資料36－6

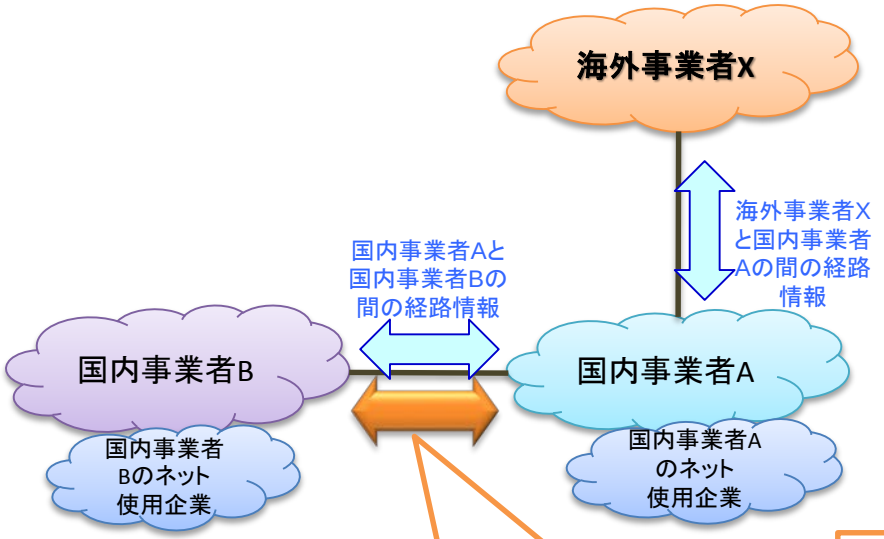
大規模なインターネット障害発生時の対策について

平成30年3月6日
事務局

昨年8月に発生した大規模なインターネット接続障害

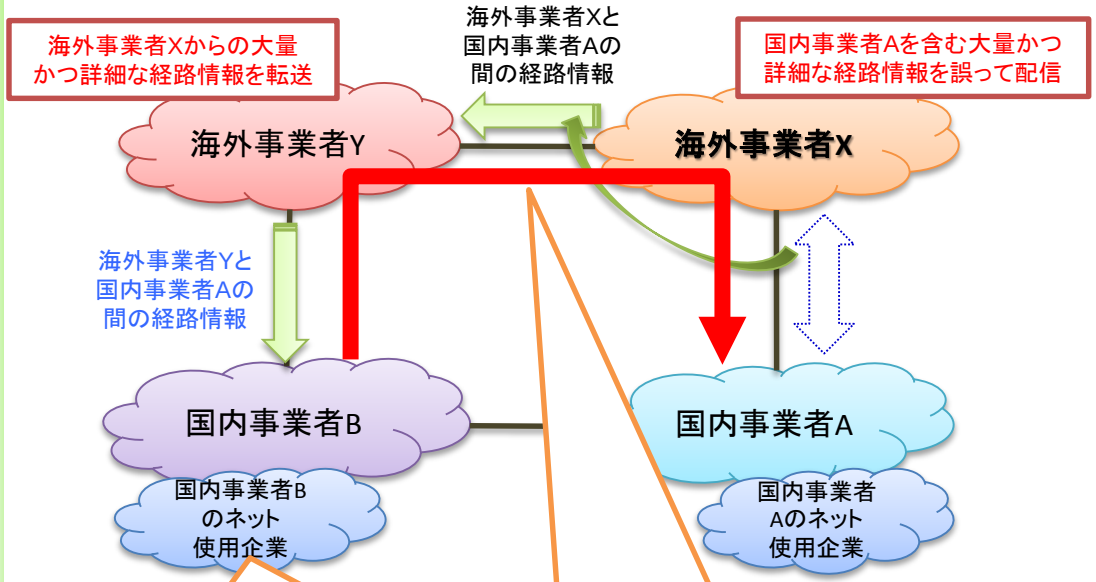
- 昨年８月25日、海外事業者Xが行う通信経路設定の誤りが原因となり、我が国の電気通信事業者（国内事業者A、国内事業者B）の一部の回線や設備に過大な負荷がかかったことにより、インターネットに障害が発生

