資料33－1 －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

平成30年5月10日
事務局

電気通信事業者等に推奨する対策の検討について

・本検討においては、大規模なインターネット障害の防止又は被害の最小化を目的として、電気通信事業者や利用者である法人に対して推奨すべき対策及びその具体的な説明を整理することとする。また、安信基準への規定化や、解説への追記等についても検討することとする※。

＊総務省においては、情報通信ネットワークの安全・信頼性対策の普及・促進を目的として、指標となる対策を「情報通信ネットワーク安全・信頼性基準」（安信基準）において規定。個々の規定は基本的には汎用的な内容であるため、具体的な説明を「情報通信ネットワーク安全・信頼性基準解説」に掲載し、公表している。

・個々の検討における論点は以下の通り。

- ✓ 安信基準に新たな規定を追加する場合、汎用的な記載とすることが適当か。それとも重要性を鑑み、具体的な記載とすることが適当か。
- ✓ 今回整理する対策が安信基準の現行の規定に包含される場合、解説のみに追記することが想定されるが、重要性を鑑み、新たな規定を追加することが適当か。
- ✓ 解説に記載する内容が読み手の十分な理解を得られるものか。特に経路情報の設定については、現行の解説には具体的な記載がないが、重要性を鑑み、分かりやすく明確な記載が必要と考えられる。

・【想定される安信基準等への反映】欄における表の説明は、以下の通り。

- ✓ 安信基準においては**情報通信ネットワークを5つに分類し、規定ごと（対策ごと）に各ネットワークにおける実施の必要性を示しており、本資料中の表においても同様に示している。**

（表の例）

設	特	他	自	ユ
◎	◎*	○	ー	ー

（表中の上段の説明）
設：電気通信回線設備事業用ネットワーク（回線設置事業者のネットワーク）。
特：特定回線非設置事業用ネットワーク（MVNOや大規模ISPのネットワーク）
他：その他の電気通信事業用ネットワーク（「設」や「特」に該当しない事業者のネットワーク）
自：自営情報通信ネットワーク（自営で回線設備を設置したネットワーク）
ユ：ユーザネットワーク上記のいずれにも該当しないネットワーク）

（下段の説明）
◎ ：実施すべきである。
◎* ：技術的な難易度等を考慮して段階的に実施すべきである。
○ ：実施が望ましい。
ー ：対象外。

インターネットの経路設定時の人為的ミスの防止に係る対策と解説（未然防止を前提とした手法）

＊未然防止を前提とした手法と、事後措置を前提とした手法があり、少なくともいずれかの実施を推奨。

・経路情報の設定作業において、容易に誤りが混入しないよう措置を講ずること。

経路情報の設定作業は、自動処理で行われる部分はあるものの、新規接続先情報の入力など人間の手作業は必ず含まれる。そのため、経路情報の設定作業のみならず、様々な作業工程においても人為的ミスを完全に防ぐことはできない。

しかしながら、経路情報に不具合が発生した場合、インターネット全体に甚大な影響が出るおそれがあることを鑑みれば、経路情報の設定作業においては、人為的ミスによる障害を避けるため、設定が反映される前に、システムによる人為的ミスの防止を目的とした処理の実施や、複数体制によるチェックの徹底が重要である。

【想定される安信基準等への反映】

別表第2　管理基準＞第3．方法＞1．(5)に本対策の規定を以下の通り汎用的な内容で追加し、解説に上記説明を盛り込むことを想定。

(想定される追加規定)	設	特	他	自	ユ
データ投入等における高い信頼性が求められる作業において、容易に誤りが混入しないよう措置を講ずること。	◎	◎	◎	―	―

・経路情報の設定に係る教育・訓練を実施すること。

経路情報に不具合が発生した場合、インターネット全体に甚大な影響が出るおそれがあることを鑑みれば、経路情報を設定してからそれによる影響が出るまでの仕組みや、想定される影響等を含むBGP全般に係る内容に加え、経路情報の設定作業における複数体制によるチェック等必要な措置についても、教育・訓練を行うことが重要である。

【想定される安信基準等への反映】

別表第2　管理基準＞第3．方法＞1．(2)エの規定に含まれる対策であり、解説に上記説明を盛り込むことを想定。

(現行の規定)	設	特	他	自	ユ
データ投入等における信頼性の高い作業能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎	◎

インターネットの経路設定時の人為的ミスの防止に係る対策と解説（事後措置を前提とした手法）

・経路情報の設定後のトラヒックの疎通状況を監視し、異常等をアラートで知らせる機能を設けること。

経路情報は、通信の到達性を確保するため、各事業者が設定し、接続する事業者間であらかじめ送受信されている。誤り等により大量かつ詳細な経路情報が設定された場合、大量の通信が意図しない経路に流入（元の経路から流出）することとなり、インターネット全体に甚大な影響を及ぼすことが想定される。

このような事態を可能な限り迅速に収束させるためには、各事業者がトラヒックに異常な増大や減少が発生していないか等を自動でチェックし、異常等をアラートで知らせる機能を設けることが有効である。

