参考資料 34－1－1

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
技術検討作業班（第 33 回）（事故報告等の在り方について）
議事要旨（案）

１　日時

平成 30 年 5 月 10 日（木）10 時 00 分～11 時 00 分

２　場所

総務省 11 階　11 階会議室

３　出席者（敬称略）

（１）作業班構成員（事故報告）

内田　真人（主任）、吉岡　克成（主任代理）、大内　良久、岡田　昌己、木村　孝、
喜安　明彦、小林　努、高橋　範、中島　　寛、拮石　康博、花石　啓介、安藤　英治、日比　学、
福井　晶喜、福島　敦、松本　佳宏、向山　友也、矢入　郁子、山口　琢也、渡部　康雄

（２）事務局（総合通信基盤局　電気通信事業部）

荻原　直彦（電気通信技術システム課長）、松井　正幸（安全・信頼性対策室企画官）、
道方　孝志（電気通信技術システム課課長補佐）、篠原　信（安全・信頼性対策室課長補佐）
深松　佑次（安全・信頼性対策室係長）

４　議事

（１）大規模なインターネット障害発生時の対策のうち、電気通信事業者等に推奨する対策の検討

事務局より、資料 33-1-1 に基づき、大規模なインターネット障害発生時の対策のうち、電気通信事業者等に推奨する対策の検討について説明があった。主な意見や質疑は次のとおり。

○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に係る対策と解説（資料 p.5）について、「(障害発生当時、一度に約２年分の経路情報に相当。)」とあるが、何を元にしているのか。

→毎月経路情報は増大しており、それを２年分に換算したという趣旨。

○ネットワーク構成と利用者周知に係る対策と解説（資料 p.7）の一つ目の対策として「重要な回線については異なる２者以上の電気通信事業者から提供を受けることにより、冗長化を図ること」とあるが、第 31 回作業班の資料では、より具体的に「データセンターなどサーバーサイドのサービス事業者の２ルート化」と記載されていた。重要な回線という切り口で、対象範囲が広がっているのか。

→趣旨は変わらず、対象範囲も「自」（自営の情報通信ネットワーク）と「ユ」（ユーザーネットワーク）としている。また全ての回線をというより、電気通信事業者から提供を受けるユーザー側の判断で重要な回線と考えるものは対策が必要ということを明確にした。

○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に係る対策と解説（資料 p.5）について、「トラヒックの瞬間的かつ急激な増加及びインターネットの経路情報等制御信号の増加の～」という改正案では、「瞬間的かつ急激な」がトラヒックの方にはかかっているが、経路情報の方にはかかっていないように読めてしまうので表現を工夫したほうがよい。
また、経路情報というワードが安信基準に具体的に記載されることについて、他の文言との並びを見て適当か。
→特に意見なし。

○ネットワーク構成と利用者周知に係る対策と解説（資料 p.7）について、「速やかに利用者に対して公開すること」という文言について、何を公開するということが明確でないがこれでよいか。
→どのような情報を利用者に対して公開するかは事業者の判断があるため詳細には記載していない。また、どのような情報を総務省に情報提供するかについても同様（提供された情報をもと、総務省が全容を把握し、利用者に周知する）。

○「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（資料 p.4）」について不要な経路情報と書いているが、不正なものもあるのではないか。
→分かるような表現に工夫する。

○「ネットワーク構成と利用者周知に係る対策（資料 p.7）」について、「その他障害」とはインターネットに繋がりにくい障害を指すのか。
→そのとおり。
→その他障害というのは広いので、大規模なものとかに限定する表現を追加すべきではないか。
→表現を工夫する。

（２）電気通信事故報告制度に係る作業班報告書の検討

事務局より、資料 33-1-2 に基づき、前回作業班の議論を踏まえた整理について説明があった。続けて資料 33-1-3 に基づき、電気通信事故報告制度に係るその他の検討について説明があった。質疑応答後、資料 33-1-4 に基づき、電気通信事故報告制度に係る作業班報告書骨子（案）について説明があった。主な意見や質疑は次のとおり。

○資料 33-1-3 について、基本的には DDoS 攻撃を念頭に置いていると思うが、その予兆となるスキャン行為、偵察行為など、事故にはまだ至っていないものはスコープ外という理解。

○資料 33-1-3 について、DDoS 攻撃が起きた際、影響を受けた利用者をどこまで把握できるのか。
→DDoS 攻撃を受けた被害者数は、今までの電気通信事故報告制度のとおり、被害者の対象者数ということになるので、実際にそれでサービスが停止して、それが停止できなかった利用者の数。

○資料 33-1-2 の LPWA サービスの事故報告基準（資料 p.6）について、ＤＮＳのサービスが攻撃を受けて、その影響を受けてさまざまなサービスが利用できなくなった例がある。そういった影響はかなり測りにくいが、このスライドで言うサービス低下は、そういうものとも違うのか。

→障害が起きた場合に、影響利用者数を測ることが一番難しい作業になる。各事業者がサービスを監視する中で、使えなくなったサーバーの把握、トラヒック量、利用者数など判断してもらい、重大事故基準なら 3 万を超えているなら総務省まで報告してもらう。ここでいう障害の利用者数の把握の仕方は、それぞれのネットワーク運用の中で判断してもらう。

→DNS 自体のサービスと、別のサービスの、複合的に効果が出てくるなど、影響の測り方が難しいように感じる。

→今後総務省としてどのような形で把握していくのか、影響利用者数の考え方なども含めて、そういった事象を電気通信事故検証会議における検証し、事業者の方々と相談しながら検討することで、一つ一つの課題をクリアしていくのだと思う。

○資料 33-1-3 について、サイバー攻撃についても資料 33-1-2 の障害情報の共有を求めるという趣旨なのか。

→資料 33-1-3 については、四半期報告の発生原因の選択肢の一つとして、サイバー攻撃を追加するという趣旨。分かりやすく記載する。

（３）その他

事務局より、次回会合の日程について説明があった。

以上