資料69-５

令和２年度
電気通信事故に関する検証報告

【概要】

令和３年９月

電気通信事故検証会議
事務局

「令和２年度電気通信事故に関する検証報告」の構成

【第１章 令和２年度検証案件の概要】

１～２．電気通信事故発生概況、経年変化の分析（直近５年間の傾向）

○電気通信事故報告件数、影響利用者数及び継続時間別 、サービス別、発生要因別、故障設備別

３．重大な事故等の発生状況

【第２章 令和２年度に発生した事故から得られた教訓等】

１．事故の事前防止の在り方（８項目）

①手順書の遵守の徹底、②適切な機器の構成の検討、③復旧手順書の作成、④復旧措置の自動化、⑤データ作成時の誤り防止の措置、⑥網羅的な試験の実施、⑦組織外の関係者との連携、⑧複数段のフェイルオーバーの仕組みの検討

２．事故発生時の対応の在り方（３項目）

①事故発生に関する適時適切な連絡や周知等の徹底、②障害発生時の責任者等への確認、③速やかな利用者への情報提供

３．事故収束後のフォローアップの在り方（１項目）

①教育・訓練の徹底

【第３章 事故防止に向けたその他の取組み】

１．災害時における通信サービスの確保の在り方について

２．昨今の重要インフラ事業者に対するサイバー攻撃の事例について

３．令和時代における事故報告・検証の在り方について

電気通信事故発生概況

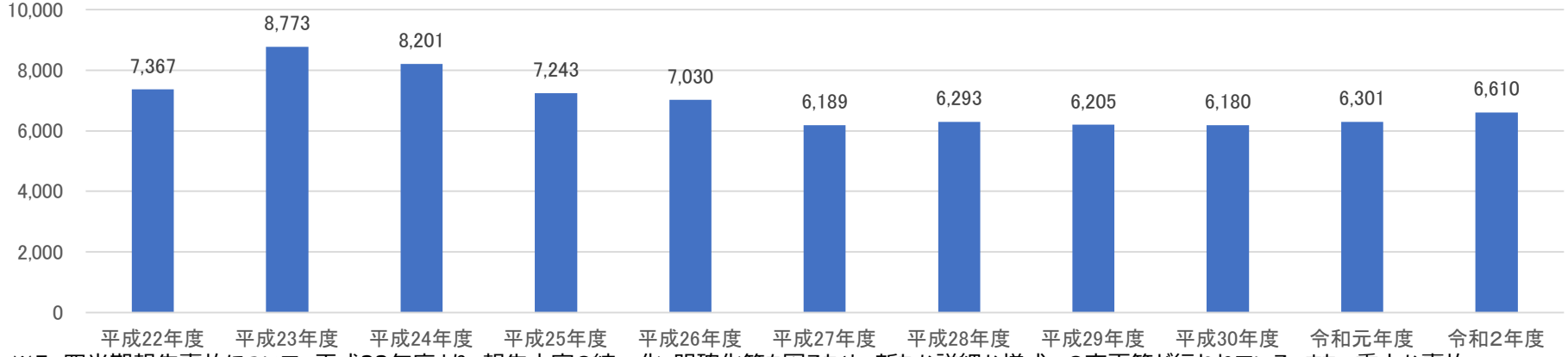
■令和２年度に報告された電気通信事故

（括弧内は前年度（令和元年度）の数値）

	報告事業者数	報告件数
重大な事故	4社　（5社※1）	4件　（3件）
四半期報告事故		
詳細な様式による報告※3	129社　（111社）	6,610件※2（6,301件※2）
簡易な様式による報告※4	33社　（24社）	55,000件　（58,211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。

電気通信事故の影響利用者数及び継続時間

■令和２年度において、**電気通信事故は6,610件**発生。影響利用者数**500人未満の事故が全体の９割以上**を占めており、継続時間**２時間以上５時間未満の事故が全体の半数**を占めている。**12時間以上の事故は全体の26%程度**。

継続時間＼利用者数	500人未満	500人以上 5千人未満	5千人以上 3万未満	3万以上 10万未満	10万以上 100万未満	100万以上	計
30分未満	四半期報告対象外			11	10	2	23 (0.3%)
30以上 1時間未満				2	2	2	6 (0.1%)
1時間以上 1時間30分未満				※1 3	※2 4	0	7 (0.1%)
1時間30分以上 2時間未満				0	5	0	5 (0.1%)
2時間以上 5時間未満	2,982	299	36	※5 1	5	0	3,223 (50.3%)
5時間以上 12時間未満	1,458	47	11	0	1	1	1,518 (23%)
12時間以上 24時間未満	965	16	9	※3 0	0	0	990 (15%)
24時間以上	711	16	9	1	※4 1	0	738 (11.2%)
計	6,116 (92.5%)	378 (5.7%)	65 (1%)	18 (0.3%)	28 (0.5%)	5 (0.1%)	6,610 (100.0%)

■色塗り部分のうち、次の要件に当てはまる場合に、重大な事故に該当。

※１　**緊急通報を取り扱う音声伝送役務**：継続時間**１時間**以上**かつ**影響利用者数**３万**以上のもの

※２　**緊急通報を取り扱わない音声伝送役務**：継続時間**２時間**以上**かつ**影響利用者数**３万**以上のもの　又は　継続時間**１時間**以上**かつ**影響利用者数**１０万**以上のもの