【想定される安信基準等への反映】

別表第1　設備等基準＞第1. 設備基準＞1.（8）オの規定に含まれる対策であり、解説に上記説明を盛り込むことを想定。

（現行の規定）	設	特	他	自	ユ
交換設備には、トラヒックの疎通状況を監視し、異常ふくそう等を速やかに検知し、通報する機能を設けること。（以下略）	◎	◎	◎	○	○

・経路情報の設定に伴い、トラヒックの疎通に係る異常等が発生した場合を想定し、復旧対応手順を作成すること。

経路情報の設定後において、トラヒックに異常な増大や減少が発生した場合に、原因や影響を把握するために確認すべき事項や復旧のために行うべき措置等について、あらかじめ手順書を作成することが重要である。なお、復旧のために行った措置が二次被害を発生させる原因となる恐れがあることに留意する必要がある。

【想定される安信基準等への反映】

別表第2　管理基準＞第3. 方法＞1.（5）エの規定に含まれる対策であり、解説に上記説明を盛り込むことを想定。

（現行の規定）	設	特	他	自	ユ
保全・運用作業の手順化を行い、手順書の作成を行うこと。	◎	◎	◎	◎	◎*

・経路情報の設定後に、トラヒックの疎通に係る異常等が発生した場合の対応について、教育・訓練を実施すること。

経路情報の設定後において、トラヒックに異常な増大や減少が発生した場合に、原因や影響を把握するために確認すべき事項や復旧のために行うべき措置等について、教育・訓練を行うことが重要である。

【想定される安信基準等への反映】

別表第2　管理基準＞第3. 方法＞1.（2）エの規定に含まれる対策であり、解説に上記説明を盛り込むことを想定。

（現行の規定）	設	特	他	自	ユ
データ投入等における信頼性の高い作業能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎	◎

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に係る対策と解説（その1）

・不要な経路情報の送受信を防ぐために有効な機能を設けること。

経路情報は、通信の到達性を確保するため、接続する事業者間であらかじめ送受信されており、ある事業者が誤設定により大量かつ詳細な経路情報が送信してしまうと、他の事業者に広範囲かつ甚大な影響を及ぼすことが想定される。

インターネットの安定性を確保するため、一定の経路情報をルータにおいてフィルターする仕組みや、一定量以上の経路情報を受け取らないようリミッターを設定する仕組みがあり、このような設定は、経路情報の受信防止又は送信防止の有効な手段になり得る。

例えば、他の電気通信事業者から経路情報を受信する際は、Prefixフィルターにより、細かい経路情報を受信しないよう設定したり、AS-PATHフィルターにより、長いAS-PATH長の経路を受信しないよう設定したり、リミッターにより、設定した閾値以上の経路情報を受信しないよう設定したりする対応が考えられる。また、経路情報を他の電気通信事業者等に配信する際は、Prefixフィルターにより、自らのAS内部で使用している細かい経路情報をそのまま外部に配信しないようにする設定が考えられる。

しかしながら、こうした設定が自らの利用者や他事業者にも影響を与える恐れがあることから、各事業者がそれぞれのネットワーク構成及び他事業者との接続状況等を熟知した上で当該設定の影響を十分に検討した上で、かつ、それぞれの運用の考え方に照らして、柔軟かつ適切な設定を行うことが重要である。

なお、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には、あらかじめ接続先と当該情報の送受信の範囲を明確にすることも有効である。

【想定される安信基準等への反映】

別表第1　設備等基準＞第1．設備基準＞1．(8)に本対策の規定を以下の通り汎用的な内容で追加し、解説に上記説明を盛り込むことを想定。

(想定される追加規定)	設	特	他	自	ユ
インターネットの経路情報等制御信号のうち不要なものの送受信を防ぐために有効な機能を設けること。	◎	◎	◎	―	―

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に係る対策と解説（その2）

・経路情報の瞬間的かつ急激な増加を考慮した設計とすること。

平成29年8月に発生した大規模インターネット障害においては、約10万件を超える情報（障害発生当時、一度に約2年分の経路情報に相当。）が配信されたことが原因のひとつとなった。

対策として、同様の障害を想定し十分な余裕をもった処理能力を確保することが考えられるものの、不要な経路制御の送受信を防ぐために有効な機能を設ける観点から設計を行うことも有効である。

しかしながら、こうした機能が自らの利用者や他事業者に影響を与える恐れがあることに留意する必要があるほか、経路情報の瞬間的かつ急激な増加を考慮しないことによる影響についても留意する必要がある。

【想定される安信基準等への反映】

別表第2　管理基準＞第3. 方法＞1. (3)イの以下の通り汎用的な内容で追記し、解説に上記説明を盛り込むことを想定。

(想定される規定の改正)※改正部分は下線部	設	特	他	自	ユ
トラヒックの瞬間的かつ急激な増加及び<u>インターネットの経路情報等</u>制御信号の増加の対策を講じた設計とすること。	◎	◎	「－」から「◎」に改正	－	－

