資料31－10

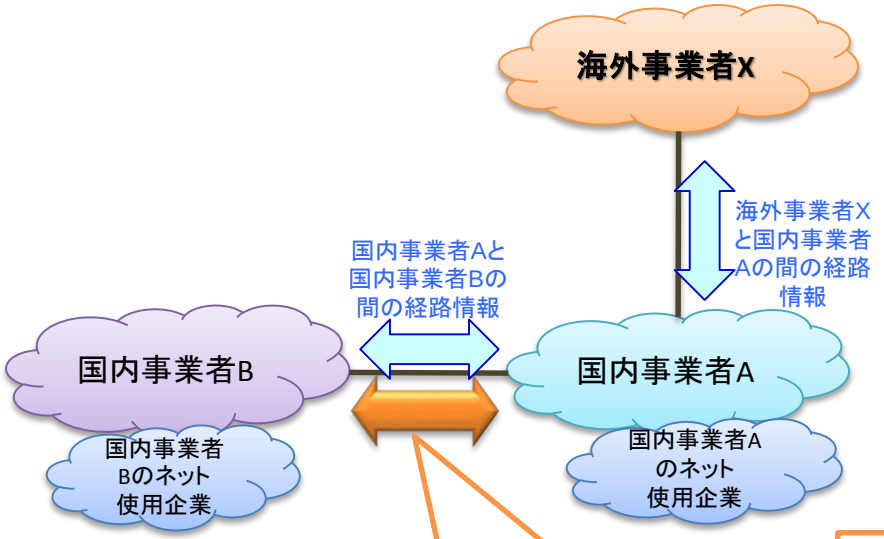
大規模なインターネット障害発生時の対策について

平成30年3月16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

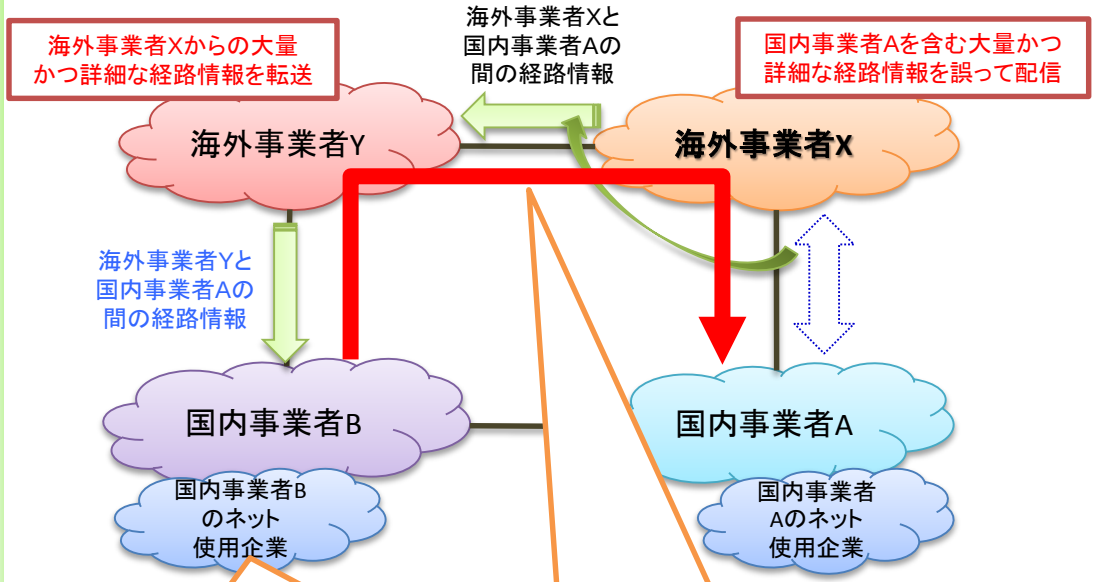
- 昨年８月25日、海外事業者Xが行う通信経路設定の誤りが原因となり、我が国の電気通信事業者（国内事業者A、国内事業者B）の一部の回線や設備に過大な負荷がかかったことにより、インターネットに障害が発生

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

利用者とのリンク又はセッションは切れていなかった

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（3月6日IPNW設備委員会資料）

＜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対策について＞

○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

障害発生時の総務省への報告について

大規模なインターネット障害やサイバー事案など、複数のネットワークに跨がって発生する事態においては、利用者に対して大きな影響があるものであり、そうした事態に迅速かつ的確に対応するためには、その全容を速やかに把握することが重要であるものの、複数の事業者が関与する場合は困難である。

一方、事業者は、自らに発生した障害の原因が自らのネットワーク内にあるか外部にあるのか否かはすぐには判断できない、また自らの障害が原因で他の事業者のサービスや業務に障害が生じている場合において、その障害の規模や業務に与える影響の大きさを知ることは困難と考えられる。

他方、電気通信事業法上の重大事故となる恐れがないものについては、速やかな報告は現状求めていない。また、品質低下でインターネットに接続しづらい障害は、電気通信事故として取り扱う整理がなされておらず、電気通信事業法上の報告の対象外とされている。