※３　**セルラーLPWA及びアンライセンスLPWAサービス**：継続時間**１２時間**以上**かつ**影響利用者数**３万**以上のもの　又は　継続時間**２時間**以上**かつ**影響利用者数**１０万**以上のもの

※４　**利用者から電気通信役務の提供の対価としての料金の支払を受けないインターネット関連サービス（音声伝送役務を除く）**：
継続時間**２４時間**以上**かつ**影響利用者数**１０万**以上のもの　又は　継続時間**１２時間**以上**かつ**影響利用者数**１００万**以上のもの

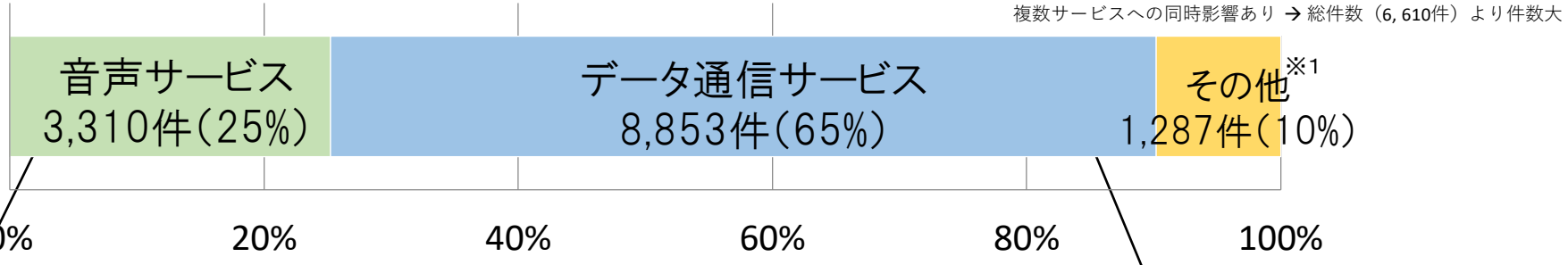
※５　**１から４までに掲げる電気通信役務以外の電気通信役務**：継続時間**２時間**以上**かつ**影響利用者数**３万**以上のもの　又は　継続時間**１時間**以上**かつ**影響利用者数**１００万**以上のもの

注１：色塗り部分には、電気通信設備以外の設備の故障による事故等が含まれており、重大な事故の件数と一致しない。

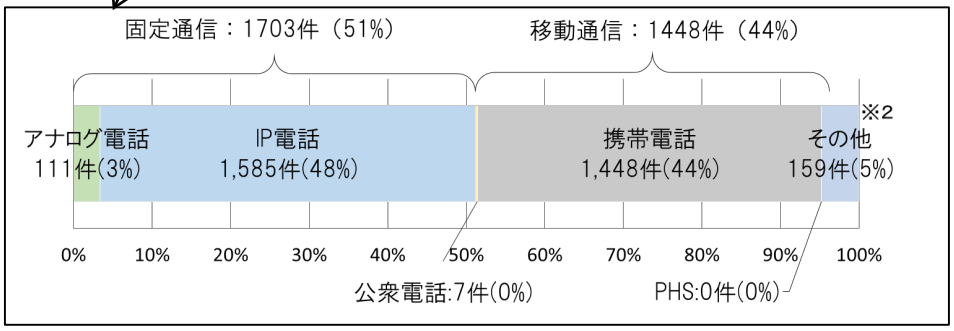
注２：同一要因の事故であっても、事業者毎にカウントしている。

サービス別

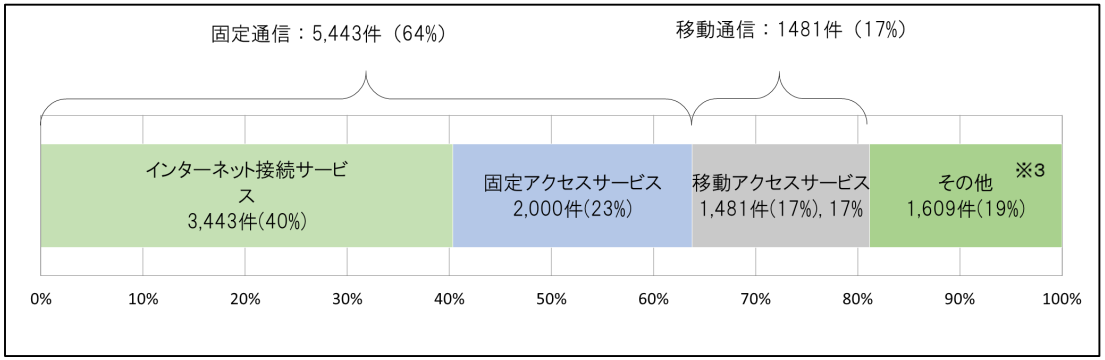
■データ通信サービスの事故が最も多く、8,853件（65%）、次いで音声サービスの3,310件（25%）となっている。
■データ通信サービスの事故の内訳は、インターネット通信サービスが最も多く3,443件（40%）となっている。
■音声サービスの内訳は、IP電話が1,585件（48%）、携帯電話が1,448件（44%）となっており、全体の92%を占める一方で、アナログ電話の件数は年々減少しており、111件（3%）となっている。



