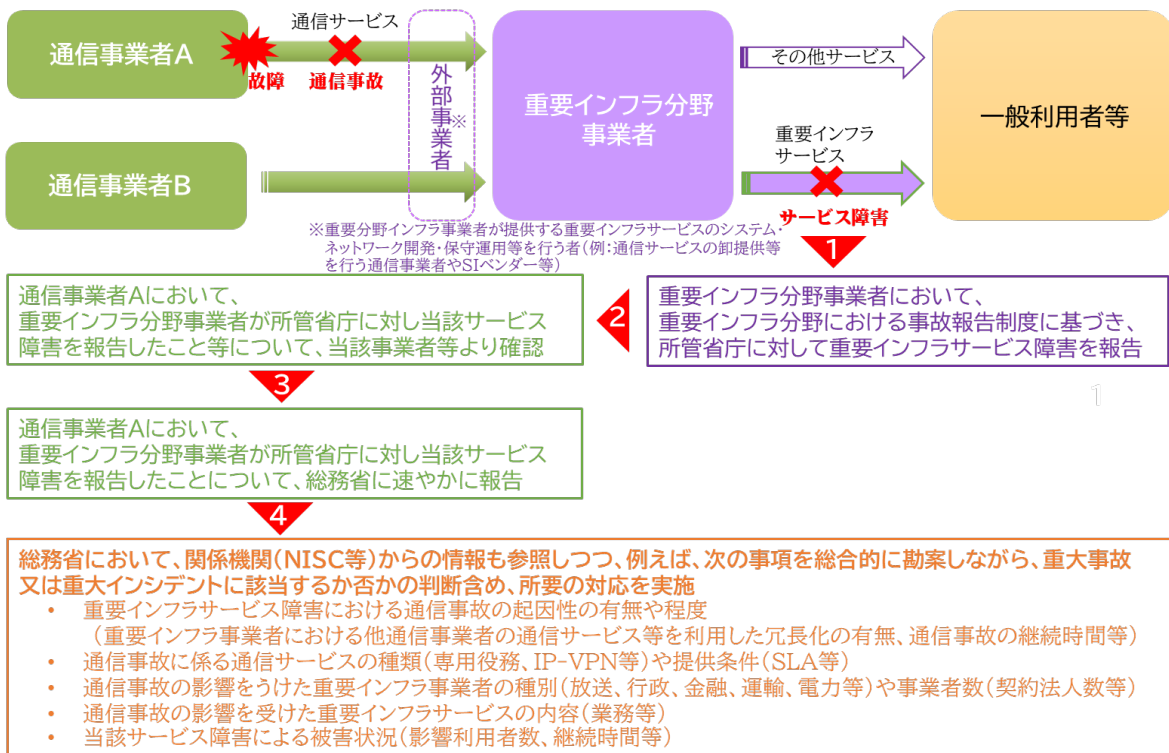
また、以上の対象となる通信事業者以外の重要インフラ分野事業者の範囲について、総務省においては、事故 GL 等により明確化することが適当である。

次に、上記のうち重要インフラサービス障害が発生した場合については、総務省への速やかな報告が行われ、重要インフラに提供される通信サービス・ネットワークの通信事故に関する的確な観察や迅速な情勢判断等によるOODAループ的な対応を可能とするため、総務省においては、所要の制度改正を行うことが適当である。

具体的には、次の考え方によることとし、今後、総務省において、具体的な報告事例を積み重ねつつ、通信事業者における報告にあたっての予見可能性や公平性を確保する観点から、事故GL等により判断基準の具体化・明確化を図っていくことが必要である。

- 1) 通信事故の報告制度と同様、他の重要インフラ分野においても、利用者利益の保護のため、各業法に基づく重要インフラサービス障害又はその兆候に関する報告制度がある。そこで、当該制度等に基づき重要インフラ分野事業者が当該障害等を所管省庁に報告した場合において、通信事業者が、当該重要分野インフラ事業者やその重要インフラサービスのシステム・ネットワーク開発・保守運用等に関する外部事業者等との間で、次の点がいずれも確認できる場合には、総務省に対して速やかに報告を行う。
 - 重要インフラ分野事業者が所管省庁に対して重要インフラサービス障害等を報告したこと、又は、その報告の必要があること
 - 当該サービス障害の原因が自らの通信事故に関係すること
- 2) 上記1)による報告を受けた後、総務省において、関係機関(NISC 等)からの情報も参照しつつ、次の点を総合的に確認・勘案しながら、重大事故又は後述する重大インシデントに該当するか否かの判断含め、所要の対応を行う。
 - 重要インフラサービス障害における通信事故の起因性の有無や程度(重要インフラ分野事業者における他通信事業者の通信サービス・ネットワークを利用した冗長化の有無、通信事故の継続時間等)
 - 通信事故に係る通信サービス・ネットワークの種類(専用役務、IP-VPN 等)や提供条件(SLA 等)

- 通信事故の影響を受けた重要インフラ分野事業者の種別(放送、行政、金融、運輸、電力等)や数(契約法人数等)
- 通信事故の影響を受けた重要インフラサービスの内容(業務等)
- 重要インフラサービス障害による一般利用者等への被害状況(影響利用者数、重要インフラサービス障害の継続時間等)



【図 2.2.15】 重要インフラ分野に提供される通信サービス・ネットワークの通信事故における報告にあたっての考え方

(4)通信サービスとしてのクラウドサービスの通信事故による、重要インフラサービス障害のうち通信サービス・ネットワークの通信事故の場合における通信事故の報告制度の在り方

①考え方

重要インフラ分野事業者である通信事業者が、クラウドサービス事業者が提供するクラウドサービス(SaaS、PaaS、IaaS 等)における他人の通信を媒介するサービスが提供可能となる機能(以下、単に「通信媒介機能」という。)を利用することにより、通信サービスを提供する場合についても基準や考え方を明確化する必要がある。

以上の場合について、当該クラウドサービス事業者は、提供するクラウドサービスのうち通信媒介機能に係る範囲において、自らが通信事業者として、当該重要インフラ分野事業者(である通信事業者)に対し、当該クラウドサービスを通信サービスとして提供していることになる場合がある。

そのため、当該クラウドサービスにおける設備故障が原因となり、その提供先である通信事業者において通信事故が発生した場合について、基本的には、当該クラウドサービス事業者は通信事業者として、上記範囲において、当該クラウドサービスのうち通信サービスに関する通信事故として報告制度の対象になると考えられる。

他方、クラウドサービスにおいては、それが構築・管理運用するデータセンタを仮想化技術により連携させつつ、多数の機能やサービス等が提供されている。そして、当該機能やサービス等の提供を受ける通信事業者等のクラウドサービス利用者においては、災害対策等のため、単一障害点を回避する設計に基づく運用として、当該クラウドサービス利用者自らが取捨選択して利用する当該機能やサービス等について、単一又は複数のデータセンタ、さらには複数のリージョンで仮想的に構築することが可能となっている。

従って、設備故障によりクラウドサービスとして提供する機能やサービス等の提供停止等が発生した場合、クラウドサービス事業者においては、クラウドサービス利用者が当該機能やサービス等の利用により提供する通信サービス等の支障の有無等を把握することが困難な状況にある。そのため、クラウドサービス事業者においては、当該クラウドサービス利用者以外も含め誰でもクラウドサービスの運用や障害状況を確認することができるステータスレポートをウェブ上で提供することや、重大な障害がクラウドサービス側で発生した場合には当該クラウドサービス利用者に対して原因分析等の文書を提供すること等により、提供する機能やサービス等の状況の可視化が行われている。

クラウドサービスについては、それが通信サービスとして提供されるか否かにかかわらず、サイバー空間における重要な基盤となりつつある。クラウドサービスの障害による影響は広範かつ複雑化し、その事業利用者のみならず、当該利用者が提供するサービスの一般利用者等にも影響がもたらされるとともに、多くの事業利用者において同時多発的に当該障害の影響が発生する場合もある。

そのため、クラウドサービスについては、その障害による利用者全体に及ぼす影響の大きさを踏まえると、提供するクラウドサービスのうち通信媒介機能に係る範囲において当該障害が通信事故に該当する場合、その直接的な影響を受けた通信事業者の数のみで算定することは適当ではないと考えられる。

従って、クラウドサービスに関する通信事業者間に跨がる通信事故の報告制度の在り方については、重大事故又は後述する重大インシデントとして総務省への速やかな報告が円滑かつ公平に行われるようにするため、その基準や考え方を明確にすることが必要である。

また、以上にあたっては、クラウドサービス事業者とクラウドサービス利用者としての通信事業者との間において、双方向のコミュニケーションを通じた、クラウドサービス障害によるクラウドサービス利用者側の影響の把握やそれを踏まえた対応等の連携協力も重要である。

②対応の方向性

他の通信事業者が通信サービスを提供するために利用される、通信媒介機能を提供するクラウドサービスの障害について、的確な観察(Observe)や、リスクの総合的な分析・評価等を可能とするPDCAサイクルを構築することが必要である。

そのため、総務省においては、事故GLにおける通信事業者間に関する「中継系事業者の事故に係る事象発生時の事故への該当性に関する判断」や、前述した重要インフラ分野に提供される通信サービス・ネットワークの通信事故に関する考え方も踏まえつつ、通信事故に該当する場合のクラウドサービス障害に関する基準や考え方を事故GLにより具体化・明確化することが必要である。

また、以上の具体化・明確化にあたっては、実際に外国法人等が提供するクラウドサービスの通信媒介機能の障害による通信事故が発生していること等から、「外国法人等が電気通信事業を営む場合における電気通信事業法の適用に関する考え方」(令和3年2月総務省)⁴も踏まえることが必要である。

⁴ 総務省ウェブページ(https://www.soumu.go.jp/main_content/000739291.pdf)参照。

なお、通信媒介機能を提供するクラウドサービスについては、電気通信事業法施行規則(第 58 条)に規定する「重要電気通信設備」として、衛星や海底ケーブルと同様、当該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場合に重大事故として報告を求めることが適当とする考え方もある。これについては、通信媒介機能を提供するクラウドサービスの通信サービス・ネットワークにおける利用状況や以上の事故 GL 等による明確化・具体化を通じた今後の通信事故としての報告等も踏まえつつ、総務省において、引続き検討することが適当である。

2.2.3 通信事故の兆候(インシデント)に関する報告制度の在り方

(1)現状・課題

通信事故の報告制度においては、通信サービス・ネットワークの提供停止又は品質低下を対象として、リスクによる影響が顕在化した「アクシデント」、そして、アクシデントの兆候段階の事態である「インシデント」について、同じ「通信事故」として定義し、それらの報告を通信事業者に求めている。

以上のうち、重大なリスクによる影響が顕在化したアクシデントのみが重大事故として定義され、総務省と通信事業者等による即応連携等の OODA ループ的な対応の対象となっている。他方、インシデントについては、重大事故ではなく、四半期報告事故としてのみ定義され、次のものが対象となっている。

- 1) 電気通信設備に関する情報(電気通信設備であるサーバのログイン ID やパスワード等)の漏えいにより通信サービスの提供に支障を及ぼすおそれがある事態
- 2) 移動通信における無線基地局の故障について、隣接の基地局による応急的なエリア補完により通信サービスの提供が継続され、利用者に直接的な影響が及んでいない事態

しかしながら、近年、四半期報告事故として報告されたインシデントの中には、例えば、サイバー攻撃により窃取された電気通信設備に関する情報が悪用され、通信サービスの提供先である重要インフラ分野事業者が緊急時の事業継続等のために利用する当該通信サービスの提供が停止するおそれがある事態など、そのリスクによる影響が顕在化した場合には重大事故と同様に社会的な影響が大きく、重大なリスクと考えられるものが含まれていたところである。

そこで、リスクの量的・質的な変化及びマルチステークホルダーへの拡散に対し、OODA ループ機能を強化する観点から、重大事故の範囲を見直し、重大事故と同様の重大なリスクであるインシデントについて、速やかな報告の対象とすることが課題となっている。

(2)考え方

インシデントのうち重大事故が発生するおそれがあると認められるもの(重大インシデント)については、通信事業者において、当該事態が認められる場合、当該通信事業者による速やかな総務省への報告を契機として、マルチステークホルダーとの即応連携により、通信サービス・ネットワークの円滑な(確実かつ安定的な)提供の確保と利用者利益の保護を図ることが必要と考えられる。

また、インシデントについては、アクシデントと異なり、実際の影響(人的、物的、社会的な被害等)が顕在化していない事態であり、そのような目に見える影響がないことから、通信事業者において、その発生を確認することが困難な場合があると考えられる。

特に、四半期報告事故が制度化された2008年度当初と異なり、近年では、実際に報告された前述のインシデントのように、益々高度化・巧妙化・悪質化するサイバー攻撃によるリスクが深刻化している状況にある。

以上を踏まえると、インシデントについて、電気通信設備に関する情報の漏えいが発生した場合に、通信事故として報告しないこと等が罰則規定の適用対象となる現行の報告制度の対象とすることは、通信事業者に対して過度の負担を課すものになっている場合があると考えられる。

(3)対応の方向性

インシデントについて、的確な観察(Observe)や迅速な情勢判断(Orient)等によるOODA ループ的対応やリスクの総合的な分析・評価等を可能とするPDCAサイクルを構築することが必要である

総務省においては、国内における他の重要インフラ分野(例えば、金融や航空等)の取り組みや海外(例えば、欧州)における通信事故の報告制度の動向も踏まえつつ、リスクによる影響が顕在化したアクシデントを対象とする通信事故の報告制度とは別に、罰則の適用対象とならない新たな報告制度を整備することが適当である。

	鉄道	航空	銀行	電気
関係法令	●鉄道事業法 ●鉄道事故等報告規則(省令)	●航空法 ●航空法施行規則(省令)	●銀行法 ●総合的な監督指針	●電気事業法 ●電気関係報告規則(省令)
事故報告	●速やかに、電話等で地方運輸局長に報告 ●発生から2週間以内に、報告書を提出 ●100万円以下の過料	●国土交通大臣に報告 ●50万円以下の罰金	●直ちに、金融庁に報告 ●発生から1ヶ月以内に、報告 (●法24条の報告には罰則あり)	●発生を知った時から24時間以内可能な限り速やかに、電話等で経済産業大臣等に報告 ●発生を知った時から30日以内に報告書を提出 ●30万円以下の罰金
インシデント報告	●報告対象は省令で個別に規定 ・列車衝突事故 ・列車脱線事故 ・列車火災事故 など	●報告対象は省令で個別に規定 ・航空機の墜落・衝突・火災 ・航空機による人の死傷又は物件の損壊 など	●報告対象は、システム障害やサイバーセキュリティ事案の発生による次の障害等(原因の如何を問わず、現に使用中のシステム・機器に発生した障害) ・預金の払戻し、為替等の決済機能に遅延・停止等 ・資金繰り、財務状況把握等への影響 など	●報告対象は省令で個別に規定 ・感電、電気工作物の破損や誤操作等により人が死傷した事故 ・電気火災事故 ・電気工作物の破損や誤操作等による他の物件の損傷等の事故 ・主要電気工作物の破損事故 ・発電設備に係る7日間以上の発電支障事故 ・供給支障事故であって支障時間が一定時間のもの ・電気工作物に係る社会的に影響を及ぼした事故 など
	●速やかに、電話等で地方運輸局長に報告 ●発生の日翌20日までに、報告書を提出 ●報告対象は省令で個別に規定 ・列車が停止信号を冒進し、本線における他の列車等の進路を支障した事態 ・鉄道線路、運転保安設備等に列車の運転の安全に支障を及ぼす故障、等が生じた事態 ・列車等から危険品、火薬類等が著しく漏えいした事態 など	●国土交通大臣に報告 ●報告対象は省令で個別に規定 ・航行中他の航空機との衝突又は接触のおそれがあったと認められたとき ・航空機に装備されたシステムにおける航空機の航行安全に障害となる複数の故障 ・航空機内の気圧の異常な低下 ・緊急の措置を講ずる必要が生じた燃料の欠乏 など	●直ちに、金融庁に報告 ●発生から1ヶ月以内に、報告 ●報告対象は、システム障害やサイバーセキュリティ事案の発生による次の障害等(原因の如何を問わず、現に使用中のシステム・機器に発生した障害)のおそれ ・預金の払戻し、為替等の決済機能に遅延・停止等 ・資金繰り、財務状況把握等への影響 など ●障害発生ない場合でも、サイバー攻撃の予告・検知等により、顧客や業務に影響を及ぼす又はその可能性が高い時	

【図 2.2.16】他の重要インフラ分野における事故等の報告制度の概観

- NIS指令(2016/1148)において、①「**デジタルインフラ**」等の「重要インフラ運営者」、②「**デジタルサービス提供者**」を対象として、その**サービス提供の継続性に重大な影響を及ぼすインシデント報告制度**が規定。
- 2020年12月の新たな「**サイバーセキュリティ戦略**」にて**NIS2指令案**等公表。**EECC指令の報告制度も含めNIS指令を全面改正**。今後、EU理事会等との調整を経て、採択後18ヶ月以内に加盟国で措置予定。

NIS指令 (2016/1148) 14条・16条	NIS2指令案20条
<ul style="list-style-type: none"> ▶ 2013年2月の「サイバーセキュリティ戦略」において、NIS指令(Directive on security of network and information systems)が提案。2018年5月より施行。 ▶ 重要インフラ運営者(OES)及びデジタルサービス提供者(DSP)は、主務官庁やCSIRTに対し、不当な遅延なく報告する義務等を規定。 ▶ OESとして、エネルギー、交通、金融、医療、水道、デジタルインフラの7分野を規定。うち、デジタルインフラにつき、IXP、DNSサービスプロバイダ、TLD名前レジストリを規定。 ▶ DSPとして、オンライン市場、オンライン検索エンジン、クラウドサービスを規定。なお、零細企業等は対象外。 ▶ 対象となる「重大な影響」につき、加盟国が特に考慮すべき指標として、影響利用者数、継続時間及び地理的範囲を共通に規定。 ▶ DSPについては、次も規定。 <ul style="list-style-type: none"> ・「重大な影響」の要考慮指標として、提供サービスの機能への影響及び経済社会活動への影響も追加。 ・「重大な影響」のみなし規定(①提供するサービスが500万ユーザ時間超の利用不可、②提供するサービスやデータのCIAの侵害が10万ユーザ時間超、③公共の安全や人命損失等の危険等) ▶ OESがそのサービス提供にあたり第三者のDSPに依存する場合、当該DSPに影響及ぼすインシデントによる重要インフラサービスの継続への重大な影響全てについて、OESが報告する義務を規定。 詳細は、「Commission Implementing Regulation(EU)2018/151」参照 	<ul style="list-style-type: none"> ▶ OESとDSPの区分を見直し、重要性等に応じ異なる規制枠組みが適用される「不可欠主体(EE:essential entities)」と「重要主体(IE:important entities)」に見直し。重要インフラの対象を拡大。 ▶ EEとして、「デジタルインフラ」が規定。NIS指令のOESとしてのデジタルインフラ(IXP、DNSサービスプロバイダ、TLD名前レジストリ)、EECC指令の電気通信ネットワーク/サービスに加え、新たに、データセンターサービス、CDN、トラストサービス、NIS指令のDSPの1つであるクラウドサービスが対象。 ▶ IEとして、「デジタル提供者」が規定。NIS指令のDSP(オンライン市場、オンライン検索)に加え、新たに、SNSプラットフォームが対象。 ▶ EE及びIEは、主務官庁やCSIRTに対し、サービス提供に重大な影響を及ぼすいかなるインシデントを不当な遅延なく報告する義務(24h以内の速報、求めで中間報告、30日以内の最終報告)を規定。 ▶ EE及びIEは、主務官庁やCSIRTに対し、重大なインシデントをもたらす可能性があると確認されるいかなる重大なサイバー脅威を不当な遅延なく報告する義務を規定。 ▶ 「重大」につき、当該主体に相当な運用上の混乱又は金銭的損失をもたらす(恐れも)がある場合、相当な物質的又は非物質的な損失により他の自然人・法人に影響を及ぼす(恐れも)がある場合と規定。 ▶ 上記インシデント及びサイバー脅威等について、各加盟国がENISAに対し、その概要を毎月報告する義務を規定。