本来の通信経路



国内事業者Aと国内事業者B間の通信は、経路情報に従い最短の国内ルートを通過

今回の障害時の通信経路



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

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

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

（参考）　経路情報の誤りによるインターネット障害の発生状況

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

大規模なインターネット接続障害から得られた教訓

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

人為的ミスの未然防止

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

誤送信された膨大かつ詳細な経路情報の受信防止及び不要な経路情報の送信防止

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

→ 「情報通信ネットワーク安全・信頼性基準」等に規定することが適当

障害に関する情報の電気通信事業者間での共有

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

利用者周知

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

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

（参考）　本事案に係る電気通信事故の該当性

電気通信事故の定義

○電気通信設備の故障により、電気通信役務の全部又は一部の提供を停止又は品質を低下させた事故（電気通信事業法施行規則58条）

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

（参考）電気通信事故に係る電気通信事業法関係法令の適用に関するガイドライン

○利用者の端末機器等と事業者側の集線装置等との間でのリンク又はセッションが確立できない状態は、「役務の提供の停止」とする。

※　ベストエフォートサービスの場合は、品質の低下の定義が確立していない。

事業者への確認結果

○NTTコム

電気通信設備に異常はなく、利用者とのリンク又はセッションは切れておらず、通信遅延のみ

○KDDI

法人向けインターネットゲートウェイサービスでは、pingによる死活監視においても接続断はなく、利用者とのリンク又はセッションは切れていない

○KDDIの上記サービスを利用してインターネット接続サービスを提供している電気通信事業者

・通信は不安定になったが、利用者とのリンク又はセッションは切れていない

・すぐに他事業者の回線に切り替えたことにより利用者への大きな影響なし

電気通信事故には該当しない

円滑なインターネット利用環境の確保に関する検討会「対応の方向性」概要（抜粋）

➢ 総務省は、円滑なインターネット利用環境の確保に関する検討会において取りまとめられた「対応の方向性（案）」について、昨年12月27日から本年1月18日まで意見募集を実施。意見募集の結果等を踏まえ、本検討会において「対応の方向性」が以下のとおり取りまとめられた。

○基本的な考え方

通信ネットワークに関わる者全体が連携することが肝要。

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

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

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

○大規模なインターネット障害発生時の対策

【対策】
- インターネットの経路情報の送受信を適切に制御する経路フィルターの設定を推奨
- インターネット障害に関する情報共有体制の整備

【課題と今後の対応】

ガイドライン等において<u>ルータの設定につき規定</u>するとともに、<u>電気通信事業者から総務省への迅速な障害報告の在り方を含めた情報共有体制</u>を検討。

検証結果及び教訓を踏まえた論点

＜障害発生時の総務省への報告について＞

・電気通信事業法上の重大な事故に該当しないものについては、速やかな報告を現状求めていない(注)。
大規模なインターネット障害やサイバー事案などによる利用者への影響を鑑みれば、一定の障害発生時には、総務省に情報提供いただくことが必要ではないか。

（注）ただし、「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」において、事故発生直後で影響利用者数や継続時間が不明であっても、重大な事故となるおそれがある場合には、速やかに報告するよう求めている。

・ベストエフォートサービスの場合は、品質の低下の定義が確立していないものの、同様に利用者への影響を鑑み、一定の障害発生時に情報提供をいただくことが必要ではないか。

＜各電気通信事業者に推奨するネットワーク運用について＞

・大規模なインターネット障害やサイバー事案を防止又は被害を最小化するために、各電気通信事業者に対して指標となる対策を示すことが必要ではないか。

LPWAの事故報告の在り方と併行して、具体的な議論に入る必要がある

（参考）電気通信事故検証会議の開催

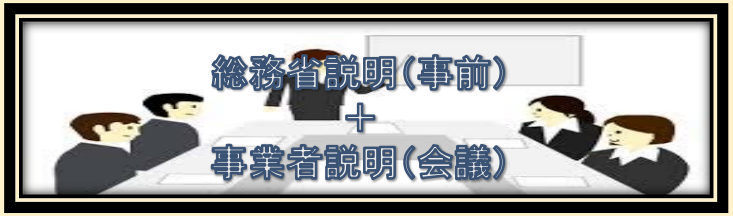
「事故が大規模化・長時間化し、その内容・原因等が多様化・複雑化する中で、その検証作業も複雑化・高度化している状況にあるため、事故報告の検証は、外部の専門的知見を活用しつつ、透明性の高い形で行われることがこれまで以上に重要となっている。」【「多様化・複雑化する電気通信事故の防止の在り方について」報告書（平成25年とりまとめ）】