・音声サービス　：アナログ電話、IP電話、携帯電話、PHS、国際電話　等
・データ通信サービス　：インターネット接続サービス、固定アクセスサービス（FTTH、DSL、CATV）、移動アクセスサービス（携帯電話・PHS、公衆無線LAN等）等
・その他(※1)　：ISDN、専用役務、MVNO、電報　等



・ その他(※2)：国際電話、FMCサービス　等

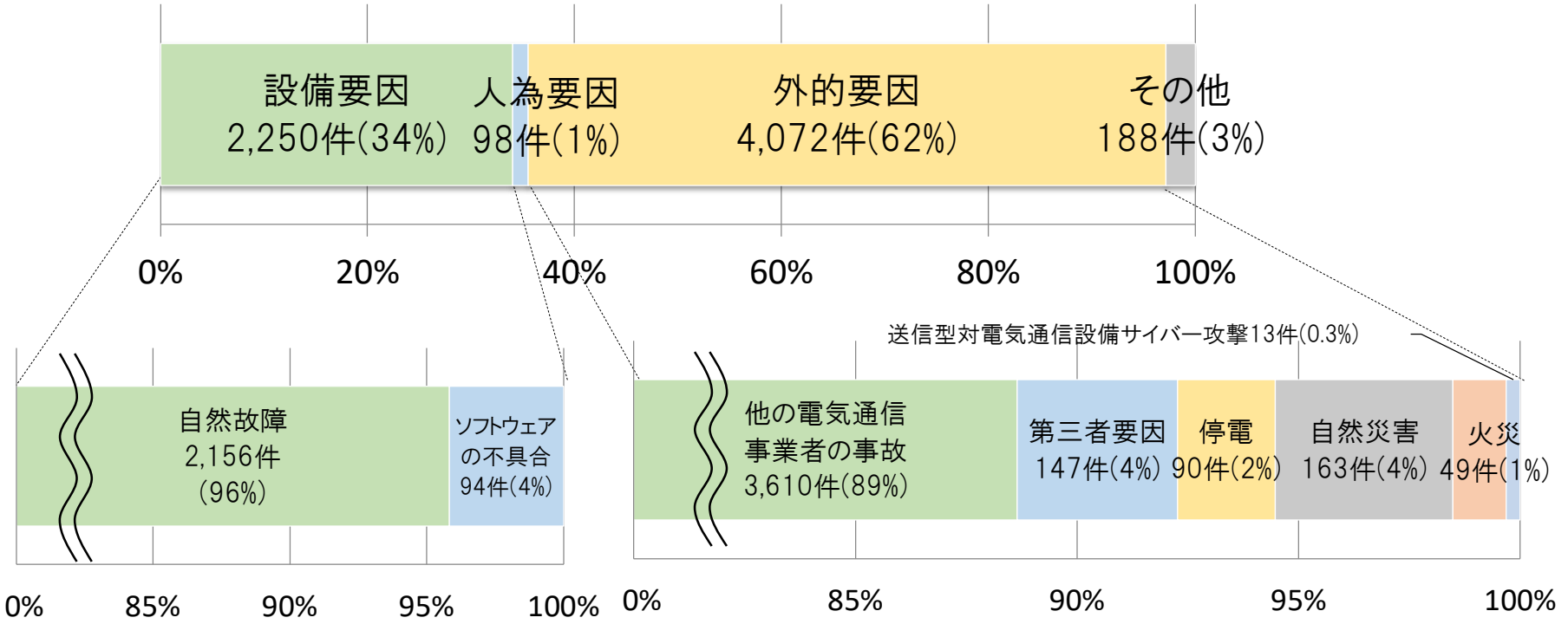


・ その他(※3)：インターネット関連サービス
（電子メールサービス等）、
IP-VPNサービス、
広域イーサネットサービス、
ローカル5Gサービス、
LPWAサービス　等

発生要因別

■自社以外の要因（外的要因）が最も多く4,072件（62%）となっており、そのうち、他の電気通信事業者の事故が3,610件（89%）となっている。
■次いで多くなっているのが設備要因の事故で2,250件（34%）となっており、その内の2,156件（96%）が自然故障によるものである。