【図 2.2.17】欧州ネットワーク・情報システムセキュリティ(NIS)指令による通信事故の報告制度

特に、インシデントのうち重大事故が発生するおそれがあると認められるもの(重大インシデント)については、通信事業者において当該事態が認められる場合に、総務省への速やかな報告を行うことにより、重大事故の発生の未然防止や利用者への被害拡大の防止等に向けて、的確かつ迅速な観察や情勢判断等によるOODAループ的な対応を可能とする観点から重要である。

更に、重大インシデントがサイバー攻撃を原因とする場合やおそれがある場合については、他の通信事業者等に対する同様の攻撃も想定される。そのため、通信事業者による共同でのサイバー攻撃への対応を支援するための第三者機関である「認定送信型対電気通信設備サイバー攻撃対処協会」⁵や NISC 等関係機関との間における攻撃関連情報の共有等による即応連携が、他の通信事業者等も含めた更なる被害の未然防止や拡大の防止等に有効であると考えられる。

以上を踏まえつつ、新たな報告制度においては、その実効性や公平性ととともに、関係機関との連携可能性を確保する観点から、例えば、前述したような、通信設備に関する情報の漏えいにより、通信サービスの提供先である重要インフラ分野事業者において、緊急時の事業継続等のために利用する当該通信サービスの提供停止のおそれがあると

⁵ 電気通信事業法第116条の2第1項の規定に基づき、2019年1月8日、総務大臣より、一般社団法人ICT-ISACが認定されている(https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000057.html参照)。

認められる事態など、報告対象となる重大インシデントの具体化・明確化を図ることが適当である⁶。

なお、以上の制度整備にあたっては、報告する通信事業者における負担軽減等に配慮する観点から、通信事故の報告制度と同様、報告システムの整備や報告を促すためのインセンティブの在り方に関する検討も重要である。

また、インターネットの輻輳や混雑を回避し、品質を維持・向上させるため、関係する民間事業者が連携協力して、情報共有等を行う「インターネットトラフィック流通効率化検討協議会」(Council for Network Efficiency by Cross-layer Technical members。以下、「CONNECT」という。)が設立⁷されているところ、重大インシデント等が発生した際に、インターネットトラフィックに関する技術者間で事後的に知見を共有する観点から、CONNECTにおける連携協力の可能性についても検討することが重要である。

⁶ 例えば、「個人情報保護法ガイドライン(通則編)の一部を改正する告示(案)」(2021年5月19日から同年6月18日まで意見募集中。 <https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=240000069&Mode=0> 参照。以下「個人情報ガイドライン」という。)においては、個人データの漏えい等に関する報告対象事態における「おそれ」について、「その時点で判明している事実関係に基づいて個別の事案ごとに蓋然性を考慮して判断することになる」とされ、「漏えい等が発生したおそれについては、その時点で判明している事実関係からして、漏えい等が疑われるものの確証がない場合がこれに該当する」とされている。また、サイバー攻撃の事案について、「漏えい」が発生したおそれがある事態に該当し得る事例として、例えば、「個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において外部からの不正アクセスによりデータが窃取された痕跡が認められた場合」、「個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合」、「マルウェアに感染したコンピュータに不正な指令を送り、制御するサーバ(C&Cサーバ)が使用しているものとして知られているIPアドレス・FQDN(Fully Qualified Domain Nameの略。サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ(サーバ等)を特定するもの。)への通信が確認された場合」や「不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合」が挙げられている。

⁷ 2020年4月に設立された(https://www.soumu.go.jp/menu_news/s-news/01kiban04_02000165.html 参照)。2021年4月時点で41者が参加している(https://www.soumu.go.jp/menu_seisaku/ictseisaku/conect/index.html 参照)。

2.2.4 四半期報告事故(簡易様式)の在り方

(1)現状・課題

四半期報告事故(簡易様式)については、利用者への影響が限定的であるため全体には及ばない電気通信設備の故障が対象となっており、当該故障による通信事故の発生件数のみの簡易な報告とされている。具体的には、次の故障が対象となっている。

- 1) 移動通信における無線基地局(携帯電話基地局等)
- 2) リモートターミナル(局設置遠隔収容装置又はき線点遠隔収容装置)
- 3) DSLAM(デジタル加入者回線アクセス多重化装置)

以上のうち、携帯電話基地局の故障については、隣接の同基地局による応急的なエリア補完により通信サービスの提供が継続され、利用者への直接的な影響が顕在化していないインシデントの場合も含め、故障した同基地局の件数が報告されている。また、通信サービスの提供停止により利用者に直接的な影響が発生した場合の件数のみが報告されている場合もある。

(2)考え方

今後整備が進展するSA方式による5Gの携帯電話基地局においては、主に一般利用者向けの通信サービスの用に供する4Gの同基地局等の故障による影響の程度と異なり、その産業・社会基盤化の進展に伴い、その故障により重要インフラサービス障害が発生するなど、社会的な影響が大きくなる場合も想定される。

従って、後述する大規模自然災害の場合を除き、その他の自然災害や自然故障等を原因とする無線基地局の故障については、その全体傾向等を把握する観点から、引続き、インシデントの場合を含む、故障した無線基地局の件数が報告されることが必要と考えられる。

(3)対応の方向性

移動通信における無線基地局(携帯電話基地局等)に関する四半期報告事故(簡易様式)について、総務省においては、次の点を事故GL等により具体化・明確化することが適当である。

- インシデントではなく、事故の報告となることから、基本的には、通信サービスの提供停止により利用者に直接的な影響が発生した場合の件数を報告すること

- 以上による報告が困難な場合には、利用者への通信サービスの提供停止があったか否かにかかわらず、インシデントの場合を含む、故障した無線基地局の件数を報告すること

2.2.5 報告システムの在り方

(1)現状・課題

現在、通信事業者が総務省に対して通信事故の報告を行うにあたり、四半期報告事故については、Excel 形式の報告様式(詳細様式及び簡易様式)に必要事項を記入又は選択したものを電子メールに添付する形で行われている。

また、重大事故を報告する場合については、速やかな報告は適宜様式により、また、事故発生後 30 日以内に行うこととされている詳細報告は、指定の報告様式に必要事項を記入したものを電子メールに添付する形で行われている。

他方、海外では、通信事故の報告等に関するシステムを整備・運用している例がある。

1) 米国 FCC (連邦通信委員会) の NORS (Network Outage Reporting System)

- ・ 1992 年より、有線コモンキャリア向けに重大な通信事故をタイムリーに報告する制度が導入されている。
- ・ 2004 年、米国の国土安全保障、公衆衛生または公共安全、及び経済福祉に影響を及ぼす可能性のあるサービス障害に関する迅速、完全、正確な情報への重要なニーズに対応するため、とりわけ国の通信ネットワーク及び重要インフラにおける非有線通信の高まる重要性の観点から、報告を求める事業者等の範囲について、有線コモンキャリア以外にも拡大(衛星、無線、相互接続された VoIP 及び信号システム 7(SS7)プロバイダー等)された。また、FCC の公共安全・国土安全保障局(PSHSB)が管理・運営するウェブベースの NORS を通じて、一定の持続時間とユーザへの影響の基準を超える重大な通信事故を報告することが義務付けられている。
- ・ NORS を通じて報告される通信事故について、FCC は、短期的に、大規模な通信事故の規模を査定するために分析するとともに、長期的に、ネットワーク信頼性に関する傾向を特定し、通信事業者が一定のネットワーク信頼性のベストプラクティスに従っていれば、その通信事故が予防等できる可能性があったか否か等を判断するために分析している。
- ・ NORS で収集された情報は、ネットワーク信頼性を改善するための FCC による調査及び勧告にも活用されている。また、継続的に、ネットワークの脆弱性を分析するためにも使われ、FCC が連邦諮問委員会法(Federal Advisory Committee Act)に基づき自らの下に設置した公的な諮問機関である「通信セキュリティ・信頼性・相互運用性評議会(Communications Security, Reliability, and Interoperability Council:CSRIC)」において、業界のベ

ストプラクティスの開発や、FCC への勧告含め FCC によるネットワーク信頼性のトレンド評価や見直すべき政策を判断する際にも活用されている。

- ・ NORS で報告される情報については、国家安全保障や商業的な競争上の懸念があることから、機密的な取扱いとされている。FCC においては、将来のネットワーク信頼性及びセキュリティを向上するため、過去と現時点の通信事故の分析が有用であることは認めつつ、通信事故に関する情報については、米国の重要なインフラであるネットワークを攻撃する悪意ある者に悪用される可能性を懸念があるため、当該情報を機密扱いとし、情報公開法(Freedom of Information Act:FOIA)に基づく情報公開請求の対象から除外している。
- ・ 他方、FCC は、国土安全保障省(DHS: Department of Homeland Security)の国家サイバーセキュリティ・通信統合センター(NCCIC : National Cybersecurity and Communications Integration Center)に対して、NORS データベースへの直接的なアクセスを認めている。また、当該機関以外は匿名化情報のみを利用していたが、今後は、一定の資格条件を満たす連邦政府や州等の機関においても、アクセス可能なユーザ数の制限や訓練の義務づけ等により、必要に応じ詳細な情報にアクセスすることも可能になる予定である。
- ・ 業界全体のネットワーク信頼性及び改善に向けた協調的な取組みのため、集積・匿名化された NORS データの限定的な分析については一般にも共有されている。

Notification > Initial > Final > Withdrawn

* Company: EXAMPLE COMPANY

* Type of Reporting Entity: -- None --

Incident Information

* Incident Date and Time: []

Date and Time Determined Reportable: []

E911 Outage: -- None --

* Time Zone: -- None --

* Reason Reportable: -- None --

Failure in Other Company?: No

Number of Potentially Affected >

Primary Contact Information >

Submit Notification

NORS Outage Reports **New** Go to: Outage Number Search

All > Class = NORS Outage Report

	Outage Number	Created by	Report Type	Company	State Affected	Reason Reportable	Type of Reporting Entity	Incident Date and Time
<input type="checkbox"/>	17-02742774	vishalsugathan@gmail.com	Notification	ACE TELEPHONE ASSOCIATION	MASSACHUSETTS	Cable telephony - 900,000 user-minutes	Satellite provider	2017-01-27 11:52:32
<input type="checkbox"/>	17-02742740	vishalsugathan@gmail.com	Notification	ACE TELEPHONE ASSOCIATION	RHODE ISLAND	MSC	Paging provider	2017-01-27 11:51:56
<input type="checkbox"/>	17-02727751	calvin.gerald@itfirm.com	Initial	Gerald - Kormann Wireless	MARYLAND	VoIP - 900,000 user-minutes	Wireless Carrier	01-27-2017 10:41:53

< **NORS Outage Report - ON-00009665** [] [] [] Submit Initial Report Withdraw Report Assignment Tracking

Notification > Initial > Final > Withdrawn

* Company: EXAMPLE COMPANY

* Type of Reporting Entity: Wireline Carrier

Outage Number: ON-00009665

Report Type: Notification

Incident Information >

Services Affected >

Number of Potentially Affected >

Primary Contact Information >

Secondary Contact Information >

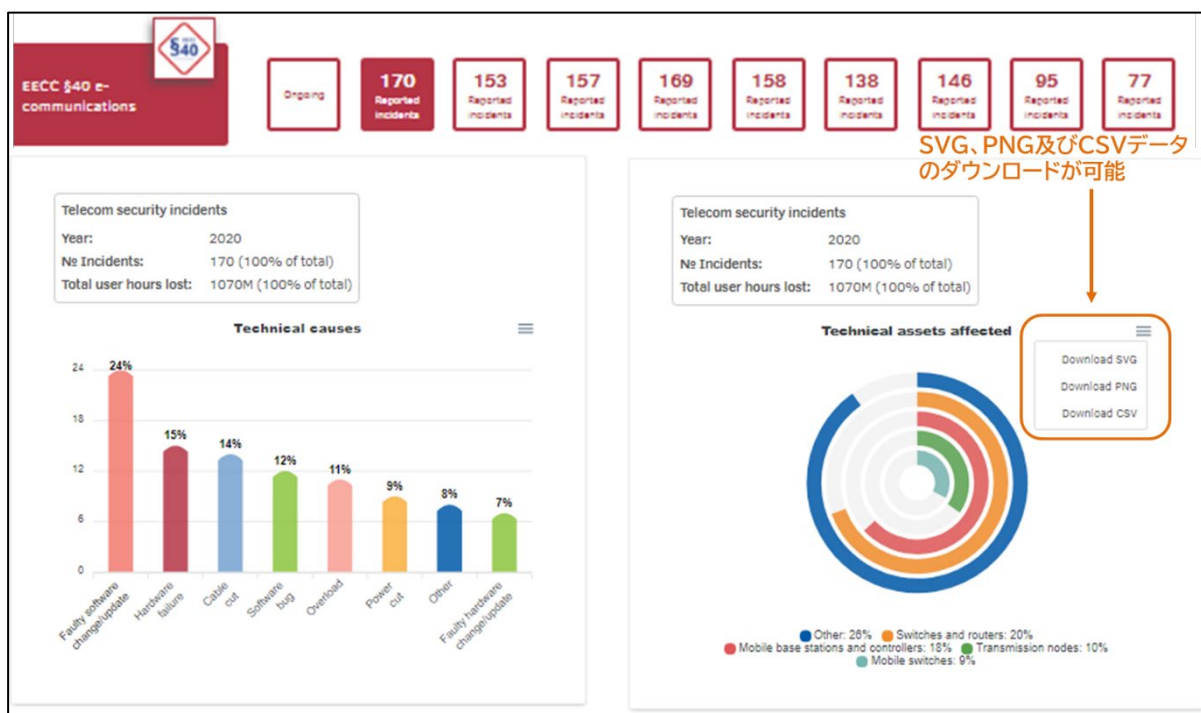
Submit Initial Report Withdraw Report Assignment Tracking

【図 2.2.18】 米国における通信事故の報告等システム「NORS(Network Outage Reporting System)」

2) 欧州ネットワーク・情報セキュリティ庁(ENISA)の Cybersecurity Incident Reporting and Analysis System(CIRAS)」

- EECC 指令 40 条や NIS 指令 14 条・16 条等で規定される通信事故等の報告について加盟国を支援するため、各加盟国の機関が使用できる報告ツールとして提供されている。
- CIRAS は、次の 3 つのツールで構成されている。
 - a) 報告プロセスの選択: 報告プロセスの選択(各国のホームページに移動し、過去のインシデントを閲覧可能)、インシデントの報告と共有、年次報告書の提出を行うことが可能。
 - b) オンラインビジュアルツール: 一般公開されており、8年分の通信事故等、合計 1,100 件のセキュリティ・インシデントを見ることが可能となっている。このツールでは、複数年にわたる傾向やパターンをカスタム分析することも可能。
 - c) スーパービジョンマップ: 加盟国やセクターごとの情報を収集することが可能で、セクターにおける主務官庁の権限に関する詳細、対象となるサービス及び起業するの推定値、インシデント報告のしきい値、導入されているセキュリティ要件の種類といった情報にアクセスすることが可能。





【図 2.2.19】 欧州における通信事故の報告等システム「CIRAS(Cybersecurity Incident report and Analysis System)」

(2) 考え方

今後、通信事業者における通信事故の報告に係る作業負担及び総務省における取りまとめや分析等に係る作業負担を軽減することが必要と考えられる。

また、通信事故の報告内容の平準化とともに、グラフによる可視化等を通じて、マルチステークホルダーにおける分析等の容易化等を可能とする観点から、オープンデータ化・ダッシュボード化を進めることが必要と考えられる。

(3) 対応の方向性

四半期報告事故については、海外(例えば、米国や欧州)における取組等を参照しつつ、総務省において、一般公開によるアクセスが可能なダッシュボード機能等を備えたウェブベースの報告システムについて、その要件定義の検討・開発等、報告制度の DX 化を推進することが適当である。

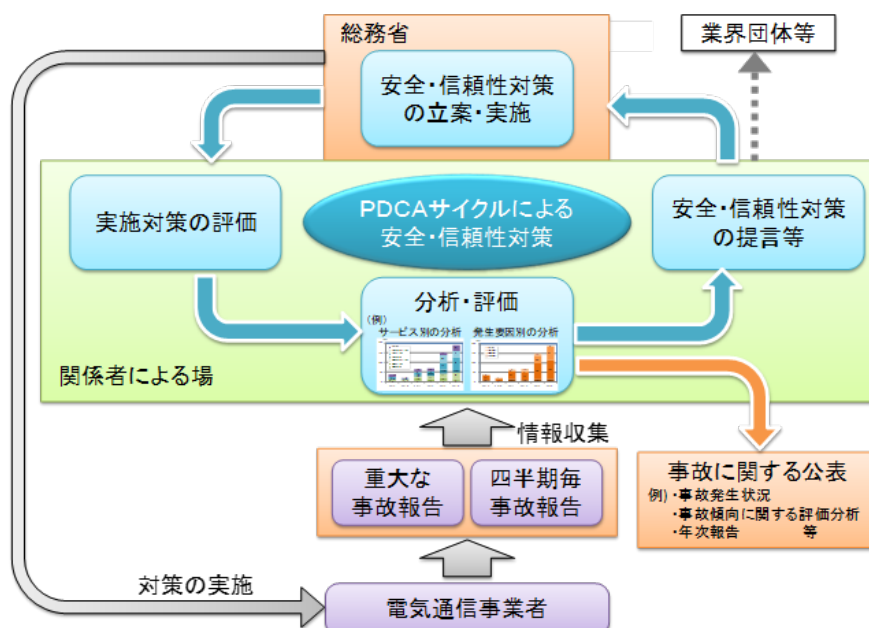
なお、当該システムで報告された通信事業者名等のデータの匿名化が必要である。具体的には、固有の通信サービスやネットワーク・設備の名称がある場合にはそれらの情報を削除するとともに、専門的な用語を用いずに汎用的かつ共通的な用語とする等の工夫により、通信事業者等が特定されないようにすることも必要である。

2.3 通信事故の検証制度の見直しの在り方

(1)はじめに

通信事故の検証制度については、2009年7月の「IPネットワーク設備委員会」報告(以下、「2009年報告書」という。)において、「機器の高度化に伴う設備のブラックボックス化、分散・冗長処理等に伴う複数機器同士の連携、制御ソフトウェアやアプリケーションの大規模化、機器ベンダやSier(システムインテグレータ)といった分業構造、電気通信サービスの多様化等の諸々の電気通信における動向が複合することで、事故の原因も複雑・多様化し、総務省による個別の指導・助言や技術基準等で個別に対応を図る手法によって対処を図っていくことが、次第に困難さを増してきており、また、その内容についても、高度に複雑化・専門化してきているという課題」認識により、他のインフラ分野(運輸分野等)や海外(米国等)での取組等を参考に、次のように提言されている。