電気通信事故検証会議の設置（平成27年5月～）

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

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

重大な事故報告



四半期事故の報告

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

事故発生事業者への
フィードバック

業界内共有
フォローアップ調査

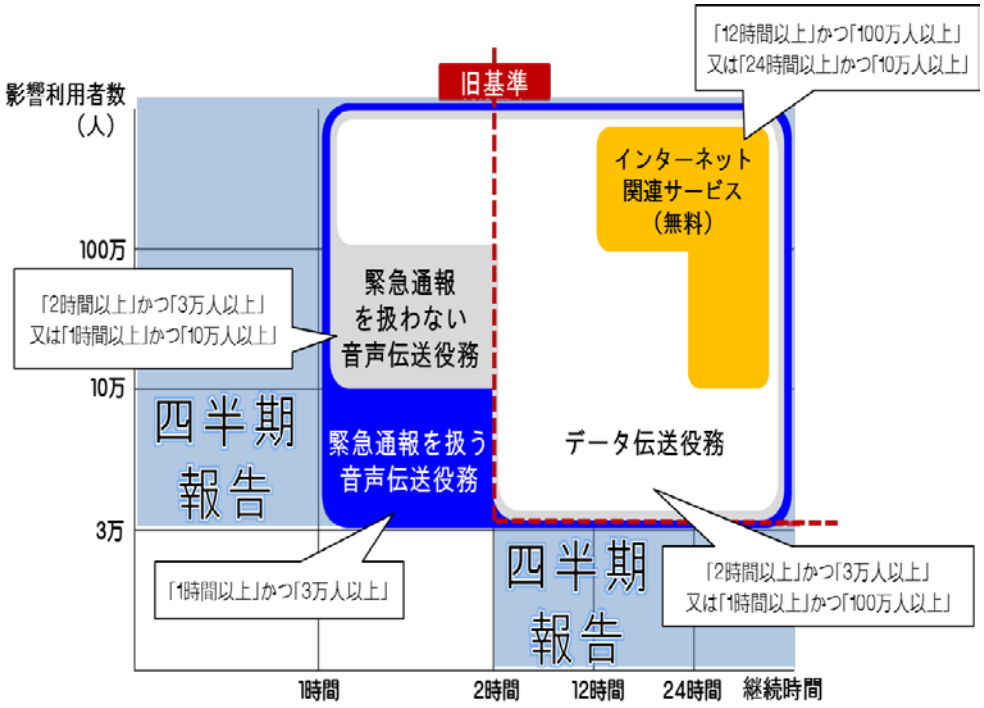
ガイドライン等へ反映

（参考）　電気通信事故の報告基準について

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

① **四半期報告事故**：「**影響利用者数3万人以上**」又は「**継続時間2時間以上**」の事故　→　四半期ごとに報告

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



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

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

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

（参考）　電気通信設備の安全・信頼性の確保に関する基準

○　通信サービスを提供する上での基盤となる電気通信設備について、サービス中断等の事故が発生した場合、国民生活や社会経済活動に深刻な影響を与えかねないため、**安全・信頼性確保に関する制度**を設けている。

強制基準	技術基準	**＜事業用電気通信設備の技術基準＞** 事業用電気通信設備規則（耐震対策、防火対策、停電対策　等） **＜利用者が接続する端末設備等の接続の技術基準＞** 端末設備等規則（安全性、電気的条件、責任の分界　等）
自主基準	管理規程	**＜事業者ごとの特性に応じた基準＞** 業務管理者の職務、組織内外の連携、事故の報告、記録、措置、周知　等
ガイドライン	安全・信頼性基準	**＜努力目標として、全ての電気通信事業者の指標となる基準＞** ソフトウェアの品質検証、事故状況等の情報公開、ネットワーク運用管理（運用基準の設定、委託保守管理）　等
監督責任	統括管理者	**＜経営レベルの設備管理＞** 経営陣から選任、事故防止対策に主体的に関与
	主任技術者	**＜事業用電気通信設備の「工事、維持・運用」を監督＞** 電気通信事業者が資格証の交付を受けている者から選任
	工事担任者	**＜端末設備等の「接続に係る工事」の実施等＞** 資格者証の交付を受けている者が端末設備等の接続に係る工事を実施又は実地で監督
報告義務	事故報告	**＜事故の影響度に応じ、期限内に所定の様式で報告＞** 重大な事故…30日以内に、事故の概要、原因、再発防止策等を詳細に報告 四半期事故…四半期ごとに、事故の概要を選択肢式で報告