※１件の事故で複数の発生要因がある場合であっても、主たる発生要因のみで集計している

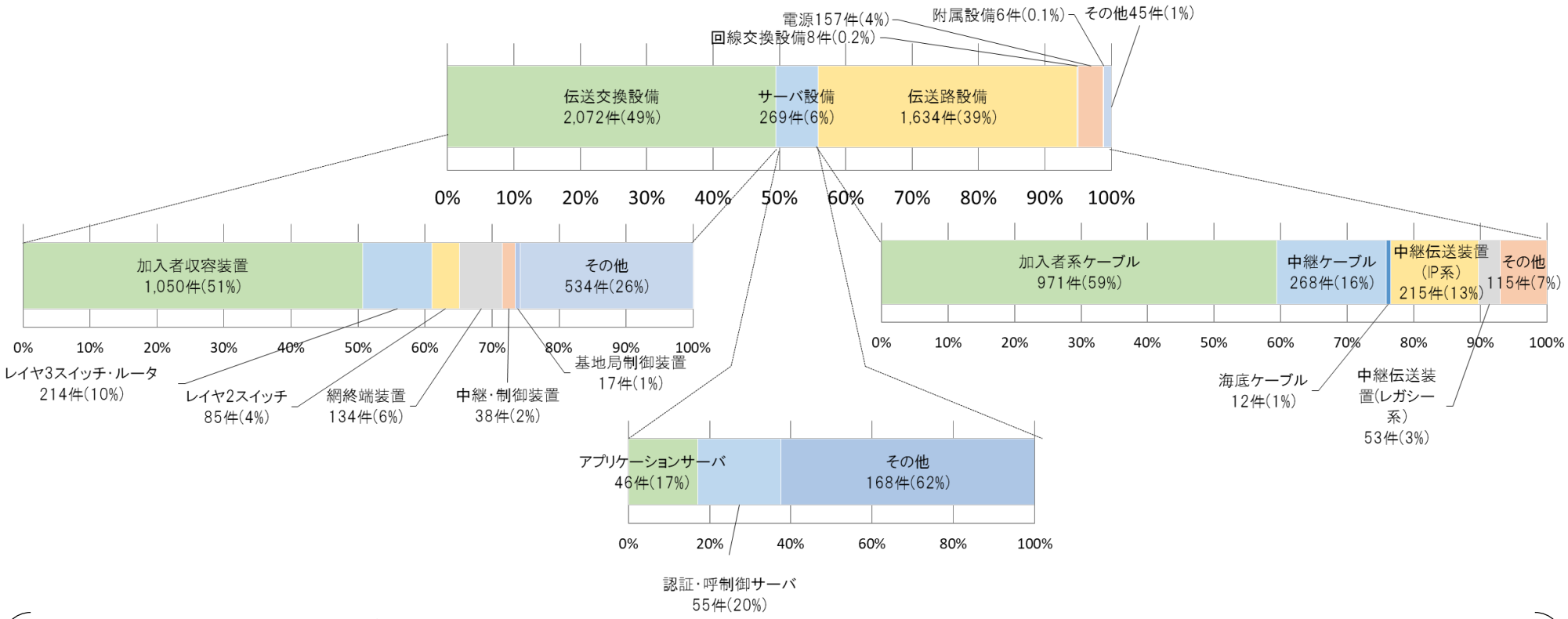


・設備要因：自然故障（機器の動作不良、経年劣化等）、ソフトウェア不具合等の、主に設備的な要因により発生した事故
・人為要因：工事時の作業ミスや、機器の設定誤り等の、主に人為的な要因により発生した事故
・外的要因：他の電気通信事業者の設備障害等による自己の電気通信役務の提供の停止又は品質の低下、道路工事・車両等によるケーブル切断等の第三者要因、停電、自然災害、火災、送信型対電気通信設備サイバー攻撃を要因とする、主に当該電気通信事業者以外の要因により発生した事故
・その他　：異常トラヒックによる輻輳、要因不明等

故障設備別

■全体の半数が伝送交換設備に起因する事故であり、そのうちの約半数が加入者収容装置の事故である。
■伝送路設備の事故は全体の39%であり、その内の約４分の３がケーブルの損傷によるものである。

※事故の総件数（6,610件）のうち、発生要因が「他の電気通信事業者の事故による要因」等のために、 故障設備が不明な事故（54件）を除いたもの。



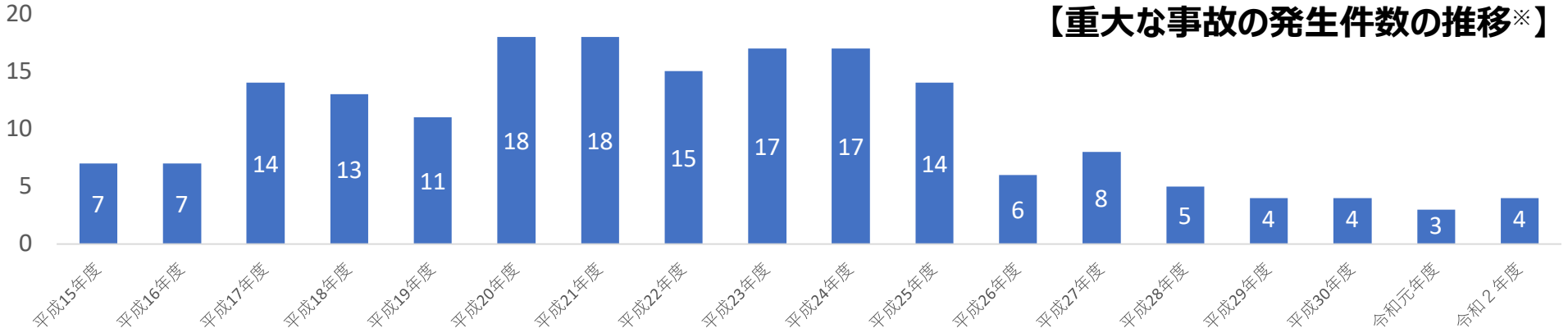
・伝送交換設備：加入者収容装置（加入者収容局などに設置する装置で、ユーザへの通信回線を提供するとともに、通信回線を集約し上位の伝送装置へ出力する機能をもつ装置）、ネットワーク機器、回線交換設備、網終端装置、停電による複数設備の障害等
・サーバ設備　：アプリケーションサーバ（メールサーバ、Webサーバ、DNSサーバ等）
認証・呼制御サーバ（加入者認証、サービス認証、呼制御等を行うサーバ等）
・伝送路設備　：加入者系ケーブル、中継系ケーブル、海底ケーブル、中継伝送装置、WDM（波長分割多重）装置、メディアコンバータ、停電による複数設備の障害等