- 1) 「総務省の他、各事業者、関係団体、専門家等が参画・連携し、事故発生状況や事故発生時等に各社から報告された内容等について詳細に分析・評価等を行うため、例えば情報通信審議会の常設の委員会として『電気通信安全・信頼性委員会(仮称)』を設置するなどの、体制の整備が必要」
- 2) 「当該体制においては、事故事例の分析・評価結果を踏まえ、安全・信頼性対策の提言を総務省や業界団体等へ行い、総務省等が提言を受けて適切な対策を実施し、実際に講じられた対策の効果を当該体制において評価し、更に新たな事故事例等の分析・評価を実施し、次の提言等に繋げていくという、PDCAサイクルにより電気通信分野における安全・信頼性対策を確固たるものにしていくことが必要」



【図 2.3.1】 関係者による事故発生状況等のフォロー等のイメージ

(出典:「IP ネットワーク設備委員会」報告 (総務省 2009 年 7 月 28 日))

また、2013年10月の「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(以下、「2013年報告書」という。)においても、次のように提言されている。

- 1) 「事故が生じた場合は、その収束後、まずは、事故発生事業者が、事故の内容や原因を自ら分析・検証し適切な再発防止策を策定することが重要であるが、当事者の自己チェックだけでは十分とは言えない場合もあることから、第三者たる国が、電気通信事業の監督者の視点から、事故報告内容の適切性を分析・検証することが、事故の再発防止を図るために重要」
- 2) 「事故報告内容については、国が単独で検証を行っているが、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」
- 3) 「情報通信審議会答申(2009年7月)においても、事故報告内容の詳細な分析・評価等を行うために、例えば、情報通信審議会に新たに委員会を設置するなどの体制整備が必要との提言がなされているところであることから、事故報告内容を再発防止に向けた各種の取組に更に有効活用できるようにする観点から、第三者検証の仕組みを新たに導入することが適当」

(2)現状・課題

以上の提言も踏まえつつ、2015年度より、総務省において、電気通信事故検証会議(以下、「検証会議」という。)が開催されている。この点、2009年報告書及び2013年報告書において、通信事故の報告内容の詳細な分析・評価等を行うための委員会を情報通信審議会に設置することが提言されていることとの関係については、主に、次の点から、当面の間の対応として、審議会等ではなく懇談会等行政運営上の会合である検証会議とされている。

- 1) 同審議会は政策諮問機関であり第三者検証機関として通信事故の報告内容の分析・評価は諮問にはなじまないこと
- 2) 通信事故はその時々で発生する事故の種類や状況が変わり早急な対応が必要になり、審議会の審議を経ると手続きに時間がかかり柔軟な対応ができないこと

検証会議は、重大事故及び四半期報告事故について、外部の専門的知見を活用しつつ分析・検証等を行うことにより、通信事故の発生に係る各段階で必要な措置が適切に確保される環境を整備し、通信事故の防止を図ることを目的としている。そのため、通信事故の当事者の責任を追求することが目的ではなく、重大事故等の概要、重大事故等を踏まえた教訓等及び四半期報告事故の統計分析等に関する検証報告書を毎年度公表

するにあたって、「本会議による検証は、事故の責任を問うために行うものではない」ことが付言されている。

また、検証会議による検証制度については、通信事故の報告制度と相俟って、実際に発生した通信事故の報告・分析・評価等を通じ、通信サービス面や通信ネットワーク・設備面における安全・信頼性対策を総務省において改めて検証し、再発防止等に向けた関係者の取組を充実・強化するために不可欠であり、通信サービス・ネットワークの安全・信頼性対策に関する PDCA サイクルの要となっている。

実際、上記 PDCA サイクルの意義や成果は現れている。この点、検証会議によるこれまでの取組を評価等する観点から、総務省において、2015 年度から 2018 年度に発生した重大事故の検証から得られた教訓等(45 項目)のうち、複数回取り上げられたため、当該教訓等に取り組むことが再発防止に特に効果等があると考えられるもの(20 項目)について、通信事業者の取組状況等に関するフォローアップアンケート調査(約 440 社より回答)が、関係事業者団体との連携・協力により 2020 年春頃に実施された。

以上の調査結果によると、当該教訓等に関する取組みが進んでいることや、検証会議による教訓等が契機となり当該教訓等が実施された状況が確認されている。従って、検証会議については、教訓等としての社会的な意義や、検証会議による検証及びその教訓等の整理に関する政策的な PDCA サイクルの意義があると認められ、その成果が現れていると考えられる。

他方、検証会議においては、環境変化に伴うリスクの多様化・複雑化やマルチステークホルダーへの拡散に対して、様々な課題が顕在化しつつある。

まず、検証対象となる事故等に関し、重大事故については、電気通信回線設備の故障に関する事故のみならず、近年、当該設備を設置しない通信事業者による事故が増加するとともに、重大事故には該当しないが、それに準ずる重大なリスクとして、例えば、次の事故等のように、検証が必要な対象が拡大している。

- 1) そもそも通信事故に該当しなかった「平成 29 年 8 月に発生した大規模なインターネット接続障害」(2017 年度)
- 2) 重大事故に該当しなかった「本格サービスが展開された場合には重大な事故に該当する可能性のある障害」(2019 年度)
- 3) アクシデントではなくインシデントである「電気通信設備に関する情報の漏えいによる通信サービスの提供に支障を及ぼすおそれに関する事故」(2020 年度)

次に、次のような重大事故も発生しており、検証の公正性や実効性の確保が課題となっている。

- 1) 故障した電気通信設備における当該故障の原因等の詳細について、事故の当事者である通信事業者に対して、当該設備の調達先である関係者からの十分な説明や情報提供が得られず、当該通信事業者において原因等の確認やリスクアセスメントが困難等とされた重大事故(2019年度)
- 2) 故障した電気通信設備に関する中核的なクラウド関連技術等について、通信事故の当事者である通信事業者に供与等している関係者が電気通信事業者ではなかったこと等から当該関係者の検証会議への参加が得られず、当該通信事業者による応急対応や再発防止策の十分な検証や、同じ技術が供与等されている別の通信事業者におけるリスクアセスメントが行えなかった重大事故(2020年度)

通信サービス・ネットワークの安全・信頼性対策に関する PDCA サイクルが取組むリスクが量的にも質的にも変化するとともに、マルチステークホルダーに拡散している状況において、通信事故の検証制度については、マルチステークホルダーとの連携・協力による同サイクルの実効性を確保するため、重大事故等の重大なリスクについて、電気通信事故検証会議の機能強化による第三者機関の在り方が課題となっている。

(3)考え方

①目的・理念

通信事故の検証制度については、電気通信事故検証会議が毎年度公表している検証報告書において、同会議による検証は「通信事故の責任を問うために行うものではない」と付言されている。

しかしながら、次の点を踏まえると、現行の検証制度については、通信事故の当事者である通信事業者に対する行政指導や行政処分等、再発防止等に向けた個別具体的な行政措置を講ずる過程における「行政調査」の一環として実施されている面があると考えられる。

- 1) 前述の 2013 年報告書において「電気通信事業の監督者の視点から、事故報告内容の適切性を分析・検証する」とされていること
- 2) 重大事故の検証結果を踏まえた行政指導が行われる場合があること(例えば、2019年1月ソフトバンク㈱に対する通信事故の再発防止に係る措置)

通信サービス・ネットワークがデジタル社会の中核基盤としてサイバー空間とフィジカル空間を繋ぐ神経網となり、その安全・信頼性を取巻くリスクが通信事業者のみならず、通信事業者以外も含むマルチステークホルダーに拡散しているとともに、サイバー攻撃の巧妙化・悪質化等も進展している。

このような中、通信事業者における教訓等が形式知化(想定内)された技術基準等の遵守をもとめる個別具体的な行政措置を通じて、安心・安全で信頼できる通信サービス・ネットワークの確保を図ることが益々困難になってきていると考えられる。実際、技術基準等の法令違反の場合においても通信事故の発生に至らない場合がある一方、当該法令を遵守している場合においても通信事故等が発生する場合もある。

そのため、以上の個別具体的な行政措置による対応と異なり、形式知化されていない未知(想定外)等のリスクについて、実際に発生した重大事故等に関する事故調査を通じた演繹的なアプローチにより評価するリスクアセスメントが益々求められている。

この点、2013 年報告書にもある通り、通信事故等が生じた場合は、まずはその当事者である通信事業者自らが原因等を分析・検証し、適切な再発防止策を策定することが重要である。しかしながら、通信事業者におけるリスクマネジメントが益々重要になる中、サイバー攻撃による場合や、中小規模事業者や新興事業者等における対応など、当事者である通信事業者の自己チェックだけでは十分とは言えない場合がある。

従って、災害対応の事後検証(AAR:After Action Review)のように、重大事故等に関するリスクをマルチステークホルダーの連携・協力により分析・評価し、見える化・共有するリスクアセスメントを通じて、通信事故等の再発防止や被害軽減等に向け、通信事業者におけるリスクマネジメントを促し、社会全体で複雑化・多様化するリスクに取り組む PDCA サイクルの強靱性・実効性を確保することが一層必要になってきている。

リスクアセスメントについては、前述のように、多くの重要インフラ事業者で実施されている帰納的なアプローチを補完する観点からも、演繹的なアプローチが重要である。そのためには、公正・中立な観点から、通信事故等の発生やその被害拡大等に関する原因究明等を通じてリスク評価を行い、その再発防止や被害軽減等に資する科学的知見を整理して公表等する事故調査機能が有効かつ不可欠と考えられる。

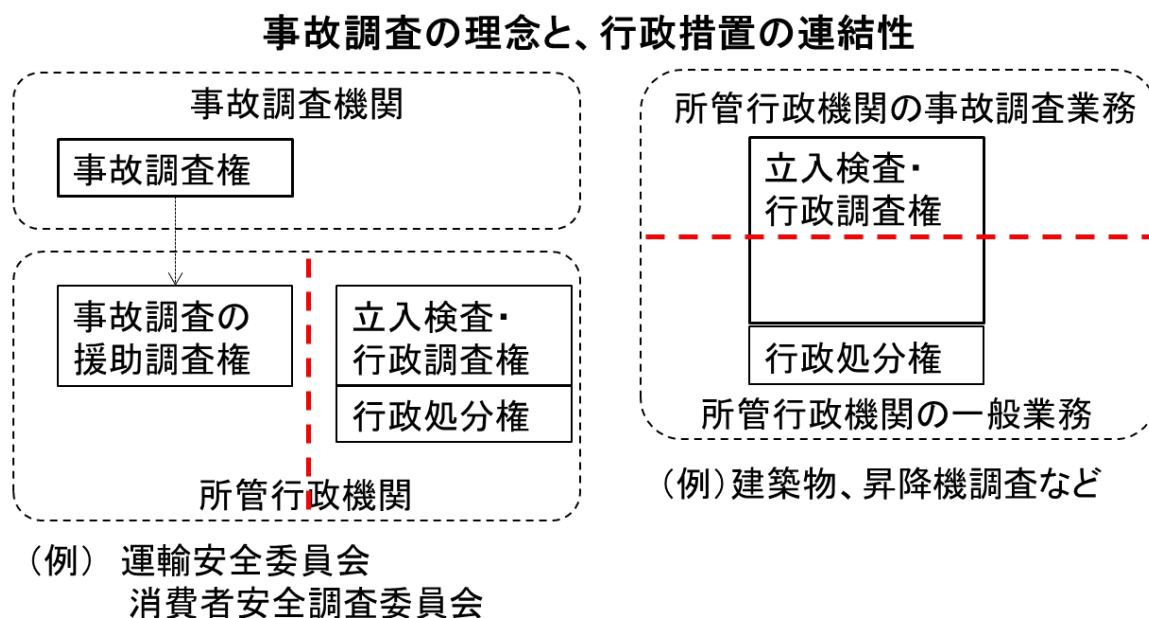
なお、事故調査については、通信事業者をはじめとする通信事故等の原因等の関係者による協力を基本とするものであり、当該関係者からの円滑な協力を得ることが必要である。そのため、現行の検証制度において見られるように、通信事故等の当事者である通信事業者に対する行政上の責任追及や、関係者において通信事故に関する情報提供に伴う不利益に繋がる等、個別具体的な行政措置を講ずる過程における行政調査の一環として実施されることは避ける必要があると考えられる。

	事故調査	行政調査(立入検査等)
目的	・事故原因の究明 ・再発防止対策 (被害の拡大防止)	・違法行為の発見 ・違法の是正改善 (反省の機会付与)
評価の判断基準・ 指針等	・因果関係 ・科学技術に関する社 会通念からの逸脱	・遵守すべき法令 (安全基準等) ・社会影響 ・公益を害する事実
調査・検査権限	事故調査権限	立入調査・検査権限
目的達成の手段	・非権力的 (公表、勧告)	・権力的 (処分、命令、行政指導)
その他	どちらかといえば、自主 改善の理念	どちらかといえば、法治国 家の理念

注:本整理表は、筆者の実務経験及び知識に基づき検討したものである。

【出典】第5回事故報告・検証制度等TF資料5-2-1(押立貴志 法政大学大学院公共政策研究科 講師)を一部加工

【図 2. 3.2】 事故調査と行政調査



【出典】第5回事故報告・検証制度等TF資料5-2-1(押立貴志 法政大学大学院公共政策研究科 講師)を一部加工

【図 2. 3.3】 組織分離と権限分離(行政法学視点)

②対象とする通信事故等の範囲

重大なリスクが顕在化したアクシデントとして、総務省や通信事業者等のマルチステークホルダー間の即応連携が求められる観点から事故報告制度の対象とされる重大事故については、その社会的な影響の大きさに鑑み、リスクアセスメントを踏まえた関係者における再発防止や被害軽減等にむけた取組が期待されることから、対象とすることが必要と考えられる。

同様に、リスクが顕在化した場合には重大事故と同様に社会的な影響が大きいと考えられる観点から新たな報告制度の対象とされる重大インシデントについても、リスクアセスメントを踏まえた関係者における予防的な対応に向けた取組が期待されることから、対象とすることが必要と考えられる。

なお、通信事故等の原因については、ヒューマンエラーや管理不良等の内部要因によるのか、卸元・委託先等における電気通信設備の故障等の外部要因によるのか、サイバー攻撃等の意図的な行為によるのか、自然災害等の不可抗力によるのか、根本的な原因か直接的・間接的な原因かなど、複合的な要因等による場合も含め、様々である。これらについて、安心・安全で信頼できる通信サービス・ネットワークの確保の観点から、事実認定や推論等を行うことが事故調査等によるリスク評価の意義・役割であることから、基本的には、自然災害やサイバー攻撃等の原因にかかわらず、重大事故及び重大インシデントに該当する場合には対象とすることが必要である。

但し、災害対策基本法等に基づく政府対策本部等において、関係府省や指定公共機関等の即応連携による OODA ループ的な対応が行われる大規模自然災害や大規模サイバー攻撃事態等の場合、特に指定公共機関としての通信事業者における通信サービス等の被害状況等については、電気通信事業法に基づく通信事故の報告制度ではなく、当該基本法等による別の枠組みにおいて報告が行われている。また、大規模自然災害等においては、同時並行的に通信サービス・ネットワーク以外の電力や道路等の生活インフラ等における障害も発生し、それらが複合的な要因として相互に影響等するため、「令和元年房総半島台風(台風第15号)」等に関する検証チームのように、政府全体による総合的な検証が行われる場合がある。

従って、以上のような別の枠組みの対象となる通信事故等については、その対象となる通信事業者の負担軽減にも配慮しつつ、当該枠組みによる総合的な検証との連携協力を推進する観点から、例えば、指定公共機関以外の通信事業者における通信事故等に関するリスクアセスメントを行うなど、必要に応じて対応することが適当である。

③必要な機能・体制等

重大事故及び重大インシデントのリスクアセスメントにおいて必要な機能としては、運輸安全委員会、消費者安全調査委員会や他の重要インフラ分野における事故調査制度に見られるように、通信事故等の原因及びそれに伴い発生した被害の拡大等の原因を究明し、それらに関するリスク評価を行うため、行政調査権限とは別の、通信事故等の原因に関係があると認められるマルチステークホルダーからの報告徴収、必要と認める場所への立入調査や物件の提出・保全等が考えられる。

以上によるリスクアセスメントを踏まえ、通信事故等の再発防止や被害軽減等の観点から、総務省等におけるOODAループ的な対応等のための報告制度等について、必要な施策等を総務省に対して勧告できる機能が必要である。例えば、前述した重要インフラ分野に提供される通信サービス・ネットワークの通信事故等に関する重大事故や重大インシデントへの該当性の判断等について、当該機能を通じて、その透明性や公平性の確保を図り、報告制度の対象となる重大なリスクに対する通信事業者等のマルチステークホルダーにおけるリスクマネジメントを促すことにより、PDCA サイクルの強靱性・実効性を確保することが重要と考えられる。

更に、社会的な影響の大きい通信事故等(例えば、大規模自然災害による場合等)のうち、通信事業者の取組のみでは再発防止や被害軽減等が見込めず、その他のマルチステークホルダーによる取組が有効と考えられる場合については、それらとの連携協力を一層推進する観点から、リスクアセスメント結果を踏まえて、関係団体や行政機関等に対して意見を述べることも重要と考えられる。

また、現行の通信事故の検証制度の運用体制においては、通信事故の報告制度に基づく重大事故に関する行政調査や、大規模災害時等における関係者との即応連携等のOODAループ的な対応も行っているところである。そのため、重大事故等の事故調査を通じたリスクアセスメントにおいては、行政調査の目的との混同や事故調査等の結果に基づく行政指導や処分を回避する観点からも、現行の運用体制とは別に十分な体制が必要と考えられる。

以上の必要な機能や体制を踏まえると、重大事故等の事故調査を通じたリスクアセスメント機能を強化するためには、次のような第三者機関が必要と考えられる。

- 1) 科学的かつ公正な判断を行うことができると認められる者や事故等に関する専門事項に関して優れた識見を有する者等の第三者により構成されること
- 2) 上記1)を円滑に実施するため、総務省による援助が可能であること
- 3) 通信事故等に関係する通信事業者等から専門的知見を集めるいわゆる「パーティー・システム」など、産学等における専門機関と連携協力すること

- 4) 通信事故等に係る通信事業者等に関する機微情報を取扱うため、中立かつ公正であること
- 5) 現行の行政調査等から一定の独立性があること

④その他(検証結果の取扱い等)

重大事故等の事故調査を通じたリスクアセスメントの結果については、機微情報を除き報告書として公表する等、マルチステークホルダーとのリスクコミュニケーションを通じて、大学や研究所等における学術・研究的な活用、消費者団体や通信事業者団体等における教育研修のための活用、通信事業者における他事業者からの教訓の活用など、様々な形で活用されることが期待される。