① 重大事故に該当しないものであっても、電気通信事業者から速やかに障害等の情報提供を得られれば、総務省において、各事業者から得られた障害等情報をもとに全容を把握し、政府内や事業者団体、電気通信消費者相談センター等との情報共有、外部からの問い合わせ対応の他、利用者周知の観点から必要に応じ速やかに事案を公表することにより、事態の早期沈静化を図ることができるのではないか。

（考慮すべき点）

－インターネットに接続しづらい障害事案に対する利用者の混乱の大きさ

－複数のネットワークを跨がるインターネット障害の発生時における、各事業者から利用者への周知範囲の限度

－総務省はインターネットに接続しづらい障害について把握する手段がないため、同障害に対する知見が蓄積されておらず、事業者との連携や、インターネットの安全信頼性に係る政策の立案等に対して責任を持って対応できていない

電気通信事業者から情報共有を得る基準について

② 総務省への情報提供のタイミングである、「一定の障害発生時」とはどのような場合を想定すればよいか。

（考慮すべき点）

・具体的に影響利用者数や時間で区切ることができるか。（1時間かつ3万ユーザー、2時間かつ1万ユーザーなど）

・社会的な影響の重大さなどを考慮することができるか。

・自社のインターネットサービスで接続しづらい事象が発生している場合についても含めるべきではないか。

・情報提供と事業者負担とのバランス

③ 他事業者や法人ユーザーに影響が与えているかどうかの情報は、全容の把握において効果的ではないか。

（考慮すべき点）

・自社のサービスに一定程度の障害が出ており、さらに他事業者に影響を与えているかもしれない場合においては、影響を与えている可能性についての情報は出すことが、全容の把握において効果的ではないか。

・自社のサービスに一定程度の障害が出ており、利用者（法人ユーザー含む）の混乱が起きそうな場合において、何らかの情報提供ができるか

電気通信事業者から情報共有を得る基準について

④　情報提供はどのような仕組みで行うのがよいのか。（例えば省令又は民間ガイドライン）

（考慮すべき点）

・情報提供の基準の設定の自由度

・事業者における総務省への情報提供に係る業務の根拠を例えば省令と民間ガイドラインのどちらに持つかによって、当該業務の位置づけに影響するか。

・現状の事故報告制度との明確な切り分けが必要か。

⑤　その他

・具体的な情報提供の方法、内容

各電気通信事業者に推奨する対策について

電気通信事故検証会議の検証結果から得られた教訓を踏まえ、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必要と考えられる以下の対策について、各電気通信事業者に推奨することが適当か。

（考慮すべき点）

・これらのうち情報通信ネットワーク安全・信頼性基準に不足する対策については、改正し盛り込むことを想定。

・個々の対策の必要性、有効性、実行性。

教訓等	個々の事業者に推奨する対策（案）
①インターネットの経路設定時の人為的ミスの防止	＊以下の2つの手法のいずれかの実施を推奨。 ①人的な手段で防止する手法 ・経路設定の人為的ミスを防止するダブルチェックに係る体制構築、教育、実行。 ②自動的な手段で防止する手法 ・経路設定後のトラヒックの疎通状況を監視し、又は経路設定前に入力内容の誤りを自動的に検証し、異常等をアラームで知らせる機能の導入。 ・上記の監視項目や検証項目のあらかじめの設定。

各電気通信事業者に推奨する対策（案）

教訓等	個々の事業者に推奨する対策（案）
②誤送信された経路情報の受信防止及び不要な経路情報の送信防止	・不要な経路情報の送受信を防ぐためのリミッターやフィルターの機能の導入。 ・経路情報のバースト的な増加や将来的な増加を考慮し、設備を設計。 ・不要な経路情報の送受信による障害の発生を防止するため、接続先とあらかじめ当該情報の送受信の範囲を明確化。
③経路設定誤り又はサイバー攻撃による障害に関する情報の事業者間での共有	・平時から、事故発生時に障害情報や再発防止策等の情報を、接続・契約関係のある事業者からに限らず、複数のルートを活用し幅広く情報収集するための通信手段の確保。また、その情報の共有。 ・事故発生時に遅滞なく情報収集が行われるよう、接続・契約関係のある事業者（海外の事業者を含む。）とリアルタイムで連絡を取ることができる通信手段の確保。

各電気通信事業者に推奨する対策（案）

教訓等	個々の事業者に推奨する対策（案）
④利用者周知	・接続先や他の事業者のネットワークに起因する障害など迅速な原因分析や状況把握が困難な障害であっても、自社に障害が発生した場合は、発生事実だけでも利用者に迅速に周知を行う体制を構築（対象が特定の法人ユーザーや特定のISPなど限定的な場合は個別に情報提供するのみでも可）。 ・あらかじめその周知内容を明確化。
⑤その他	・データセンターなどサーバーサイドのサービス事業者（電気通信事業者の場合、そうでない場合）の２ルート化。