重大な事故の発生状況

■ 令和２年度において、**重大な事故は４件**発生。直近５年間では３～５件の間で推移している

■ ４件発生した重大な事故のうち、１件は音声サービス（IP電話）の事故、３件はデータ通信サービス（携帯電話１件、インターネット関連サービス（電子メール） ２件）の事故となっている。

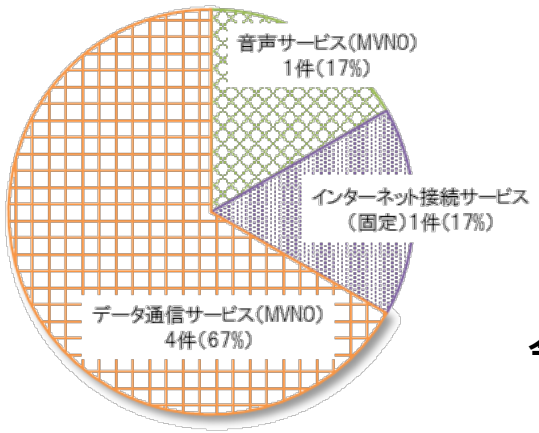
【重大な事故の発生件数の推移※】



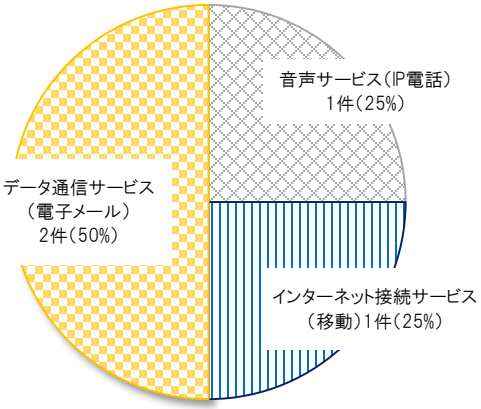
※ 報告件数。なお、重大な事故について、平成20年度から、電気通信役務の品質が低下した場合も重大な事故に該当することとなり、さらに、平成27年度から、電気通信サービス一律から電気通信サービスの区分別に重大な事故に該当する基準が定められており、年度ごとの推移は単純には比較できない。

【重大な事故のサービス別内訳※】

※ 報告のあった１件の事故について、複数のサービス・事業者に同時に影響している場合があるため、それらの場合を含めたものとなっている。



令和元年度



令和２年度

令和2年度に発生した重大な事故①

発生日時	継続時間 影響利用者数 （影響地域）	事故の内容	発生原因	再発防止策
令和２年４月30日	①2時間 ②81時間32分 166,803人 （全国）	①インターネット関連サービス（有料）（電子メール）の提供の停止（利用不可） ②インターネット関連サービス（有料）（電子メール）の品質の低下（遅延）	①電源ラインの異常が発生し、回路保護のために電源ユニットが停止したことから、仮想OS、メールボックス等にアクセスできなくなった。 ②受信メールとユーザのひも付けの正常性の確認をせずにメールBOXの復旧を優先させたことにより、メールの消失が発生したため、アーカイブからメールの復旧を行い再配送を実施した。	1．DB認証の管理機能を仮想OSから切り出して他の物理サーバに配置し、その複製を別のストレージに配置した。これにより、同様の障害が発生しても他のサーバにてDB認証機能が有効であるため、ストレージの復旧作業のみ実施すればよく、早期復旧を可能となった。 2．同様の障害発生時に、メールボックスサーバの復旧を実施する手順を明確化。また、対処1．の対策を踏まえた、作業、確認手順を変更した。 3．機器の交換を実施した。
令和２年５月30日	5時間36分 最大220万人 （全国）	インターネット接続サービスの提供の停止（利用不可）	ストレージのハードウェア故障と同時に、同故障時に冗長先への迂回措置を行うソフトウェアバグに起因して障害が発生した。 故障の大規模化を避けるため冗長構成をとっていたが、ストレージのハードウェア故障を検知するソフトウェアバグにより冗長設備への切替が行われず、通信に必要となる複数のサーバでストレージへのアクセスができなくなったため、当該システムを利用する全利用者に影響が発生した。	＜暫定対処＞ 1．ストレージのハードウェア故障を検知した場合に運用者オペレーションで切替を実施する手順を整理 ＜恒久対処＞ 1．ストレージのハードウェアを正常な機器に交換 2.ストレージのハードウェア故障を検知するソフトウェアのバージョンアップ 3．作業手順書を故障発生時の対応に合わせて整備