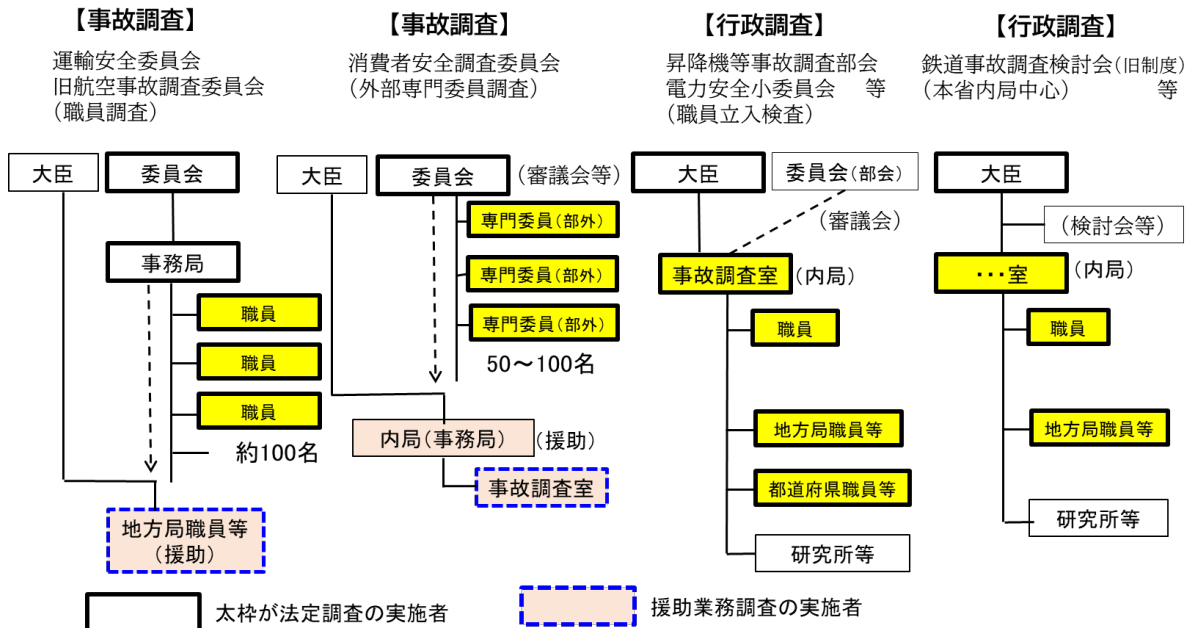
これにより、デジタル社会における通信事故の防止や被害の拡大防止等に向けて、マルチステークホルダーにおけるリスクへの対応の最適化を通じた連携・協力が推進され、安心・安全で信頼できる通信サービス・ネットワークを確保するための PDCA サイクルの強靱性・実効性が確保されることが期待される。

また、事故調査については、マルチステークホルダーの円滑な協力を得るためには、当該関係者における調査に係る負担軽減に配慮するとともに、報告等される機微情報を保護することが重要であり、公表の際にはその点に留意することが必要である。

(4)対応の方向性

重大事故等に関する事故調査を通じた演繹的なアプローチによるリスクアセスメント機能の強化について、総務省においては、国内における他の重要インフラ分野等(例えば、運輸、消費者安全、食品安全や電力等)や海外(例えば、米国)における取組みも踏まえつつ、現行の検証制度を見直し、通信サービス・ネットワークの安全・信頼性対策におけるリスクマネジメントに関するPDCAサイクルの強靱性・実効性を確保するため、第三者機関の設置等、所要の制度整備を行うことが適当である。

なお、将来的には、当該機関において蓄積される通信事故等の事故調査やリスクアセスメント結果等の専門的知見について、重大事故や重大インシデントの再発防止や被害軽減等に向けた通信事業者等の関係者間における紛争の円滑な処理に資することも考えられる。例えば、通信サービスの提供に関する業務やその円滑な提供の確保のための情報提供や設備の利用等に関し、通信事業者間において協定・契約の協議が調わず、電気通信紛争処理委員会にあっせん・仲裁(電気通信事業法第154条第1項等)が申請された場合等において、重大事故等の再発防止等の観点から、当該機関による専門的知見の提供等の連携・協力も期待される。



【出典】第5回事故報告・検証制度等TF資料(押立貴志 法政大学大学院公共政策研究科 講師)を事務局にて一部加工

	運輸安全委員会	消費者安全調査委員会	昇降機等事故調査部会	電力安全小委員会	ガス安全小委員会
目的	・航空・鉄道・船舶事故等の原因究明等	・消費生活上の生命・身体被害に係る事故の原因究明等	・昇降機等事故の原因究明・再発防止策の審議	・発電・電気設備、工事に係る保安行政の在り方等の審議	・都市ガスの保安の在り方について審議
発足のきっかけ	・1971年7月ばんだい号墜落事故等、F86空中衝突事故	・ガス瞬間湯沸器事故、こんにゃくゼリー窒息事故等	・2006年6月シティハイツ竹芝エレベータ事故	・2011年3月東日本大震災をきっかけとした組織改編	
位置づけ	・国土交通省の外局(国家行政組織法第3条)	・消費者庁に設置された審議会等(国家行政組織法第8条)	・国土交通省の社会資本整備審議会に設置(国家行政組織法第8条)	・経済産業省の産業構造審議会 保安・消費生活用製品安全分科会に設置(国家行政組織法第8条)	
組織構成	・委員会 ・事務局	・委員会 ・事故調査部会(製品等事故、サービス等事故)	・事故調査部会	・小委員会	
業務内容	・事故・重大インシデントの原因や被害の原因の調査 ・事故情報の統計的分析 ・関係行政機関や原因関係者への勧告・意見 ・調査結果の公表 等	・事故原因等の調査(原因関係者への報告徴収等) ・他行政機関等による調査結果の評価 ・内閣総理大臣への勧告・意見具申 ・関係行政機関へ意見具申 ・調査結果の公表 等	・事故原因等の調査 ・事故・不具合情報の分析 ・関係行政機関に対する意見具申 ・調査結果の公表 等	・事故情報の分析結果の審議 ・火力発電所の計画外停止(故障・トラブル)の分析、電気保安統計の作成・分析 等	・事故情報の分析結果の審議 ・都市ガス事業者に係る年間の事故報告を集計し、要因分析を行った結果について審議等
委員の役割	・担当調査官の指名 ・調査結果の審議	・対象事故選定・調査 ・調査結果の評価	・事故調査 ・調査結果の審議	・集計・分析結果の審議	
事務局の役割	(委員会内に設置) ・調査・分析の実施	消費者庁消費者安全課 事故調査室 ・事故情報収集窓口	国土交通省建築指導課 昇降機等事故調査室 ・事故調査の実施	経済産業省産業保安グループ 電力安全課 ・事故情報の集計・分析、公表	経済産業省産業保安グループ ガス安全室 ・事故情報の集計・分析、公表
調査対象事故	・設置法に定める事故(墜落、衝突、脱線、火災、死傷、物件損壊、重大インシデント等)	・消費者安全法に定める事故(生命身体事故等において原因究明が必要なもの)	・特定行政庁等からの事故・不具合情報の中から選定	・電気の供給支障、電力設備の損壊、感電死傷、電気火災等	・供給支障、ガス中毒、着火・爆発等(消費、供給、製造の各段階)
調査方法	・担当調査官2~3名	・事故調査部会	・部会委員、事務局職員	・個別事故の調査は無し(事業者が報告)	
立入調査	・委員会に立入検査権限	・委員会に立入検査権限	・国土交通省職員に立入検査権限	・経済産業省職員に立入検査権限	
公表方法	・報告書・統計情報の公表	・報告書の公表	・報告書の公表	・集計・分析資料の公表	

【図 2.3.4】 他分野における事故調査等に関する第三者機関(例)

2.4 自然災害を原因とする通信事故の報告制度等の在り方

(1)現状・課題

近年、豪雨、台風、地震等による大規模自然災害が頻発化・激甚化している。例えば、広島県や愛媛県等における「平成 30 年 7 月豪雨」、震度 7 を計測し、日本初のブラックアウトによる大規模停電も発生した「平成 30 年北海道胆振東部地震」、「令和元年房総半島台風(台風第 15 号)」、「令和元年東日本台風(台風第 19 号)」や、予測困難な線状降水帯による「令和 2 年 7 月豪雨」等、各地で甚大な被害をもたらす大規模自然災害が毎年発生している。

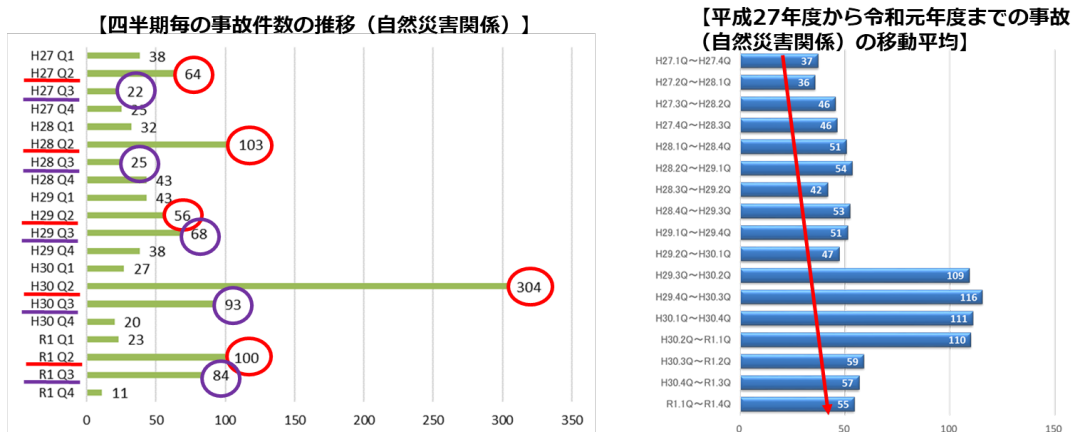
	災害名		災害名
1	平成 26 年台風第 8 号 (平成 26 年 7 月 6 日～7 月 11 日)	24	平成 29 年 6 月 30 日からの梅雨前線に伴う大雨及び 平成 29 年台風第 3 号 (九州北部豪雨を含む) (平成 29 年 6 月 30 日～7 月 10 日)
2	平成 26 年台風第 12 号及び第 11 号 (平成 26 年 7 月 30 日～8 月 11 日)	25	平成 29 年 7 月 22 日からの梅雨前線に伴う大雨 (平成 29 年 7 月 22 日～26 日)
3	平成 26 年 8 月 15 日からの大雨 (8 月 15 日～8 月 26 日) ※ 8 月 20 日広島土砂災害を除く	26	平成 29 年台風第 18 号 (平成 29 年 9 月 13 日～18 日)
4	平成 26 年 8 月 20 日広島土砂災害 (平成 26 年 8 月 19 日からの大雨による広島県における被害)	27	平成 29 年台風第 21 号 (平成 29 年 10 月 21 日～23 日)
5	平成 26 年御嶽山噴火 (平成 26 年 9 月 27 日)	28	平成 29 年からの大雪等 (平成 29 年 11 月～30 年 3 月)
6	長野県北部を震源とする地震 (平成 26 年 11 月 22 日)	29	華津白根山の噴火 (平成 30 年 1 月 23 日)
7	平成 26 年の大雪等 (平成 26 年 11 月～27 年 3 月)	30	鳥取県北部を震源とする地震 (平成 30 年 4 月 9 日)
8	口永良部島噴火【噴火警戒レベル 5】 (平成 27 年 5 月 29 日)	31	大分県中津市の土砂災害 (平成 30 年 4 月 14 日)
9	霧積山噴火【噴火警戒レベル 3】 (平成 27 年 6 月 30 日)	32	大阪府北部を震源とする地震 (平成 30 年 6 月 18 日)
10	平成 27 年台風第 11 号 (平成 27 年 7 月 16 日～7 月 18 日)	33	平成 30 年 7 月豪雨 (平成 30 年 6 月 28 日～7 月 8 日)
11	飯島の火山活動【噴火警戒レベル 4】 (平成 27 年 8 月 15 日)	34	口永良部島の火山活動【噴火警戒レベル 4】 (平成 30 年 8 月 15 日)
12	平成 27 年台風第 15 号 (平成 27 年 8 月 22 日～8 月 26 日)	35	平成 30 年台風第 21 号 (平成 30 年 9 月 3 日～9 月 5 日)
13	平成 27 年 9 月関東・東北豪雨【台風第 18 号を含む】 (平成 27 年 9 月 9 日～9 月 11 日)	36	平成 30 年北海道胆振東部地震 (平成 30 年 9 月 6 日)
14	平成 27 年台風第 21 号 (平成 27 年 9 月 27 日～28 日)	37	平成 30 年台風第 24 号 (平成 30 年 9 月 28 日～10 月 1 日)
15	平成 28 年 (2016 年) 熊本地震 (平成 28 年 4 月 14 日、16 日)	38	熊本県熊本地方を震源とする地震 (平成 31 年 1 月 3 日)
16	平成 28 年 6 月 20 日からの梅雨前線に伴う大雨 (平成 28 年 6 月 20 日～6 月 25 日)	39	北海道胆振地方中東部を震源とする地震 (平成 31 年 2 月 21 日)
17	平成 28 年台風第 7 号 (平成 28 年 8 月 16 日～8 月 18 日)	40	山形県沖を震源とする地震 (令和元年 6 月 18 日)
18	平成 28 年台風第 11 号及び第 9 号 (平成 28 年 8 月 20 日～8 月 23 日)	41	6 月下旬からの大雨 (令和元年 6 月 28 日～7 月 5 日)
19	平成 28 年台風第 10 号 (平成 28 年 8 月 26 日～8 月 31 日)	42	梅雨前線に伴う大雨及び令和元年台風第 5 号 (令和元年 7 月 17 日～22 日)
20	平成 28 年台風第 16 号 (平成 28 年 9 月 16 日～9 月 20 日)	43	令和元年台風第 10 号 (令和元年 8 月 12 日～16 日)
21	平成 28 年鳥取県中部を震源とする地震 (平成 28 年 10 月 21 日)	44	令和元年 8 月の前線に伴う大雨 (令和元年 8 月 26 日～29 日)
22	茨城県北部を震源とする地震 (平成 28 年 12 月 28 日)	45	令和元年房総半島台風 (令和元年 9 月 7 日～9 日)
23	平成 29 年 3 月 27 日栃木県那須町の豊崩 (平成 29 年 3 月 27 日)	46	令和元年東日本台風 (令和元年 10 月 10 日～13 日)

(出典) 内閣府 (2020) 「令和 2 年版防災白書」

【図 2.4.1】我が国における近年の甚大災害発生状況(2014 年以降)
(出典:「令和 2 年版情報通信白書」(2020 年 7 月総務省))

通信事故の報告制度において、自然災害を発生要因とする事故については、直近5年間に共通して、出水期に係る第2四半期や台風シーズンに係る第3四半期に多く報告されている傾向がある。また、大規模自然災害が集中した平成30年度においては全体の通信事故の報告件数のうち約7%となっているが、例年は全体の同件数の2~3%となっている。

- 四半期毎の事故件数のうち、「自然災害」を発生要因とする事故については、**第2四半期における過去5年の平均は約125件**。特に、平成30年度は平均の**2倍以上**であり、西日本を中心とした「平成30年7月豪雨」、関西地方等における「台風第21号」（平成30年9月4日に日本上陸）や「北海道胆振東部地震」（同年9月6日）等によるものと推察。
- また、**第3四半期における過去5年の平均が約58件**。特に、令和元年度は平均を大きく上回る**84件**（直近5年間で最多は平成30年度）であり、「令和元年東日本台風（台風第19号）」や「台風第21号」等によるものと推察。
- 平成27年度から令和元年度までの「自然災害」を発生要因とする事故の**移動平均**によると、平成30年度第2四半期を含む期間の件数が多く、それ以外の期間においては**若干の増加傾向**。



【図 2.4.2】 自然災害を発生要因とする通信事故の報告件数
 (出典:「令和元年度電気通信事故に関する検証報告」概要(2020年9月))

しかしながら、通信事故の報告制度においては、自然災害が大規模か否か、大規模自然災害であっても指定公共機関である通信事業者か否か等により、報告制度の対象となる通信事業者等が異なり、同一の自然災害であっても、それによる通信事故に関する被害状況の把握、それを踏まえた総合的な分析・検証や有効かつ迅速な復旧等の対策の検討等が十分に行うことができない現状にある。

例えば、大規模自然災害の場合、全国系の通信事業者については、災害対策基本法に基づく指定公共機関として、同法に基づく被害状況等の報告(以下、「災対法に基づく報告」という。)が行われている。これは、関係機関との相応連携によるOODAループ的対応を可能とする観点から、災害発生から復旧までの間、通信事業者から総務省を経由して政府対策本部等に対し、日々刻々と被害状況等に関する報告や公表が行われるものである。従って、早期復旧に取り組む通信事業者における負担軽減等を図るため、重大事故に該当する場合であっても、通信事故の報告制度に基づく報告対象としておらず、前述の通信事故の報告件数には含まれていない。

国民の生命、身体及び財産を災害から保護し、もって、社会の秩序の維持と公共の福祉の確保に資することを目的とする

1. 防災に関する責務の明確化

- 国、都道府県、市町村、**指定公共機関**等の責務 - 防災に関する計画の作成・実施、相互協力等
- 住民等の責務 - 自らの災害への備え、自発的な防災活動への参加等

2. 防災に関する組織—総合的防災行政の整備・推進

- 国：中央防災会議、非常（緊急）災害対策本部
- 都道府県・市町村：地方防災会議、災害対策本部

3. 防災計画—計画的防災行政の整備・推進

- 中央防災会議：防災基本計画
- 指定行政機関・**指定公共機関**：防災業務計画
- 都道府県・市町村：地域防災計画

4. 災害対策の推進

- 災害予防、災害応急対策、災害復旧という段階ごとに、各実施責任主体の果たすべき役割や権限を規定
- 市町村長に避難の指示、警戒区域の設定、応急公用負担等の権限を付与
- ＜市町村は防災対策の第一次的責務を負う＞

5. 財政金融措置

- 【原則】実施責任者負担
- 【例外】激甚な災害については、地方公共団体に対する国の特別の財政援助等
- 激甚災害に対処するための特別の財政援助等に関する法律

6. 災害緊急事態

- 災害緊急事態の布告 ⇒緊急災害対策本部の設置
- 緊急措置（生活必需物資の配給等の制限、金銭債務の支払猶予、海外からの支援受入れに係る緊急政令の制定）

【指定公共機関の通信事業者】

- 日本電信電話(株)
- 東日本電信電話(株)
- 西日本電信電話(株)
- エヌ・ティ・ティ・コミュニケーションズ(株)
- (株)NTTドコモ
- KDDI(株)
- ソフトバンク(株)

【出典】内閣府（防災情報のページ）

【図 2.4.3】 災害対策基本法における指定公共機関の位置づけ

この点、災対法に基づく報告においては、通信事故の報告制度における報告事項と同様の事項（故障設備、影響地域、影響利用者数、応急復旧措置、復旧見込み等）のみならず、当該制度の対象外とされている事項として、例えば、被災地域毎における携帯電話基地局の停波局数、固定電話のアクセス回線部分や利用者宅内機器の故障件数やその復旧見込み等も報告される場合があり、自然災害に応じ様々な対応状況となっている。