令和2年度に発生した重大な事故②

発生日時	継続時間 影響利用者数 （影響地域）	事故の内容	発生原因	再発防止策
令和２年６月29日	①2時間36分 135,000回線 （石川県） ②4時間21分 8,000回線 （兵庫県）	緊急通報を取り扱う音声伝送サービス（IP電話）の提供の停止（着信不可・誤着信）	光電話の工事の委託事業者の事前作業において、ゲートウェイ設備と交換機に誤ったデータが設定されていた。 また、データ作成後のデータ確認および試験において、業務マニュアルの確認項目に具体的かつ詳細な記載が不足していたため、設計や試験において必要作業の漏れが発生し、データ不一致を発見することができなかった。	【事前作業における対策】 1. データ作成時は、データを2名の作業者がそれぞれ作成し、それらの差分をプログラムにより自動的にチェックし、データの正常性を確認することを、業務マニュアルとして定める。 2. 自動動作確認試験機を新たに導入。 3. データの確認を行う作業者に対して、研修説明会を実施し、教育を行う。 4. 物理構成が基本方針と異なる場合は、基本方針と異なる箇所を明示し、情報伝達を実施。 【切替時における対策】 ・切替作業直前に、自動動作確認試験機による最終確認を行い、正常性を再確認した後に切替作業を行う。
令和２年７月31日	8時間7分 106,027人 （全国）	インターネット接続サービス（有料）（電子メール）の提供の停止（利用不可）	ストレージ装置のポートの一つで信号出力低下が発生したことにより仮想サーバ群の入出力応答がタイムアウトし、ファイルシステムがOSから認識できない状態になった。このため、一部仮想サーバでメール送受信及びアカウント管理サービスが停止した。	1. ポートの予防交換が可能なよう、ポートの故障予兆サインを監視する。 2. 同様の障害に対し短時間で復旧できるよう、ハードウェアの健全性確認のチェック項目及び冗長系パスの手動切替手順を整備する。 3. 利用者の収容規模に応じて、仮想サーバ別の復旧優先順位を整理し、大規模な仮想サーバ再起動を想定した復旧手順書を整備する。 4. ポートの信号出力低下時に適切にフェールオーバーするよう、発動条件を整理し適切な閾値設定を行う。

主な教訓等①

■令和２年度に発生した**重大な事故等**について、当事者である電気通信事業者から事故の内容等の説明を受け、検証を行い、**当該事故等から得られる教訓等**を整理。主なものは次のとおり。

（1） 手順書の遵守の徹底

- **手順書通りの作業を実施させるための工夫**を行う
  - ✓ 手順書の中でも重要なところは太字や赤字にし、**必須の手順を明確にする**
  - ✓ 適切に手順書に従って進んでいるかを確認する**進捗管理ツールを利用する**

（2） データ作成時の誤り防止の措置

- **ヒューマンエラー防止の観点**から、**自動でデータを作成する仕組みや自動で入力チェックを行う仕組みを検討する**
- 自動化が難しい場合には、**設定値のダブルチェックを行う**

（3） 組織外の関係者との連携

- ネットワーク・設備の運用維持管理に当たり、積極的に**情報共有体制を構築**する
- **ベンダー等との定期的な情報交換の場を設定**したり、ベンダー等との**保守契約を主体的なものに見直す**
- 外部委託を行う場合は、**定期的な業務報告**、**監査**等の**委託業務の適正性を確保するための仕組み**を構築する

主な教訓等②

（以下、【BP】はベストプラクティス）

（4） 複数段のフェイルオーバーの仕組みの検討

- 仮想化システムの利用に当たっては、装置からのアラートを検出し、フェイルオーバーするだけでなく、例えば、ファイルシステムが応答しなくなった際、別の系に切り替えられるように、ＯＳレベルから冗長化の構成を考えてシステム設計する等、**複数段のフェイルオーバーの仕組みを検討する**

（5） 速やかな利用者等への情報提供

- 事故発生時には、事故原因の特定や被疑箇所の特定ができていない状況においても、**まずは事故・障害が発生している旨の第一報を発出する**
- 事故の原因特定や復旧状況に進捗があった場合には、**随時情報を更新して途中経過も含めて周知する**
- **利用者側の対策によりサービスの利用が可能になる方法**が見つかった場合、それを**速やかに利用者に周知する**【BP】
- ホームページへの形成以外に、SNSの公式アカウントからの情報提供等、**多様な媒体を用いて情報提供を行う**【BP】
- 総務省に対しても、速やかに報告を行う

（6） 訓練・教育の徹底

- **模擬環境を作り、そこで実際に模擬故障を起こしての訓練を行う**、**日常業務の一環として訓練を行う**等、**訓練が形骸化しないための工夫**を行う

災害時における通信確保の在り方

- 近年、我が国では、地震、台風、大雨、大雪、洪水、土砂災害、火山噴火等の自然災害が頻発し、人的・物的に大きな被害を受けており、これら災害時には、停電による影響、通信設備の故障、ケーブル断等により、通信サービスにも大きな支障が生じている
- 令和２年度は、平成23年３月に発生した東日本大震災の発災から10年となることから、東日本大震災以降の、総務省及び電気通信事業者等による災害時における通信サービスの確保の主な取組の紹介を行った

携帯電話事業者による災害対策の強化

	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	令和２年７月豪雨等	R3.3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	微増	3294台
停電対策	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	微増	約6060台
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	変化なし	2～4ルート
伝送路断対策	マイクロエントランス回線	70回線	約5.1倍	359回線	約1.1倍	377回線	約0.9倍	357回線 ※他社間への移管により減少	微増	367回線	約0.7倍	260回線
伝送路断対策	衛星エントランス回線	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	約1.5倍	814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	約1.2倍	236台
エリアカバー対策	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	約1.1倍	410台
エリアカバー対策	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	変化なし	116局

※1 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

検証チーム※2最終とりまとめ概要

※2 令和元年度台風第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

課題		対応策
通信障害の状況把握と情報提供	・携帯電話の通信障害状況をエリアマップで公表しているが、定量的な影響が不明、HPのみでの公表のため障害地域では利用者が閲覧できず ・倒木等による通信線の被災箇所等について関係機関への情報共有が不十分 ・固定電話利用者の通信障害に対する全体把握が困難	①携帯電話の通信障害について、影響利用者数等の定量的な指標での情報提供 →「推定影響回線数」等を関係局長級会議等で提供 ②携帯電話利用者（障害地域内の利用者含む）へのわかりやすい情報提供 →被災自治体（災害対策本部等）での報告等 ③関係機関との情報共有に関する総務省リエゾン・通信事業者リエゾンの役割明確化 →「災害時テレコム支援チーム」の派遣等 ④利用者への固定電話の疎通状況確認の呼びかけなど、障害把握の方法を改善 →被災自治体（災害対策本部等）での説明等
復旧作業復旧プロセス情報提供	・携帯電話・固定電話の復旧見込みが非公表 ・復旧に関する関係機関との情報共有、対応調整が不十分 ・県・市町村間の非常時の通信手段が一部活用されず	⑤携帯電話の復旧見込みの公表のタイミング・具体的内容を検討し運用開始（固定電話についても検討） →同上（①） ⑥早期復旧のための関係機関との連携強化に関する総務省のリエゾン業務のマニュアル化、訓練等による充実 →同上（③） ⑦災害対策用移動通信機器の自治体への事前貸与をプッシュ型で実施 →台風到来時期に備えた事前貸出含め、実施
非常用電源の長時間化等	・長期間の停電のため重要な通信施設の非常用電源が持続せず	⑧携帯電話基地局等の非常用電源を長時間化 →令和２年6月、告示改正 ⑨総務省（総合通信局）への移動電源車の追加配備 →令和３年３月配備 ⑩基地局を搭載した係留ドローンの活用 →令和２年6月、告示改正

重要インフラ事業者に対するサイバー攻撃

■サイバーセキュリティ戦略本部重要インフラ専門調査会において行われている重要インフラにおける補完調査結果から、重要インフラ事業者へのサイバー攻撃の事例を紹介した

■特に、以下に示すような事例については、電気通信事業者において発生した場合、重大な事故や重大な事故につながるおそれのある事態となる可能性があるため注意が必要

※　括弧内は事例が発生した年

Dos攻撃・DDoS攻撃

- DDoS攻撃によるサービス障害(H27)
- DDoS攻撃(H29)
- 脆弱性を悪用した攻撃(H30)
- 広域DoS攻撃によるWebサイト閲覧攻撃(H30)
- 商用ネットワークの通信負荷による通信障害(H30)

ランサムウェア感染

- ランサムウェア被害(H28)
- WannaCryによるサイバー攻撃(H29)
- 重要インフラ事業者における２度のランサムウェア被害(R2)
- 重要インフラ事業者における「WannaCry」の感染(R2)

マルウェア感染

- 端末へのマルウェア感染(H26)
- USBメモリを介したマルウェア感染(H27)
- 不審メールによるマルウェア「Emotet」への感染(R1)

不正アクセス

- 管理サーバへの不正アクセス(H28)
- 認証の脆弱なIoT機器への第三者アクセス(H29)
- IoTデバイスへの不正侵入及び改ざん(H30)
- 他人の認証情報の悪用による情報の不正取得(H30)
- 重要インフラ事業者が利用するサーバへの不正アクセス(R1)
- クラウド型メールサービスへの不正ログイン(R1)

令和時代における事故報告・検証の在り方

検討の経緯・背景

・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月から、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)について検討を開始。委員会では、平成29年12月からは、「IoTの普及に対応した電気通信設備に係る技術的条件」について検討を行ってきたところ。

・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である情報通信ネットワークについては、自然災害やサイバー攻撃等のリスクの深刻化、仮想化・ソフトウェア化等によるネットワーク構築・管理運用の高度化・マルチステークホルダー化等の新たな環境変化に伴い、通信事故等の発生により生命・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。

・本年3月、委員会では、これらのリスクに対応し、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事故報告・検証制度等の在り方について、「安心・安全で信頼できる情報通信ネットワーク確保のための事故報告・検証制度等の在り方」として検討を開始することとし、「事故報告・検証制度等タスクフォース」を開催し、検討を実施。