	固定電話	携帯電話
NTT 西日本	<ul style="list-style-type: none"> ・ 5,717→3,611 回線 ※支障エリアを含む自治体は以下の通り。 熊本県（3市町村） 八代市、葦北郡芦北町、球磨郡球磨村 大分県（2市） 日田市、佐伯市 京都府（1市） 京都市左京区 岐阜県（1市） 高山市 ※1村の役場エリアに支障あり。 熊本県（1村） 球磨郡球磨村 ○電話系サービス アナログ電話：4,791→2,936 回線 熊本県 2,219 回線、大分県 405 回線、京都府 230 回線、岐阜県 82 回線 ひかり電話：267 回線（光アクセスサービス内数） 熊本県 198 回線、京都府 69 回線 ○その他サービス 光アクセスサービス：374 回線 熊本県 264 回線、京都府 110 回線 ADSL アクセスサービス：224→50 回線（アナログ電話内数） 熊本県 50 回線 ISDN アクセスサービス：396→198 回線 熊本県 141 回線、大分県 17 回線、京都府 29 回線、岐阜県 11 回線 専用線サービス：156→103 回線 熊本県 56 回線、大分県 8 回線、京都府 33 回線、岐阜県 6 回線 	<ul style="list-style-type: none"> ・ 22 市町村の一部エリアに支障あり。 ※支障エリアを含む自治体は以下のとおり。 熊本県（9市町村） 球磨郡（球磨村、山江村、相良村、多良木町、水上村）、葦北郡芦北町、八代市、山鹿市、阿蘇郡小国町 鹿児島県（4市町） 伊佐市、曾於郡大崎町、志布志市、鹿屋市 大分県（4市町） 玖珠郡（九重町、玖珠町）、日田市、由布市 岐阜県（2市） 下呂市、高山市 愛知県（1市） 豊田市 京都府（1市） 京都市 和歌山県（1町） 有田郡有田川町 ※熊本県 球磨郡球磨村の仮設役場エリアは利用可 ※合計 123→124 局停波 （内訳） 熊本県 66 局、鹿児島県 5 局、大分県 32 局、岐阜県 8→11 局、愛知県 1 局、京都府 10→9 局、

※総務省「令和2年7月豪雨に関する被害状況について（第18報）」（2020年7月9日12:00現在https://www.soumu.go.jp/main_content/000696743.pdf）

【図 2.4.4】 「令和 2 年 7 月豪雨」における被害状況

携帯電話

携帯電話

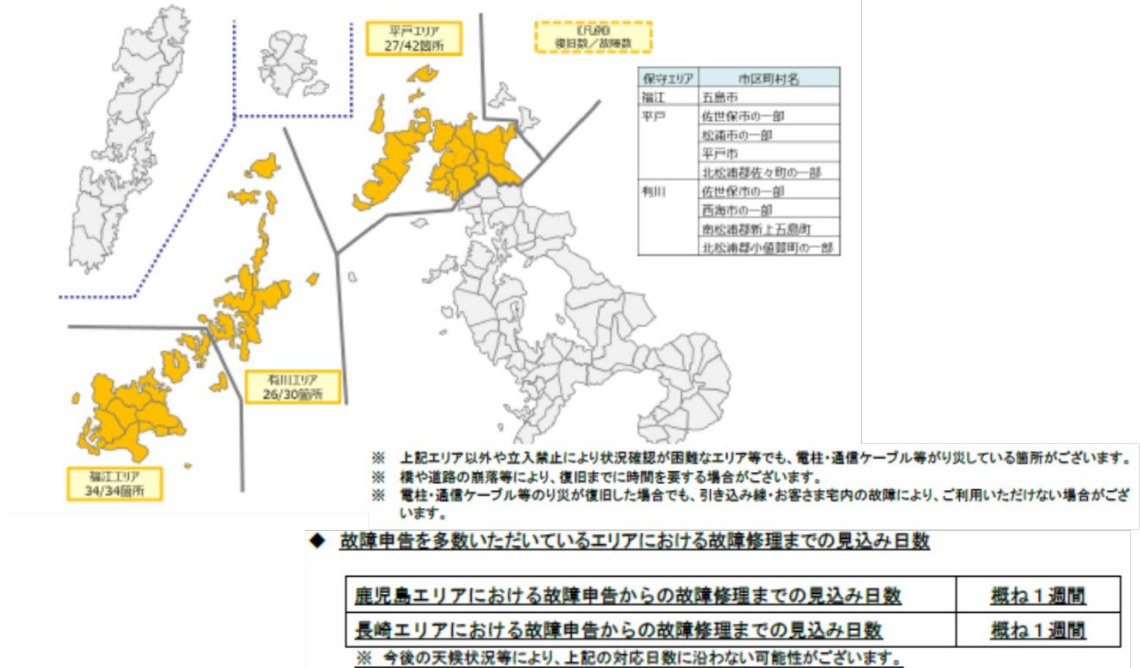
KDDI (au)	<p>・15 市町村の一部エリアに支障あり。 ※支障エリアを含む自治体は以下のとおり。 熊本県 (8 市町村) 人吉市、八代市、球磨郡 (山江村、球磨村、相良村)、葦北郡 (芦北町、津奈木町)、阿蘇郡小国町 大分県 (2 市町) 日田市、由布市 福岡県 (1 市) 八女市 京都府 (1 市) 京都市 大阪府 (1 市) 高槻市 岐阜県 (2 市) 下呂市、高山市 ※熊本県 球磨郡球磨村の仮設役場エリアは利用可 ※合計 103 局停波 (内訳) 熊本県 45 局、大分県 21 局、福岡県 11 局、京都府 9 局、大阪府 2 局、岐阜県 15 局</p>	ソフトバンク	<p>・23 市町村の一部エリアに支障あり。 ※支障エリアを含む自治体は以下のとおり。 熊本県 (14 市町村) 人吉市、八代市、球磨郡 (あさぎり町、多良木町、山江村、水上村、蒲池町、球磨村、相良村、錦町)、葦北郡 (津奈木町、芦北町)、阿蘇郡 (小国町、高森町) 鹿児島県 (2 市町村) 曾於郡大崎町、垂水市 大分県 (4 市町) 日田市、玖珠郡 (玖珠町、九重町)、由布市 京都府 (1 市) 京都市 岐阜県 (2 市) 下呂市、高山市 ※熊本県 球磨郡球磨村の仮設役場エリアは利用可 ※合計 165→174 局停波 (内訳) 熊本県 100→99 局、鹿児島県 12→13 局、大分県 26→27 局、岐阜県 16→24 局、京都府 11 局</p>
-----------	---	--------	--

※総務省「令和2年7月豪雨に関する被害状況について(第18報)」(2020年7月9日12:00現在https://www.soumu.go.jp/main_content/000696743.pdf)

【図 2.4.5】「令和 2 年 7 月豪雨」における被害状況

【長崎エリア】(9月25日時点)

※NTT西日本「台風10号による通信サービスへの影響について(第11報)」(2020年9月25日報道発表資料)



【図 2.4.6】 令和 2 年台風 10 号における通信ビルから利用者宅までの状況(固定電話)

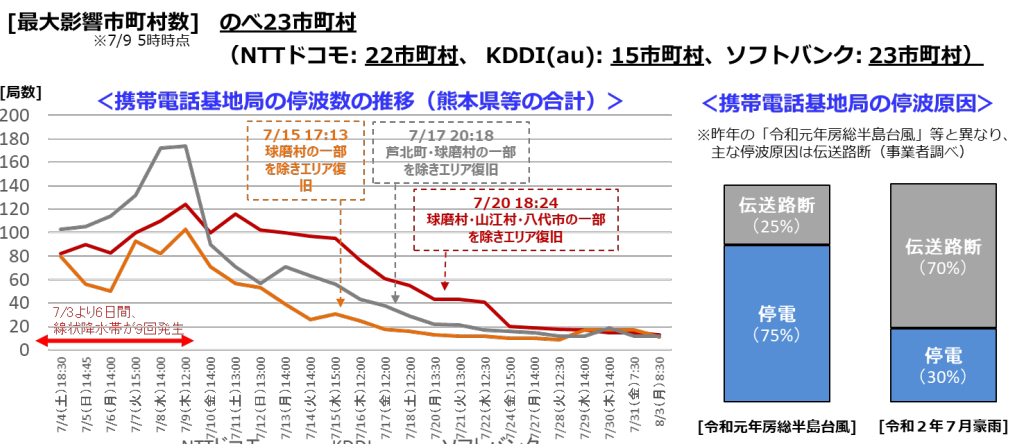
また、自然災害を発生要因とする通信事故として四半期報告事故として報告されているもののうち、それらの発生が大規模自然災害の期間と重なるものがある。これらについては、指定公共機関以外の、主に地域系や中小規模等の通信事業者における通信事故と考えられる。しかしながら、災対法に基づく報告の対象となる、顕著な災害を起こしたことから気象庁において名称が定められる自然現象(例えば、「令和元年房総半島台風」等)を原因とするものか否か、当該現象が原因となる場合において指定公共機関における通信設備の故障によるものか、自らの設備の故障によるものか、又は、その他停電等が原因か否か等が必ずしも明らかになっていない。

更に、大規模自然災害の場合、関係機関との相応連携によるOODAループ的対応を可能とする観点から、指定公共機関以外の通信事業者のうち一部の通信事業者については、総務省において、災対法に基づく報告と同様の被害状況等の報告の対象としている。当該報告については、総務省が整備した「非常時情報伝達ネットワーク」システムを通じて行われており、今秋頃、同システムは「災害情報自動集約ネットワークシステム(DaaS-Net)」に移行する予定である。

上記システムによる報告において、指定公共機関以外で対象となる通信事業者の範囲については、各総合通信局等に共通の統一的な基準ではなく、各地域の実情等を踏まえたものとなっている。従って、指定公共機関以外の通信事業者においては、同じ大規模自然災害であるにもかかわらず、通信事故の報告制度に基づく四半期報告事故として報告されず、前述の通信事故の報告件数には含まれていない場合もあり、通信事業者間における報告負担等に不公平が発生しているおそれも考えられる。

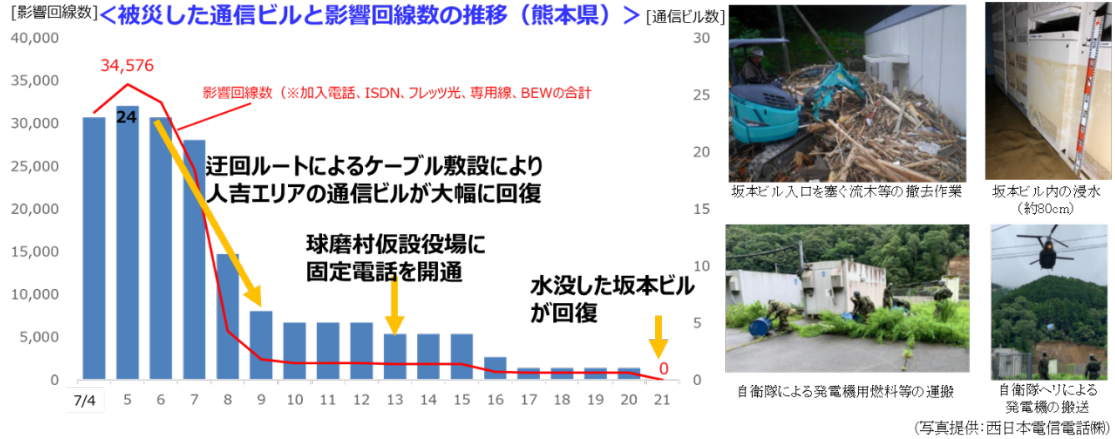
激甚化等する自然災害により通信障害も広域化・長期間化する中、被災地における通信環境の確保は、安否確認・生活改善や円滑な復旧活動等のために益々重要になっている。このため、自然災害により影響を受けた通信設備に関する影響範囲や応急復旧対策等の対応状況等について、主な原因等に関する全体的な傾向、接続先や卸先等の他の通信事業者への影響、停電や伝送路の損壊等に関する災害対策との関係等を分析・評価するとともに、通信事業者をはじめとする関係事業者や関係団体と共有することにより、今後の自然災害に備え、通信分野における一層の被害最小化や早期復旧等に向けた強靱化を確保するためのPDCAサイクルの構築を図ることが益々重要になっている。

- 球磨川等の決壊や土砂崩れ等による道路崩落や橋梁落下等により、携帯電話基地局同士をつなぐ基幹的な中継系伝送路の断線等による基地局の停波が発生。
- 携帯電話事業者においては、車載型基地局、可搬型衛星エントランス基地局、隣接基地局によるエリア補完や移動電源車等により、災害対策拠点となる市町村庁舎等のカバーエリアを優先しつつ、応急復旧対応等を実施。現在、立入困難区域（住民は避難中）を除き、全てエリア復旧済み。
- また、携帯電話事業者により、災害用伝言サービス、避難所における携帯電話の貸出しや充電用設備の提供、「00000JAPAN」によるWi-Fi無料開放等の被災者支援も実施。更に、衛星携帯電話等の貸出しにより、被災自治体、自衛隊や地方整備局等の復旧活動も支援。



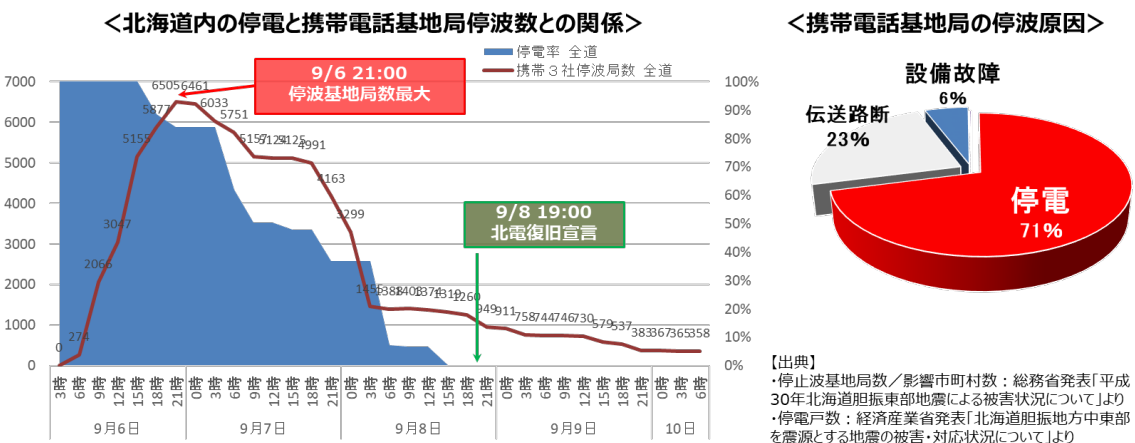
【図 2.4.7】 「令和2年7月豪雨」による影響(携帯電話)

- 球磨川等の決壊や土砂崩れ等による道路崩落や橋梁落下等により、多ルート化している両系の中継ケーブルの断線や水没等による通信ビルの機能停止が発生。
- NTT西日本においては、断線したケーブルの張替え、迂回ルートによるケーブル敷設、浸水した通信装置の入替え等により、通信ビル間の設備のサービスを回復。通信ビルから利用者宅近傍及び利用者宅までの被災設備について、避難中の住民に意向確認中の箇所等を除き、概ね復旧完了。
- また、NTT西日本により、災害用伝言サービス、公衆電話の無料開放、避難所における特設公衆電話やWi-Fiの設置等の被災者支援も実施。更に、衛星携帯電話等の貸出しにより、被災自治体、自衛隊や地方整備局等の復旧活動も支援。



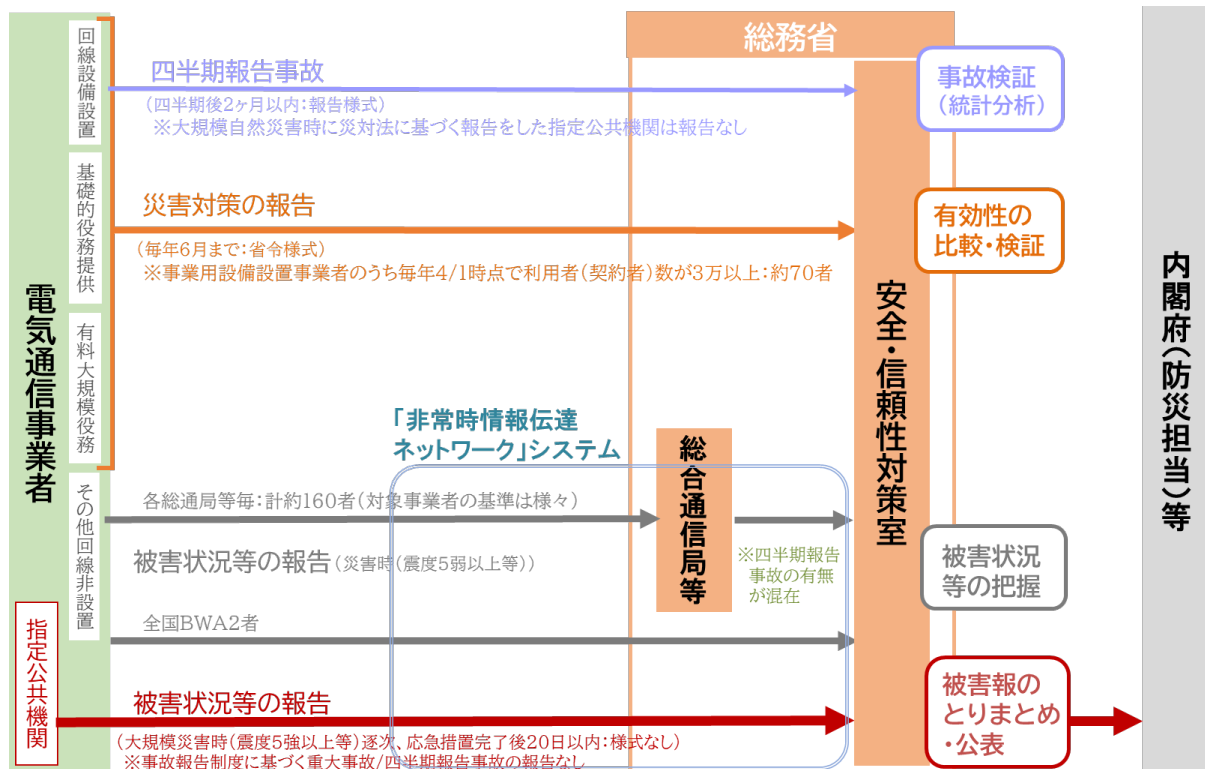
【図 2.4.8】 「令和2年7月豪雨」による影響(固定電話)

- 広域・長時間停電により、多くの携帯電話基地局が停波。他方、このような通常の規模を大きく上回る停電状況においても、エリア対策や非常用電源の確保等の応急復旧が実施され、サービス支障エリアは抑制。
- バッテリー枯渇等により、発災後24時間前後で基地局の停波のピークを迎えたが、その後、段階的に復電が行われたことにより、段階的に停波局数が減少。
- 中心的被災自治体等における通信サービスについて、被害状況の把握から応急復旧の初動対応等、迅速な応急復旧のための体制整備が課題。



【図 2.4.9】 「平成 30 年北海道胆振東部地震」による影響(携帯電話)

このため、自然災害による通信事故については、小規模・短時間の事故に内在している将来の大規模・長時間な事故へ発展する要因を含む事故を把握等するための四半期報告事故の中でも、外的要因としてその原因が明らかであり、また、通信設備の復旧まで長期間となる傾向もあること等から、早期復旧を優先する通信事業者における負担軽減等に配慮しつつ、自然災害を発生要因とする通信事故の報告及びその分析・検証等の在り方について、より有効かつ迅速な復旧等の災害対策を総合的に推進する観点から検討することが課題になっている。



【図 2.4.10】 自然災害に関する電気通信事故の報告制度等の現状

(2)考え方

①自然災害を発生要因とする通信事故に関する報告制度の在り方

自然災害を原因とする通信事故については、大規模自然災害の頻発化・激甚化による通信障害の広域化・長期間化する中、通信事業者、総務省や災害対応機関における即応連携による災対法等に基づく OODA ループ的な対応とともに、マルチステークホルダーにおける自然災害に関するリスクへの対応を通じた連携・協力が将来的にむけて推進されるための政策的 PDCA サイクルの実効性を強化していくことが益々重要になってきている。

そのため、被災地における被災者の安否確認・生活改善や円滑な復旧活動等のための通信環境の確保の観点から、特に、被災地における通信サービス・ネットワークの安全・信頼性におけるリスクが甚大である大規模自然災害については、指定公共機関である主要通信事業者による負担軽減を図り、その OODA ループ的な対応を最優先するため、DaaS-Net を通じて報告される被害状況等については、引続き災対法に基づく報告によるものとし、通信事故の報告制度の対象外とすることが必要と考えられる。

また、大規模自然災害の場合において、災対法に基づく報告と同様、DaaS-Net を通じた被害状況等の報告の対象となる指定公共機関以外の通信事業者の範囲については、負担軽減や公平性の観点から、全国で統一・共通的な基準が必要であると考えられる。なお、当該基準の対象となる通信事業者については、指定公共機関と同様、通信事故の報告制度の対象外とすることが必要と考えられる。

具体的には、電気通信事業報告規則第 7 条の 4 に基づく「災害対策の報告」として、停電や伝送路の損壊への対策のための応急復旧機材の配備状況等に関する報告の対象となっている「事業用電気通信設備を設置する通信事業者(毎報告年度の最初の日において3万人以上の利用者に電気通信役務を提供する者に限る。)」については、大規模自然災害により重大事故が発生する可能性が高いことから、災対法に基づく報告と同様の被害状況等の報告の対象とする必要があると考えられる。また、利用者が 3 万人未満であっても、指定公共機関等に対して伝送路等の通信サービスを提供している通信事業者についても同様の対象とする必要がある。

※電気通信事業報告規則第7条の4（災害対策の報告）等に基づくNTTドコモ、KDDI、ソフトバンクの合計値

対策項目	H23.2月 時点	東日本 大震災等	H28.3月 時点	熊本地震・ H29年7月 九州北部 豪雨等	H30.3月 時点	H30年7月 豪雨、H30 台風21号・ 北海道胆振 東部地震等	H31.3月 時点	令和元年 房総半島 台風・ 東日本 台風等	R2.3月 時点	
停電対策	移動電源車・ 可搬型発電機	約830台	約2.7倍	2265台	約1.1倍	2572台	約1.1倍	2730台	約1.2倍	3239台
	予備バッテリー の24時間化	約1000局	約5.9倍	約5850局	変化なし	約5850局	変化なし	約5850局	微増	約6050 局
伝送路断対策	基幹伝送路の 冗長化	2~3ルー ト	複数ルート化の 更なる強化	2~4ルー ト	変化なし	2~4ルー ト	変化なし	2~4ルー ト	変化なし	2~4ルート
	マイクロ イントラス回線	70回線	約5.1倍	359回線	約1.1倍	377回線	約0.9倍	357回線 ※他対策への移管 により減少	微増	367回線
	衛星 イントラス回線	26回線	約12倍	301回線	約1.3倍	377回線	約1.2倍	439回線	約1.5倍	655回線
エリアカバー対策	車載型基地局	41台	約3.4倍	140台	約1.2倍	165台	微増	168台	約1.2倍	199台
	可搬型基地局	約50台	約5.5倍	274台	変化なし	271台	約1.3倍	351台	約1.1倍	381台
	大ゾーン基地局	0局	新たに設置	116局	変化なし	116局	変化なし	116局	変化なし	116局

【図 2.4.11】 災害対策の報告等に基づく主要携帯電話事業者の対策(例)

更に、各地域の実情や、被災者に対する安否確認や地方自治体からの情報提供等の災害時における重要性等をふまえ、以上により対象となる通信事業者以外の通信事業者や通信サービスについても、必要に応じ、災対法に基づく報告と同様、DaaS-Net を通じた被害状況等の報告の対象とし、これらの通信事業者についても、通信事故の報告制度の対象外とすることが適当であると考えられる。

他方、災対法に基づく報告の対象となる指定公共機関及び当該報告と同様の被害状況等報告の対象となる通信事業者以外の通信事業者においては、引続き通信事故の報告制度の対象として、大規模自然災害による通信事故については、四半期報告事故等の報告が必要と考えられる。

大規模自然災害については、全ての通信事業者が直面する、不可避かつ不可抗力で甚大なリスクであることから、再発防止や被害軽減等に向けて、通信事故に関する被害状況の把握、それを踏まえた総合的な分析・検証や有効かつ迅速な復旧等の対策の検討等を十分かつ適切に行うための PDCA サイクルの構築を図ることが重要である。

この点、四半期報告事故における「主な発生原因」として「自然災害」が報告される場合、大規模自然災害が根本原因なのか、直接原因や間接原因なのかについては、災害毎、事業者毎等で様々であり、明らかではないと考えられる。実際、大規模自然災害によるものと考えられる四半期報告事故の報告においては、「主な発生原因」について、「自然災害」として報告される場合のほか、「他の電気通信事業者の事故による要因」、「停電」、「火災」、「第三者要因」、「不明」や「その他」等として報告されている場合がある。

従って、大規模自然災害の影響があると考えられる通信事故の場合、通信事業者においては、四半期報告事故の報告にあたり、少なくとも「自然災害」を「主な発生原因」として選択することが望ましい。また、その原因となる大規模自然災害との関連性を明確にするため、大規模自然災害について、気象庁が名称を定める顕著な災害を起こした自然現象(例えば、「令和元年房総半島台風」等)となる場合は、詳細様式にその旨が記載されることが必要であると考えられる。

以上の通り、大規模自然災害を発生要因とする通信事故については、指定公共機関による災対法に基づく報告、一部の通信事業者による当該報告と同様の被害状況等の報告、そして、その他の通信事業者による四半期報告事故の報告という3つの報告制度を通じて、通信事業者における負担軽減や公平性の確保を図りつつ、OODAループ的な対応を優先するとともに、携帯基地局へのエントランス回線や基幹回線等の伝送路断による携帯電話サービスの障害等の通信サービス・ネットワーク全体に跨がる通信事故の被害状況の把握、それを踏まえた分析・検証や有効・迅速な応急復旧対応等を総合的に検討することが可能になると考えられる。

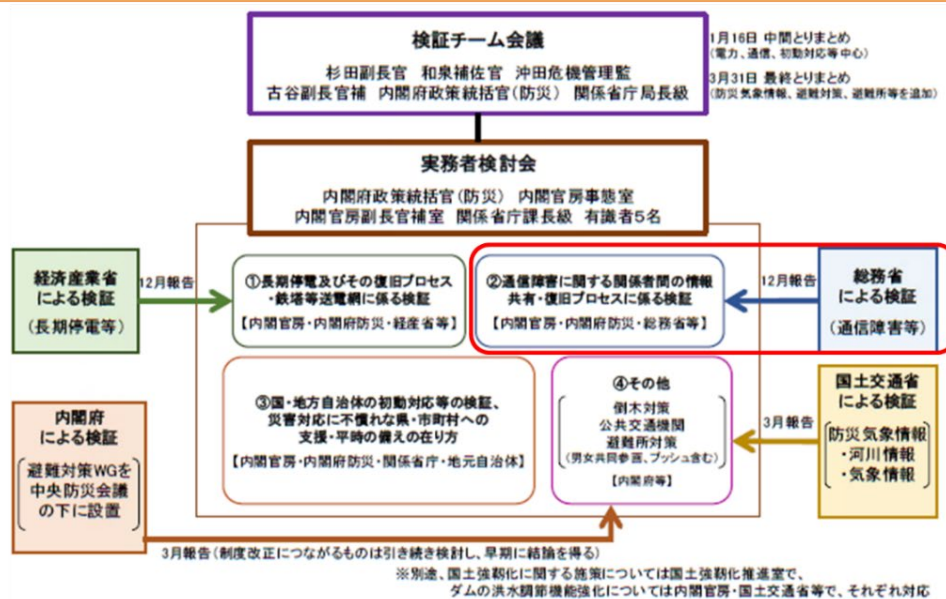
なお、大規模自然災害以外の自然災害による通信事故については、引続き全ての通信事業者を対象として、四半期報告事故として報告されることが適当である。その際、自然災害の影響があると考えられる通信事故の場合、詳細様式においては、少なくとも「自然災害」を「主な発生原因」として選択することが望ましい。

②自然災害を発生要因とする通信事故に関する検証制度の在り方

大規模自然災害を原因とする通信事故については、災対法に基づく政府対策本部等を中心とした、通信事業者、総務省や地方自治体等の災害対応機関における即応連携によるOODAループ的な対応とは別に、マルチステークホルダーにおける大規模自然災害に関するリスクへの対応を通じた連携・協力が将来的にむけて推進される観点から、政策的な PDCA サイクルの実効性を強化するため、基本的には、前述した第三者機関によるリスクアセスメントの対象とすることが適当であると考えられる。

この点、大規模自然災害を原因とする通信事故の場合、通信事故以外の電力や道路等の生活インフラ等における障害も同時並行的に発生し、それらが複合的な要因として相互に影響等するため、事後の検証として、「令和元年房総半島台風(台風第15号)」等に関する検証チームのように、関係府省における対応の在り方も含め、政府全体による総合的な検証が行われる場合がある。

- 令和元年台風第15号・第19号等の一連の災害において課題となった長期停電及びその復旧プロセス、その他課題となった事項について検証を行うため、令和元年10月2日に政府の検証チームが設置。
- 令和2年1月16日に検証レポートの中間とりまとめ、同年3月31日に最終とりまとめ。



【図 2.4.12】 令和元年台風第15号・第19号をはじめとした一連の災害に係る検証チーム

従って、以上の災対法に基づく枠組みによる総合的な検証の対象となる場合において、特に指定公共機関としての通信事業者における通信事故の状況等については、災対法に基づく被害状況等の報告が行われ、電気通信事業法上の通信事故の報告制度の対象外にもなることから、基本的には、現行の「災害時における通信サービスの確保に関する連絡会」を通じた指定公共機関を中心とする検証で十分であり、重大事故等に関するリスクアセスメントの対象とする必要性は高くないと考えられる。

- 平成30年における災害への対応の振り返りを踏まえ、災害時における通信サービスの確保に向けて、平時から体制を確認し、より適時適切な対応を行うことができるよう、総務省と主要電気通信事業者との間で「災害時における通信サービスの確保に関する連絡会」を平成30年10月に設置。
- 「令和元年台風第15号・第19号をはじめとした一連の災害に係る検証チーム」最終とりまとめ（令和2年3月31日内閣府）における課題や具体的な対応策等について検討。

設置する会合	主な議題	構成員	開催頻度
災害時における通信サービスの確保に関する連絡会	<ul style="list-style-type: none"> ・中心的被災市町村の役場の通信サービス確保のための初動対応 ・総務省／事業者リエゾンの連携の強化 	<ul style="list-style-type: none"> ■総務省：電気通信事業部長 電気通信技術システム課長 安全・信頼性対策室長 ■事業者：指定公共機関たる電気通信事業者の担当役員クラス※1 	年2～3回
部会	<ul style="list-style-type: none"> ・「重要インフラの緊急点検」の結果等を踏まえた措置 ・燃料の確保の在り方 ・電力の確保の在り方 	<ul style="list-style-type: none"> ■総務省：電気通信技術システム課長 安全・信頼性対策室長 ■事業者：指定公共機関たる電気通信事業者の災害対策室長等 	随時開催
地方連絡会	<ul style="list-style-type: none"> ・輸送手段の確保の在り方 ・迅速な情報把握・整理・公表の在り方 	<ul style="list-style-type: none"> ■総務省：各総合通信局長及び沖縄総合通信事務所長 ■事業者：指定公共機関たる電気通信事業者等※2 	随時開催

※1 日本電信電話(株)、東日本電信電話(株)、西日本電信電話(株)、NTTコミュニケーションズ(株)、(株)NTTドコモ、KDDI (株)、ソフトバンク(株)。また、オブザーバとして、楽天モバイル(株)、TCA(一般社団法人電気通信事業者協会)が参加。
 ※2 沖縄における地方連絡会にあっては、KDDI (株)に代えて、沖縄セルラー電話(株)が参加。

【図 2.4.13】災害時における通信サービスの確保に関する連絡会

しかしながら、以上の総合的な検証との連携協力を推進する必要がある場合や、当該総合的な検証の対象とならない場合等も考えられる。従って、前述した第三者機関において、対象となる通信事業者の負担軽減にも十分配慮しつつ、必要に応じて、例えば、大規模自然災害における通信事業者以外の原因による通信事故、自然災害等も含む複合連鎖災害による通信事故や指定公共機関以外の通信事業者における通信事故等に関するリスクアセスメントを行うことも可能とすることが適当である。

③報告システムの在り方

大規模自然災害時における通信サービス等に関する被害状況等の報告において利用されている Daas-Net については、今秋頃から運用が開始される予定である。この点、海外においても、自然災害時における通信障害の報告等に関するシステムを整備・運用している例がある。今後の DaaS-Net の運用において、実際の運用状況も踏まえつつ、将来的には、被災地の地方自治体等も含めた関係機関との情報共有等による一層の連

携・協力が期待される。

例えば、米国の FCC において、2005 年のハリケーン・カトリーナが通信・放送ネットワークにもたらした深刻な被害を契機として、2007 年に「DIRS : Disaster Information Reporting System」が構築された。同システムは、有線、無線、ケーブル・プロバイダーや放送事業者が、災害等の危機的なインシデント期間中にアクティベートされ、通信・放送インフラ状況及び状況認識情報を FCC に対して任意で報告するものであり、FCC において、報告されたインフラ状況情報の分析等を行っている。

DIRS は、NORS と同様、ウェブベースの報告システムであり、国家安全保障や商業的な競争上の懸念があることから、機密的な取扱いとされ、情報公開法に基づく情報公開請求の対象から除外されている。他方、FCC は、NCCIC に対して、DIRS データベースへの直接的なアクセスを認め、影響を受ける地域での当該機関の状況認識及び通信インフラの復旧有線順位付けの判断のためにこの分析が利用されている。なお、当該機関以外は匿名化された情報のみを利用していたが、今後は、必要に応じて一定の資格条件を満たす連邦政府や州等の機関においても、アクセス可能なユーザ数の制限や訓練の義務づけ等により詳細な障害データにアクセスすることが可能になる予定である。

また、FCC においては、災害等のインシデント期間中、一般に対しても、企業名を特定しない集積された情報を提供するとともに、提出された情報に基づいて、さらなる調査や分析を含む報告を公表する場合もある。

(3)対応の方向性

自然災害を原因とする通信事故の報告・検証制度については、総務省において、災害対策基本法に基づく枠組みとの連携・協力を一層推進するため、次の所要の制度整備等を講ずることが適当である。

- ① DaaS-Net による被害状況等の報告について、指定公共機関以外で対象となる通信事業者に関する全国共通の統一的な基準等による運用
- ② DaaS-Net による被害状況等の報告の対象となる場合について、通信事故の報告制度の対象外とすることの明確化
- ③ 四半期報告事故に関するウェブベースの新たな報告システムについて、気象庁が名称を定める顕著な災害を起こした自然現象の選択機能等の追加
- ④ 四半期報告事故の発生要因について、直接原因が第三者設備故障や停電等であっても、その根本要因が自然災害と考えられる場合等に関する事故 GL の明確化

- ⑤ 重大事故等に関するリスクアセスメントについて、内閣府(防災担当)等の防災関係機関との連携・協力を推進するための体制等の整備

2.5 サイバー攻撃を原因とする通信事故の報告制度等の在り方

(1)現状・課題

近年、サイバー攻撃については、攻撃手法の巧妙化のみならず、目的・狙いも多様化・悪質化している。従業員やユーザになりすまして侵入するケースや、ログが消去されるなど、侵入した痕跡を残さないようにしたと推測されるケースも発生し、不正なアクセスがあったと気づくのに時間がかかる、又は、気づくのが困難なケースが顕在化している。更に、実際に気づいていないケースも少なからずある可能性も考えられる。

また、社内業務用システムなど、電気通信設備以外の設備におけるシステムに侵入し、又は、それを経由して電気通信設備に侵入するケースや、通信サービスの提供停止に至らない侵入・攻撃によるケースも発生している。これらの狙いは、電気通信設備やその他の設備等の機微情報に関するデータの窃取、又は、大規模通信障害を引き起こす準備等も想定される。

以上については、通信分野のみならず、国内全体又は世界的な課題となっている。例えば、デロイトトーマツグループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020 年版」(令和年 3 月)によると、国内の上場企業の課題として、「サイバー攻撃・ウイルス感染等による情報漏えい」が国内第 3 位・海外第 5 位となり、ともに順位が上昇している。

日本国内			海外拠点	
疫病の蔓延 (パンデミック) 等の発生 (②)	34.4% (24)	第1位	疫病の蔓延 (パンデミック) 等の発生 (②)	39.6% (27)
異常気象 (洪水・暴風など)、大規模な自然災害 (地震・津波・火山爆発・地磁気嵐) (②)	30.9% (1)	第2位	グループガバナンスの不全 (⑦)	18.5% (2)
サイバー攻撃・ウイルス感染等による情報漏えい (⑩)	21.3% (5)	第3位	異常気象 (洪水・暴風など)、大規模な自然災害 (地震・津波・火山爆発・地磁気嵐) (②)	13.5% (5)
人材流失、人材獲得の困難による人材不足 (⑪)	19.5% (2)	第4位 / 第3位	製品/サービスの品質チェック体制の不備 (⑨)	13.5% (3)
製品/サービスの品質チェック体制の不備 (⑨)	15.7% (4)	第5位	サイバー攻撃・ウイルス感染等による情報漏えい (⑩)	11.7% (10)
長時間労働、過労死、メンタルヘルス、ハラスメント等労務問題の発生 (⑪)	12.5% (11)	第6位 / 第5位	人材流失、人材獲得の困難による人材不足 (⑪)	11.7% (6)
事業に影響するテクノロジーの変革 (⑤)	11.7% (-)	第7位	為替変動 (③)	10.4% (8)
グループガバナンスの不全 (⑦)	11.4% (9)	第8位	市場における価格競争 (③)	9.5% (11)
市場における価格競争 (③)	10.8% (7)	第9位	事業に影響するテクノロジーの変革 (⑤)	9.0% (-)
サイバー攻撃・ウイルス感染等による大規模システムダウン (⑩)	10.8% (12)	第9位 / 第10位	従業員の不正・贈収賄等 (⑧)	8.6% (4)

※ () カッコ内は前回順位
 ※ 各項目名に続く () 内の番号は、本調査において設けたリスクおよびクライシスの種類上の分類

【図 2.5.1】日本国内と海外拠点それぞれにおける、優先して着手が必要と思われるリスク (出典:デロイトトーマツグループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020 年版」(2021 年 3 月))

また、世界経済フォーラム(World Economic Forum)「グローバルリスク報告書 2021」(令和3年 1 月)によると、今後 10 年間における最も可能性があり、かつ、影響

の大きいリスクとして、自然災害や新型コロナウイルス感染症等と並び、「Cybersecurity failure」が挙げられている。また、影響の大きいリスクとしては、サイバー攻撃が原因かどうかにかかわらず、「IT Infra breakdown」も挙げられており、我が国としても、国際的な情勢に遅れず、所要の対応を進めることが求められている。