・委員会は、タスクフォースにおける検討結果に基づき、本年6月に第五次報告(案)としてとりまとめ。7月9日から8月10日までパブリックコメント手続きを実施し、19者から意見提出があったところ。

検討の方向性

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、重大なリスクに関するリスクアセスメント機能の強化等の観点から次の点を検討

・BtoB/GtoX(通信事業者to法人利用者/行政機関to一般利用者等)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等の在り方

・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等の在り方

・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

・激甚化・頻発化する大規模自然災害やサイバー攻撃の巧妙化・悪質化等による通信障害等を踏まえた自然災害・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重要インフラ向け通信サービス・ネットワークに関する報告制度の在り方

現状と考え方

通信事故から波及する重要インフラサービスの障害やクラウドサービス障害を原因とする通信事故が発生しており、重大なリスクに関するOODAループ機能やリスクアセスメント機能の強化のため、報告制度を見直すことが必要。

課題と対応の方向性

- BtoB/GtoX型の通信サービス・ネットワークのうち、通信分野と相互依存が深まる重要インフラに提供されるものの通信事故に関する考え方等が不明確。
- クラウドサービスが通信サービスに該当する場合、重要インフラである通信分野に提供される際のクラウドサービス障害に関する通信事故としての考え方等も不明確。

- 重要インフラに提供される通信サービス等の通信事故につき、総務省への速やかな報告に関する考え方の明確化や四半期報告事故に係る報告事項の追加等、所要の制度整備が適当。
- 通信サービス等に提供されるクラウドサービスの障害につき、通信事故への該当性に関する考え方の現行GLによる明確化等が適当。

②インシデント（事故の兆候段階の事態）に関する報告制度の在り方

現状と考え方

通信設備に関する情報が、サイバー攻撃により漏えいし、重要インフラ分野事業者の通信サービスが利用不可となるおそれのある事態等の重大なインシデントが発生しており、重大なリスクに関するOODAループ機能やリスクアセスメント機能の強化のため、報告制度を見直すことが必要。

課題と対応の方向性

- インシデントについては、一部のみが四半期報告事故として対象となるが、報告しない場合等には罰則の適用可能性。
- 重大事故と同様に社会的な影響が大きい重大なリスクとなるインシデント（重大インシデント）については、重大事故としての速やかな報告の対象外。
- 通信事業者による報告は、電子メールによる添付ファイル送信。

- 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、インシデント(通信事故の兆候段階である事態)につき、重大インシデントの速やかな報告等、所要の制度整備が適当。
- 報告の迅速化・負担軽減やマルチステークホルダーによる分析の容易化等のため、ダッシュボード機能等を備えた報告システムの整備など、報告制度のDX化の推進が適当。

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

現状と考え方

2015年度から開催されている電気通信事故検証会議により、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サイクルについては、一定の意義・成果があるところ、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の強化によ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、検証会議の機能強化が必要。

課題と対応の方向性

- 検証制度の対象について、通信事故に該当しない障害や重大インシデント等の重大事故以外の重大なリスクにも拡大。
- 原因の関係者による参加や情報提供等が得られず、原因究明やリスクアセスメントにおける公正性や実効性の確保が困難。

- 重大事故・インシデントの原因に関係するマルチステークホルダーからの報告徴収等を通じた原因の究明等によるリスクアセスメント等、第三者機関に関する所要の制度整備が適当。
- 事故調査・リスクアセスメントの結果公表やリスクコミュニケーション等により、マルチステークホルダーの取組に貢献。

④自然災害や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

現状と考え方

激甚化・頻発化等する大規模自然災害により、通信障害における広域化・長期間化が進展していること、また、サイバー攻撃の巧妙化・悪質化等により、通信サービスの提供停止に至る通信事故、通信設備に関する情報の漏えい等の重大なインシデントが発生していることから、OODAループ的な対応やPDCAサイクルの強化が必要。

課題と対応の方向性

- 災害対策基本法に基づく被害状況等の報告や報告制度に基づく四半期報告事故等による対応強化、総合的な検証等が可能な環境の構築が必要。
- 報告制度等とサイバーセキュリティ対策における一層の連携・協力の推進による対応や強化が必要。

- 報告対象となる通信事業者の範囲を明確にした上で、自然災害時における被害状況等の報告を求めるための所要の制度整備を行うとともに、報告システムのDX化を推進。
- サイバー攻撃を原因とする重大インシデントの速やかな報告や、サイバー攻撃による重大事故等に関する詳細報告期限の柔軟化等、所要の制度整備等が適当。

【参考】「電気通信事故検証会議」の概要

電気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、報告された事故について、外部の専門的知見を活用しつつ、検証を行うことにより、電気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、電気通信事故の再発防止を図る。
（平成26年：電気通信事業法改正付帯決議、平成27年：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）

■ 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。

【構成員】（令和2年7月現在）
相田　仁　　（東京大学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　（早稲田大学理工学術院　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ストラテジー・アンド・コンサルティング株式会社　ディレクター）
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。

■ 電気通信事業部長主催の会議として、2015年5月に設置。

■ 電気通信事故検証会議の開催状況

https://www.soumu.go.jp/main_sosiki/kenkyu/tsuushin_jiko_kenshou/index.html