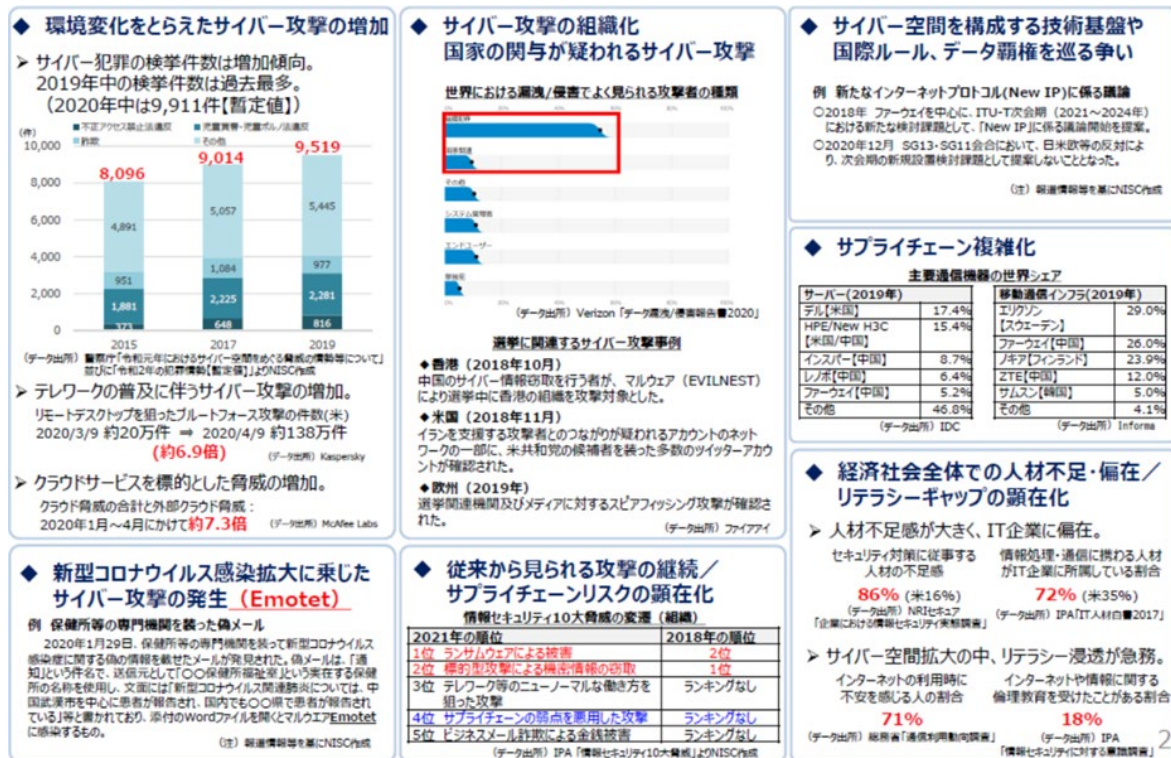


【図 2.5.2】今後 10 年間に於ける最も可能性や影響の大きいリスク

(出典:世界経済フォーラム(World Economic Forum)「グローバルリスク報告書 2021」(令和3年1月))

このような中、政府では、サイバーセキュリティ戦略本部において、サイバーセキュリティ基本法に基づく、次期のサイバーセキュリティ戦略の策定に向けた検討が進められている。その際、環境変化をとらえたサイバー攻撃の増加、サイバー攻撃の組織化、国家の関与が疑われるサイバー攻撃、新型コロナウイルス感染拡大に乗じたサイバー攻撃の発

生、サイバー空間を構成する技術基盤や国際ルール・データ覇権を巡る争い、サプライチェーンの複雑化・サプライチェーンリスクの顕在化等、国際情勢から見たリスクや近年の脅威動向を踏まえつつ、検討が行われている。



近年の主なサイバー攻撃事例

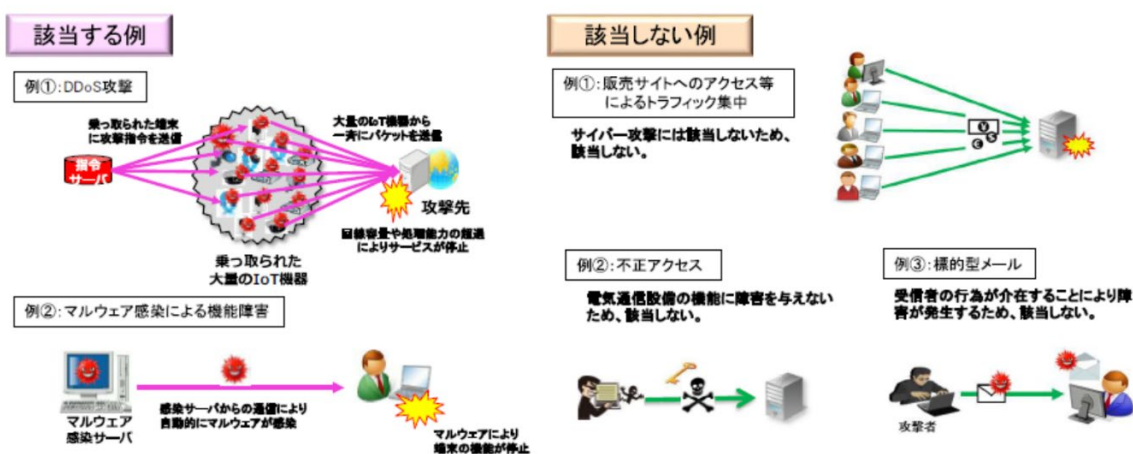
- **暗号資産が不正に送信されたとみられる事案 (2018年1月)**
国内仮想通貨交換業者から約580億円相当の暗号資産 (NEM) が不正に送信されたとみられる事案が発生した。
- **2020年東京大会のチケット抽選に関するフィッシング (2019年7月)**
2020年東京大会のチケット抽選に関係があると見せかけた偽のショートメッセージサービス (SMS) が、スマートフォン利用者に送られているとの報道。誘導先のサイトで米Appleのギフト券の番号を入力させて窃取する仕組み
- **三菱電機への不正アクセスによる個人情報・企業機密等の漏えい (2020年1月)**
三菱電機は、同社のネットワークが第三者による不正アクセスを受け、個人情報や企業機密が外部に流出した可能性があると公表。流出した可能性のある情報に、防衛省の「注意情報」が含まれていたと判明
- **NTTコミュニケーションズへのBYOD端末等を通じた不正アクセス事案 (2020年5月)**
NTTコミュニケーションズは、同社の設備が攻撃者からの不正アクセスを受け、社内に保存されていたファイルが閲覧され、一部の情報が外部に流出した可能性を公表。調査の結果、当初は海外拠点への攻撃及び侵入を起点とした不正アクセスが明らかになったが、その後社内のBYOD端末による不正アクセスも発覚
- **ホンダへのサイバー攻撃 (2020年6月)**
本多技研工業は、各国の拠点のコンピュータがダウンし、工場からの出荷が停止したことを公表。その原因は、ランサムウェアを使った攻撃によるものとみられている。
- **ドコモ口座をはじめとした電子決済サービスを利用した口座振替による不正出金事案 (2020年9月)**
「ドコモ口座」をはじめとした電子決済サービス、ゆうちょ銀行の「mijica」及びSBI証券において、不正アクセスにより、不正送金や顧客資産の流出が発生したが、相次いで発覚
- **慶応義塾大学への不正アクセスによる個人情報漏えい (2020年10月)**
慶応義塾大学は、湘南藤沢キャンパスのネットワークシステム、授業支援システム等に対する不正アクセスにより、利用者の個人情報が漏えいした可能性があると公表
- **カブコンへのサイバー攻撃による個人情報の流出 (2020年10-11月)**
カブコンは、サイバー犯罪グループからランサムウェアによる不正アクセス攻撃を受け、社外の個人情報約39万件が流出した可能性があると公表
- **SolarWinds社製品へのサイバー攻撃 (2020年12月)**
米SolarWinds社は、同社のソフトウェア (orion platform) の脆弱性を悪用した、同ソフトウェアを利用しているシステムへのサイバー攻撃を認識したと公表

【図 2.5.3】環境変化、国際情勢から見たリスク/近年の脅威動向 (出典:「次期サイバーセキュリティ戦略の検討に当たっての基本的な考え方(案)の概要」(サイバーセキュリティ戦略本部(2021年2月9日))

サイバー攻撃を原因とする通信事故について、2018 年度までは、通信事故の報告制度に基づく四半期報告事故における発生要因として、「外的要因」のうち「第三者要因」や「その他」等の中に含まれる形で報告されており、発生状況等を明確に把握できていない状況であった。

そこで、サイバー攻撃のうち、特に通信事業者における電気通信設備の機能に障害を与えるものについては、一定規模以上の通信サービスの提供停止や品質低下による通信事故の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ため、2019 年度から、四半期報告事故における発生要因の分類として、新たに DDoS 攻撃等の「送信型対電気通信設備サイバー攻撃」が追加された。

- 「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。



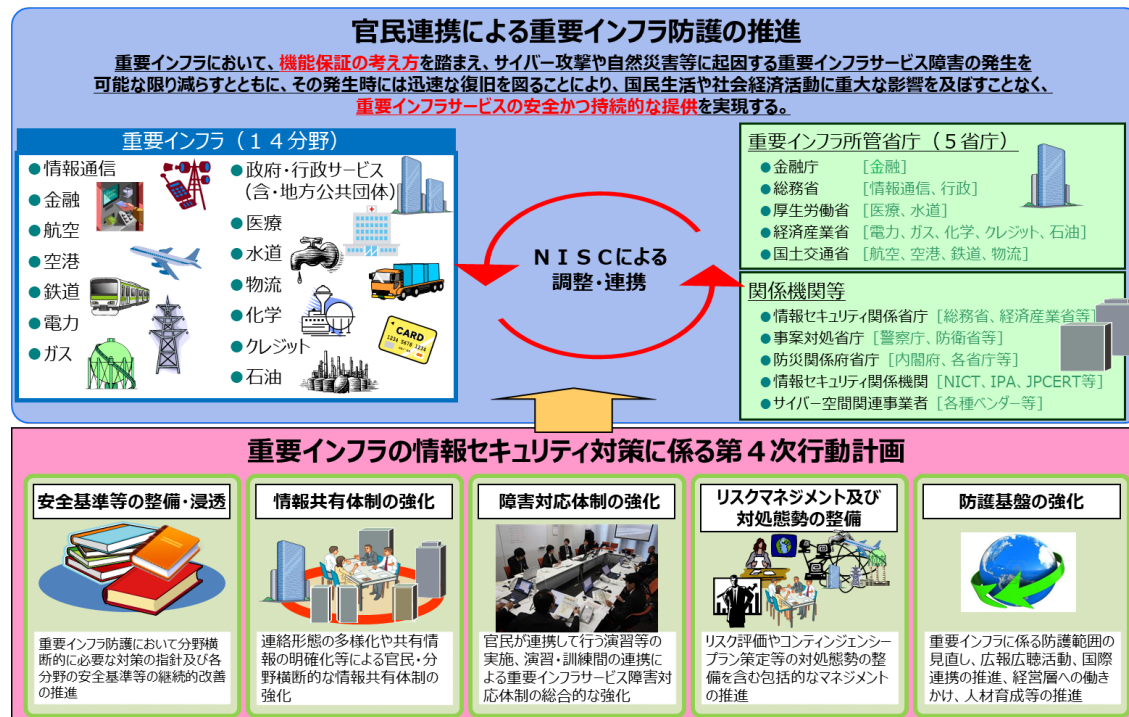
【図 2.5.4】送信型対電気通信設備サイバー攻撃

以上の結果、2019 年度においては、送信型対電気通信設備サイバー攻撃を発生要因とする四半期報告事故が 8 件、また、2020 年度(第3四半期まで)においては、同様に 12 件の報告があり、電気通信設備に対するサイバー攻撃が確認されたところである。しかしながら、これらは、サイバー攻撃の一部であり、電気通信事業者に対するサイバー攻撃全体における氷山の一角にすぎないと考えられる。

通信分野は、「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」(以下、「行動計画」という。)に規定されている通り、「他の重要インフラ分野からの依存度が高く、かつ、比較的短時間の重要インフラサービス障害であってもその影響が大きくなるおそれのある」ものとされている。

上記行動計画の策定時においては、通信事業者等の重要インフラ事業者等の行動規範として、自主的に見直しの必要性を判断して改善できるサイクル自体は浸透しつつあるが、PDCAのうち、C(確認)とA(是正)については、十分に定着していないという課題や、情報系(IT)のみならず、通信ネットワーク等の制御系(OT)を含めた情報共有の質・量の改善等が課題として挙げられている。

1. 本行動計画のポイント ◆重要インフラサービスを、 安全かつ持続的に提供 できるよう、自然災害やサイバー攻撃等に起因する 重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能 となるよう、 経営層の積極的な関与 の下、情報セキュリティ対策に関する取組を推進。 (機能保証の考え方) ◆また、取組を通じ、 オリパラ大会に関係する重要なサービスの安全かつ持続的な提供 も図る。		
2. 重要インフラの情報セキュリティ対策の現状と課題 ◆第3次行動計画に基づく施策群により、 自主的な取組が浸透 しつつあるが、PDCAのうちC Aに課題。一部で 先導的な取組 も進展。 ◆機能保証のため、情報系(IT)に限らず、 制御系(OT)を含めた情報共有の質・量の改善 や、重要インフラサービス障害に備えた 対処態勢の整備 が必要。 ◆国内外の多様な主体との連携、情報収集・分析に基づく 国民への適切な発信 の継続・改善が必要。		
3. 本行動計画の3つの重点 次の3つを重点として、第3次行動計画の5つの施策群の補強・改善を図る。		
① 先導的取組の推進(クラス分け) ■他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野(例：電力、通信、金融)において、一部事業者における先導的な取組(I S A C※)の設置やリスクマネジメントの確立等を強化・推進 <small>※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織</small> ■上記先導的な取組の、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化	② オリパラ大会も見据えた情報共有体制の強化 ■サービス障害の深刻度判断基準の導入に向けた検討 ■連絡形態の多様化(連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由)による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討 <small>※重要インフラ事業者等の情報共有を担う組織</small> ■ホットライン構築も可能な情報共有システムの整備(自動化、省力化、迅速化、確実化) ■情報連絡・情報提供の範囲にOT、IoT等を含むことを明確化(I T障害→重要インフラサービス障害) ■演習の改善、演習成果の浸透による防護能力の維持・向上 ■サプライチェーンを含む「面としての防護」に向け範囲の拡大	③ リスクマネジメントを踏まえた対処態勢整備の推進 ■「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透 ■事業継続計画及び緊急時対応計画(コンティンジェンシープラン)の策定等による重要インフラ事業者等の対処態勢の整備 ■事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化
4. 本行動計画の期間 ▶ 第4次行動計画はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。		



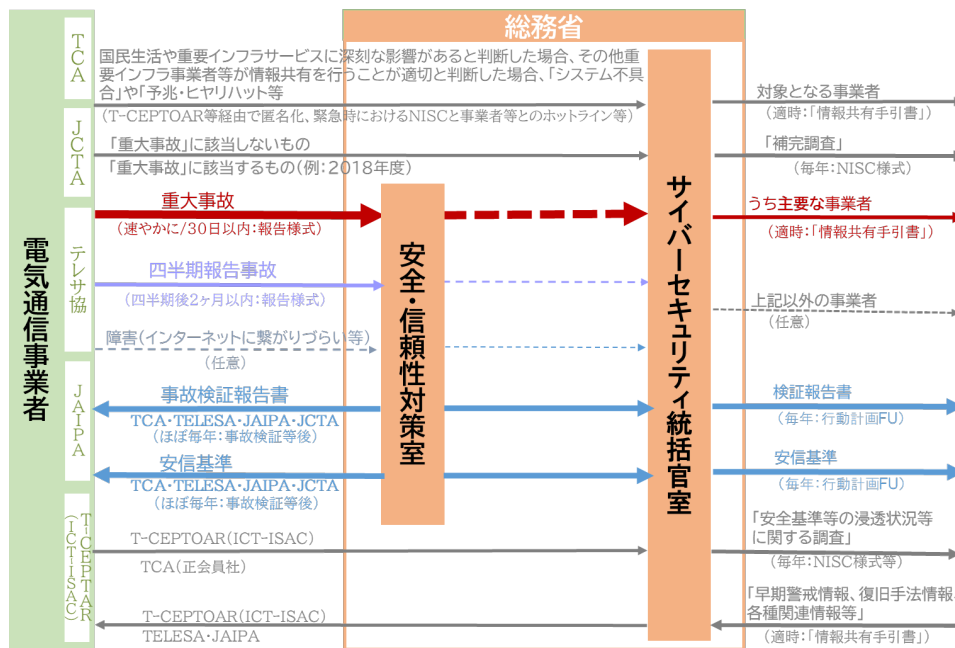
【図 2.5.5】「重要インフラの情報セキュリティ対策に係る第4次行動計画」の概要

また、「IoT・5G セキュリティ総合対策 2020」(2020年7月総務省)においても、「サイバー攻撃を起因とする電気通信事故に関する情報、それらの情報を踏まえた再発防止に向けた教訓等及び情報通信ネットワーク安全・信頼性基準等に関する内閣官房内閣サイバーセキュリティセンターや電気通信事業者との間の情報共有の在り方等、情報通信ネットワークの安全・信頼性対策とサイバーセキュリティ対策との更なる連携強化を図ることが期待される」と規定されている。

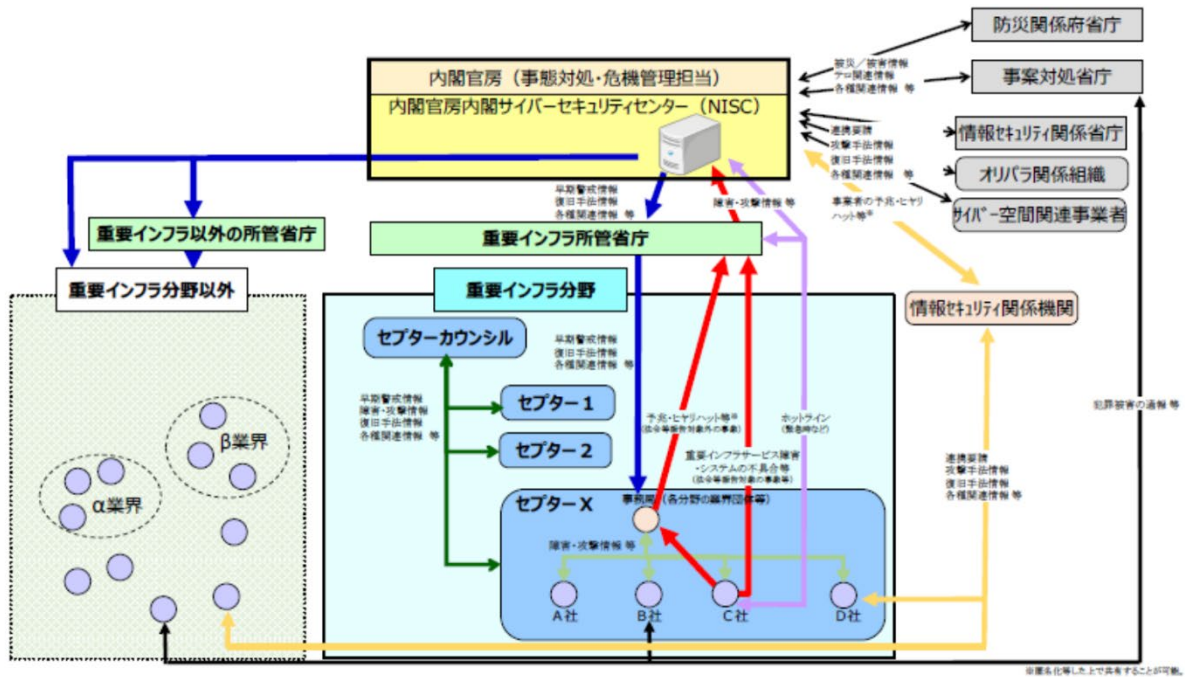
この点、通信事故の報告制度において、サイバー攻撃を原因とする通信事故については、四半期報告事故のうち、電気通信設備の故障によるもののみが対象となっている。また、上記行動計画に基づき、サイバー攻撃を原因とするか否かにかかわらず、重大事故のうち主要な通信事業者に関するものが、総務省から内閣サイバーセキュリティセンター(以下、「NISC」という。)に情報共有されている。

また、重大事故及び四半期報告事故については、電気通信事故検証会議による教訓等の整理、通信サービス・ネットワークの安全・信頼性対策に関する推奨基準である「情報通信ネットワーク安全・信頼性基準」(総務省告示)の改正、それらの通信事業者関係団体((一社)電気通信事業者協会(以下、「TCA」という。))、(一社)テレコムサービス協会、(一社)日本インターネットプロバイダー協会(以下、「JAIPA」という。))、(一社)日本ケーブルテレビ連盟)との共有等によるPDCAサイクルが実施されている。

他方、NISC においても、通信分野((一社)ICT-ISAC、TCA)を含む重要インフラ事業者等における安全基準等の浸透状況の把握、行動計画等の検証や良好事例の収集等のため、「安全基準等の浸透状況等に関する調査」が実施されている。この点、これらの目的は共通しているが、対象となる関係団体が異なる状況等となっている。



【図 2.5.6】 サイバー攻撃に関する電気通信事故の報告制度等の現状



【図 2.5.7】「重要インフラの情報セキュリティ対策に係る第4次行動計画」情報共有体制

2021年3月末日現在

重要インフラ分野	情報通信			金融				航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油	
	電気通信	放送	銀行等	証券	生命保険	損害保険	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油		
名称	T-CEPTOAR	ケーブルテレビ CEPTOAR	放送 CEPTOAR	金融CEPTOAR連絡協議会				CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	GAS CEPTOAR	自治体	医療	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR	CEPTOAR
事務局	(一社) ICT-ISAC	(一社) 日本ケーブルテレビ連盟	(一社) 日本民間放送連盟	(一社) 全国銀行協会	日本証券業協会	(一社) 生命保険協会	(一社) 日本損害保険協会	定期航空協会	空港・空港ビル協議会	(一社) 日本鉄道電気技術協会	電力ISAC	(一社) 日本ガス協会	地方公共団体情報システム機構	(公社) 日本医師会	(公社) 日本水道協会	(一社) 日本物流団体連合会	石油化学工業協会	(一社) 日本クレジット協会	石油連盟	
構成員 (0名)	23社 1団体	311社 1団体	195社・ 1団体	1,324社	201社 7機関	42社	47社	14社 1団体	8社	22社 1団体	24社 3機関	10社・ 1団体	47 都道府県 1,741 市区町村	1グループ 20機関	8水道 事業体	6団体 17社	13社	51社	11社	
NISCからの情報の提供先(構成員以外)	395社・ 1団体	394社	11社	2社・ 1団体	-	-	-	-	-	-	14社・ 1機関	166社・ 1団体	-	391社・ 1団体	内閣に 1,324事業 体へ開示	-	-	-	-	

■ その他
 既存事業領域を越える連携等
 情報通信 (ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟)、金融 (金融ISACにおいて、加盟金融機関間で情報共有・活動連携)、航空・空港・鉄道・物流 (交通ISACにおいて、参加事業者間で情報共有・活動連携)、電力 (電力ISACにおいて、加入する電気事業者間で情報共有・活動連携)、化学 (石油化学工業協会と日本化学工業協会の情報共有・活動連携)、クレジット (ネットワーク事業者と情報共有・活動連携)、制御システム (JPCERT/CCが提供するConPaS等)、J-CSIP (IPA: 標的型攻撃等に関する情報共有)、サイバーテロ対策協議会 (重要インフラ事業者等と警察との間で連携、47都道府県に設置)、早期警戒情報CISTA (JPCERT/CC: セキュリティ情報全般)

【図 2.5.8】セプター(CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response)

以上の通り、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通信事故の報告・検証制度等の在り方が課題となっている。

(2)考え方

①サイバー攻撃を原因とする通信事故等に関する報告制度の在り方

通信事故の報告制度において、サイバー攻撃を原因とする事故については、2019年度より、四半期報告事故の発生原因の分類の1つとして、送信型対電気通信設備サイバー攻撃が新たに追加されている。

他方、同じ四半期報告事故の対象とされている、電気通信設備以外の設備(利用者登録システムや社内の業務管理用システム等)の故障により通信サービスの提供に支障を来した事故や、電気通信設備に関する情報(電気通信設備であるサーバのログインIDやパスワード等)の漏えいにより通信サービスの提供に支障を及ぼすおそれがあるインシデントについては、それらの発生原因として、サイバー攻撃か否かを明記することが求められていない。

電気通信設備以外の設備を経由等した電気通信設備に対するサイバー攻撃、前述のような電気通信設備に関する情報の窃取や当該情報の滅失・毀損等によるサイバー攻撃⁸等による通信サービスに対する影響等を総合的に把握するため、これらの事故及びインシデントについても、今後、発生要因がサイバー攻撃である場合はその旨明記することが適当である。

また、重大事故についても、その詳細な報告様式において、その発生原因が送信型対電気通信設備サイバー攻撃であるか否か等を記載することが事故 GL において明確にされていない。従って、重大事故の原因がサイバー攻撃である場合については、当該様式における報告事項として、それに関する内容を記載することを明記することが適当である。この点につき、重大インシデントの報告制度においても、同様と考えられる。

他方、通信事故やインシデントの発生原因として、それがサイバー攻撃か否かは容易に確認できない場合がある。例えば、何か不審な通信があっただけではサイバー攻撃かどうか、同攻撃があったとして情報の漏えいかどうかの確認には時間がかかる場合がある。そのため、重大事故や重大インシデントの場合における詳細報告の期限に関し、事故等の発生から30日以内の報告が難しい場合については、柔軟な期限設定とすることが適当である。

以上の参考として、例えば、改正個人情報保護法により義務化された個人データの漏えい等の報告に関する「個人情報保護法ガイドライン(通則編)の一部を改正する告示(案)」においては、基本的には、個人データの漏えい等が発生し、又は発生したおそれがある事態等を知った日から30日以内に確報が必要とされているところ、サイバー攻撃

⁸ 例えば、個人情報ガイドラインにおいては、「不正アクセスにより個人データが漏えいした場合」や「ランサムウェア等により個人データが暗号化され、復元できなくなった場合」等が事例として挙げられている。

等の「不正の目的をもって行われたおそれがある」場合については、確報について60日以内という柔軟な報告期限の設定や、当該時点において、「合理的努力を尽くした上で、一部の事項が判明しておらず、全ての事項を報告できない場合には、その時点で把握している内容を報告し、判明次第、報告を追完する」こと等の特例が設けられている。

②サイバー攻撃を原因とする通信事故等に関する検証制度の在り方

サイバー攻撃を原因とする通信事故やインシデントのうち、社会的な影響の大きい重大事故又は重大インシデントについては、報告制度等を通じた通信事業者、総務省やNISC等の専門機関における即応連携によるOODAループ的な対応に加え、前述した第三者機関によるリスクアセスメントの対象とすることも必要であると考えられる。

重大事故等については、サイバー攻撃による被害者となる通信事業者等をできる限り増やさず、将来における通信事故の防止や被害の拡大防止等が今後益々必要になると考えられる。また、巧妙化・悪質化するサイバー攻撃のように、形式知化されていない未知(想定外)等のリスクについては、マルチステークホルダー間で見える化・共有することにより、それらの関係者において、安心・安全で信頼できる通信サービス・ネットワークにおけるリスクの量的・質的な変化やマルチステークホルダーへの拡散への対策を最適化することを促すための仕組みが一層必要になってきている。

この点、サイバーセキュリティ戦略本部で検討されている「次期サイバーセキュリティ戦略 骨子」(令和3年5月13日第28回会合)においても、次の通りとされている。

- サイバー空間の脅威の増大、脆弱性の顕在化、安全保障環境の変化等、不確実性を増す環境下で、サイバー空間においても、公共空間として実空間と変わらぬ安全・安心を確保していくため、攻撃者との非対称な状況を看過せず、それぞれの観点について深化・強化し、その環境・原因の改善に正面から取り組んでいくことが求められている。
- また、それに伴いサイバー空間に関わるあらゆる主体の役割が増しており、自律的な取組(「自助」)や多様な主体の緊密連携(「共助」)は引き続き重要であるが、その上で、それらの基盤となる「公助」の役割をはじめ、各主体の役割や防御すべき対象を不断に検証し、多層的な取組を強化する。
- 「任務保証」は今後も重要であり引き続き推し進めるとともに、これを深化させ、あらゆる組織が、サイバー空間を提供・構成する主体として、自らが遂行すべき業務やサービスからエンドユーザに至るバリューチェーン全体の信頼確保を「任務」と捉えることで、サイバー空間を構成する多様な製品・サービスについて、その安全性・信頼性が確保され、利用者が継続的に安心して利用できる環境をめざす。

- 組織化・洗練化されたサイバー攻撃の脅威の増大等がみられる中で、国として、各国政府・民間等様々なレベルで連携をしつつ、個々の主体による「リスクマネジメント」を補完し、一層実効的に取組を強化する。具体的には、我が国として、サイバー攻撃に対して能動的に防御するとともに、脅威の趨勢を踏まえ、常に想定されるリスク等の見直しや事後追跡可能性の確保に努める。

サイバー攻撃については、それが意図的な行為であるとともに、国家レベルの関与による巧妙化・悪質化等、高度かつ特殊な場合も想定される。従って、第三者機関において、サイバー攻撃を原因とする通信事故等に関する原因究明調査やリスクアセスメントを行うことにより、NISC やサイバーセキュリティに関する研究機関や専門家等との連携・協力を通じて、マルチステークホルダーにおけるリスクへの対応が推進されるための政策的 PDCA サイクルを構築し、リスクマネジメントを強化していくことが重要であると考えられる。

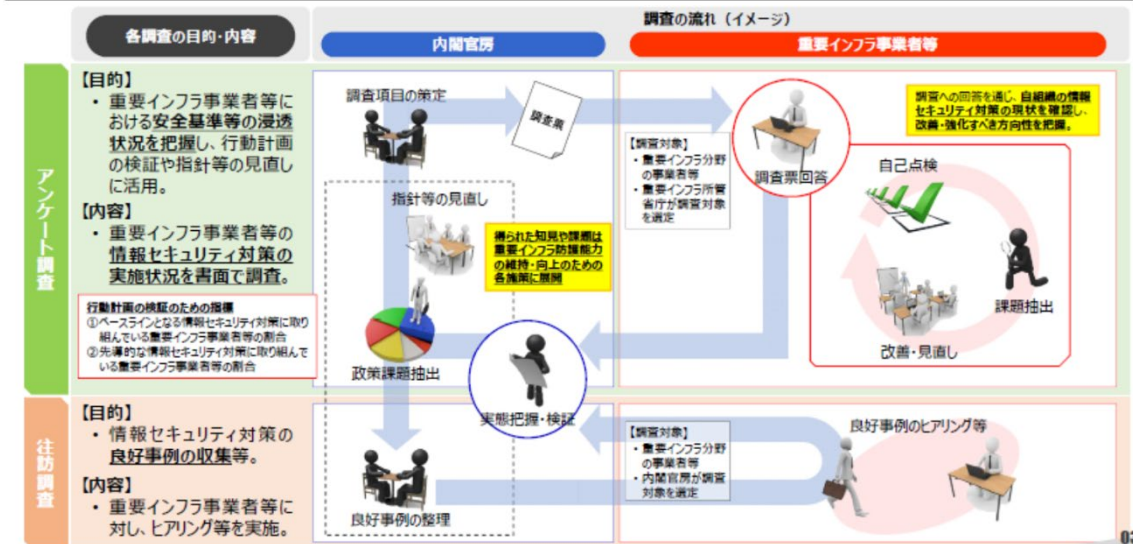
③関係機関との情報共有等連携の在り方

通信事故等に関する NISC との情報共有について、主要な通信事業者であるか否かにかかわらず、通信事故やインシデントのうち、通信分野における重要インフラサービス障害に関係するものに加え、関係省庁等による即応連携の必要性が高いと考えられる他の重要インフラに影響を及ぼす事故等とすることが適当である。

また、総務省における通信事故の報告・検証制度等による PDCA サイクルと、NISC における「安全基準等の浸透状況等に関する調査」等による PDCA サイクルに関し、通信分野については、対象となる通信事業者における負担の軽減にも配慮する観点から、それらの対象となる関係事業者団体の共通化等により、連携を強化することが適当である。

更に、通信事故に該当しないインターネットにつながりづらい障害等については、重大事故及び重大インシデントに関する OODA ループ的な対応を充実させる観点から、ICT-ISAC における観測や情報共有の仕組み等との連携・協力も引続き重要と考えられる。

- 「重要インフラの情報セキュリティ対策に係る第4次行動計画」（以下「行動計画」という。）では、各重要インフラ分野に共通して求められる情報セキュリティ対策を「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（以下「指針」という。）として取りまとめ、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から「安全基準等」^(注)で規定されることが望ましい項目を整理している。
 - 内閣官房は、重要インフラ事業者等における安全基準等の浸透状況等を把握するため、重要インフラ事業者等に対し、情報セキュリティ対策の実施状況について「アンケート調査」及び「往訪調査」を実施している。
- (注) 各重要インフラ事業者等の判断や行為の基準となる基準又は参考となる文書類であり、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく事業者等が自ら定める「内規」等が含まれる。



【出典】「重要インフラ分野における安全基準等の浸透状況等に関する調査について[2019年度]」（2020年7月13日内閣サイバーセキュリティセンター-重要インフラグループ）
<https://www.nisc.go.jp/active/infra/pdf/shintou19.pdf>

【図 2.5.9】安全基準等の浸透状況等に関する調査

(3)対応の方向性

サイバー攻撃を原因とする通信事故の報告・検証制度については、総務省において、サイバーセキュリティ基本法や行動計画等に基づく枠組みとの連携・協力を一層推進するため、次の所要の制度整備等を行うことが適当である。

- ① 電気通信設備以外の設備の故障に関する四半期報告事故の報告制度について、発生要因の1つとしてサイバー攻撃の追加
- ② サイバー攻撃を原因とする重大事故の報告制度について、詳細報告に関する柔軟な提出期限の設定や事故 GL の明確化
- ③ サイバー攻撃を原因とするインシデントについて、上記①②と同様の措置等を含むインシデントに関する新たな報告制度の整備
- ④ 通信事故やインシデントの報告制度について、NISC や ICT-ISAC 等の関係機関との情報共有等による即応連携・協力の推進
- ⑤ 重大事故等に関するリスクアセスメントについて、NISC や ICT-ISAC 等の関係機関との連携・協力を推進するための体制等の整備

第3章 今後の対応

3.1 今後の制度整備等に向けて

本中間報告では、電気通信事故検証会議が開催され始めた 2015 年度以降における様々な環境変化に伴い、通信サービス・ネットワークの安全・信頼性対策に関する PDCA サイクルが取扱うリスクが多様化・複雑化し、マルチステークホルダーに拡散していること等から、「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」について検討を行った。

具体的には、検討事項のうち、①重要インフラに提供される通信サービス・ネットワークの通信事故に関する報告制度の在り方、②インシデントに関する報告制度の在り方、③電気通信事故検証会議の機能強化による第三者機関の在り方、④これらを踏まえた自然災害やサイバー攻撃を原因とする通信事故に関する報告制度等の在り方について議論を行った。

本中間報告で示した対応の方向性に基づき、総務省においては、所要の制度整備等を速やかに進めることで、2020 年代半ば頃に向けて、デジタル社会における安心・安全で信頼できる通信サービス・ネットワークの確保のため、通信事業者が引続き主導的な役割を担うことができる環境を整備することが適当である。

以上の環境整備により、総務省及び通信事業者において、重大事故や重大インシデント等の重大なリスクに対し、サイバー攻撃、大規模自然災害やその他の原因に応じて、利用者への周知・情報提供も含め、マルチステークホルダーとの情報共有等の適時適切な即応連携による OODA ループ的な対応が強化されることを期待する。

また、電気通信事故検証会議の機能強化による第三者機関において、重大事故等の原因究明やリスクアセスメント、それらの結果をふまえたリスクコミュニケーション等を通じ、マルチステークホルダーにおけるリスクマネジメントを推進するとともに、重大事故や重大インシデント等の報告制度の在り方を含め、持続的な改善に向けた PDCA サイクルの実効性・強靱性が確保されることを期待する。

OODA ループ的な対応及び PDCA サイクルが取組むリスクについては、国内外の環境変化等により今後も引続き変化し続けていくと考えられる。それらの状況等を踏まえつつ、総務省においては、以上の環境整備以降も不断に見直し検討を行い、必要な対応を実施することが重要である。

3.2 引続きの検討課題に向けて

今後は、残された次の検討課題等について、本夏以降、引続き本タスクフォースにおいて、関係事業者等からヒアリングしつつ、検討を行う。

- ① 外国企業等による提供も含めた、テレワーク・遠隔学習等向けのインターネット関連サービス等の通信事故に関する報告基準の在り方
- ② データ伝送サービス(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の在り方
- ③ 通信事故に該当しない、インターネットにつながりづらい障害に対するSNSの活用等による対応の在り方

なお、以上の検討にあたっては、以下の状況等を踏まえつつ、検討することとする。

- ① 改正電気通信事業法(2021年4月施行)に基づく外国企業等からの通信事業者等に関する届出等の状況
- ② 「ブロードバンド基盤の在り方に関する研究会」(総務省において2020年4月より開催)によるブロードバンドサービスのユニバーサルサービス化の検討状況
- ③ 「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ワーキンググループ」(総務省において2020年12月より開催)による同サービスの品質計測手法の検討状況

別表1 事故報告・検証制度等タスクフォース 構成員

(令和3年4月12日現在 敬称略、主任を除き50音順)

	氏名	主要現職
主任	内田 真人	早稲田大学 理工学術院 教授
	石田 幸枝	(公社)全国消費生活相談員協会 理事
	井ノ口 宗成	富山大学 都市デザイン学部 都市・交通デザイン学科 准教授
	落合 孝文	渥美坂井法律事務所・外国共同事業 弁護士
	喜安 明彦	(一社)電気通信事業者協会 安全・信頼性協議会 会長
	熊取谷 研司	(一社)日本ケーブルテレビ連盟 技術部長
	高口 鉄平	静岡大学学術院 情報学領域 教授
	実積 寿也	中央大学 総合政策学部 教授
	蔦 大輔	森・濱田松本法律事務所 弁護士
	中尾 彰宏	東京大学大学院 工学系研究科 教授
主任代理	林 秀弥	名古屋大学大学院 法学研究科 教授
	引地 信寛	(一社)ICT-ISAC 事務局長
	福智 道一	(一社)日本インターネットプロバイダー協会 理事
	向山 友也	(一社)テレコムサービス協会 技術・サービス委員会 副委員長
	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