・将来の経路情報の増加を考慮した設計とすること。

現状において、インターネットの経路情報は、日々増えているところであり、ルーターの設計においては経路情報の将来的な増加（瞬間的かつ急激な増加を除く。）の見通しを踏まえて検討することが重要である。

【想定される安信基準等への反映】

別表第2　管理基準＞第3. 方法＞　1. (3)アの規定に以下の通り汎用的な内容で追記し、解説に上記説明を盛り込むことを想定。

(想定される規定の改正)※改正部分は下線部	設	特	他	自	ユ
将来の規模の拡大、トラヒック増加（端末の挙動によるものを含む。）、<u>インターネットの経路情報等制御信号の増加</u>及び機能の拡充を考慮した設計とすること。	◎	◎	◎	◎	◎

・事故又は障害発生時に迅速な原因分析や状況把握等のため、電気通信事業者間での情報共有を含め、複数のルートを活用し幅広く情報収集に努めること。

インターネットにおける障害においては、まず、発生した事象が自社単独で起きている事象なのか、他の電気通信事業者でも同様に起きている事象なのかどうか、他の電気通信事業者がどのように復旧対応したかを把握することが、自らの対応策を検討する上で大変重要であり、自社内の状況確認に加え、必要に応じて契約関係等がある電気通信事業者との状況確認や、ネットワーク技術者間の情報交換など一定程度の取り組みが行われている。

誤った経路情報やサイバー攻撃による障害などネットワークをまたがって発生する障害については、障害の発生状況や影響範囲、収束状況などの把握が困難な場合があることから、報道やSNS、総務省への確認等を通じて幅広く情報収集を行うことが有効である。

【想定される安信基準等への反映】

別表第2　管理基準＞第3．方法＞2．(1)に本対策(情報収集に係る部分)の規定を以下の通り追加し、解説に上記説明を盛り込むことを想定。

(想定される追加規定)	設	特	他	自	ユ
事故又は障害発生時に迅速な原因分析、状況把握及び復旧対応等のため、電気通信事業者間での情報共有を含め、複数のルートを活用し幅広く情報収集に努めること。	◎	◎	◎	○	○

・契約関係等がある事業者(海外の事業者を含む。)との障害対応時の連絡先を把握しておくこと。

事故又は障害発生時に有益な情報共有が行われるよう、直接接続関係にあり、契約を締結している事業者(海外の事業者を含む。)との障害対応時の連絡先を把握しておくことが重要である。

【想定される安信基準等への反映】

別表第2　管理基準＞第3．方法＞2．(1)アの規定に含まれる対策であり、解説に上記説明を盛り込むことを想定。

(現行の規定)	設	特	他	自	ユ
迅速な原因分析のための関連事業者等(接続先、委託先、製造業者等をいう。)との連携を図るよう取り組むこと。	◎	◎	◎	○	○

ネットワーク構成と利用者周知に係る対策と解説

・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。

重要な回線については事故または障害の発生時に大きな影響を受ける恐れがあることから、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、冗長化を図ることが重要である。

【想定される安信基準等への反映】

別表第2　管理基準＞第3．方法＞1．(3)に本対策の規定を以下の通り追加し、解説に上記説明を盛り込むことを想定。

(想定される追加規定)	設	特	他	自	ユ
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。	―	―	―	○	○

・インターネットにつながりにくい障害が発生した場合に、速やかに利用者に対して公開すること。

インターネットにつながりにくい障害であって、接続先や他の事業者のネットワークに起因するものの場合、自社に原因がないもの又は自社に原因があるか不明なものについては、迅速な原因分析や状況把握が困難である可能性がある。そのため、利用者への情報提供に時間を要する可能性があるが、情報提供の遅れが利用者の混乱を拡大させる恐れがある。法人ユーザーの顧客が多数存在する場合は混乱が相当規模に発展する恐れもある。

そのため、利用者の混乱を防止する観点から発生事実のみであっても利用者に公開することが重要と考えられる。なお、対象が特定の法人ユーザーや特定の等限定的な場合は、個別に情報提供する方が、無用な混乱を防ぐ観点から適当と考えられる。

また、あらかじめ、その周知内容を決めておくことが重要と考えられる。

【想定される安信基準等への反映】

別表第2　管理基準＞第3．方法＞2．(2)アの規定に以下のとおり汎用的な内容を追記し、解説に上記説明を盛り込むことを想定。

(想定される追加規定)※改正部分は下線部	設	特	他	自	ユ
事故・ふくそう<u>その他障害</u>が発生した場合に、速やかに利用者に対して公開すること。	◎	◎	◎	―	―

（参考）情報通信ネットワーク安全・信頼性基準概要

● 情報通信ネットワーク全体から見た安全・信頼性対策について網羅的に整理、検討を行い、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持・運用等を総合的に取り入れた、安全・信頼性に関する推薦基準（ガイドライン）を作成。

安全・信頼性基準

設備等基準・・・ 情報通信ネットワークを構成する設備及び情報通信ネットワークを構成する設備を設置する環境の基準（65項目165対策）

設備基準 47項目116対策	1.一般基準 （15項目65対策）	2.屋外設備 （17項目22対策）	3.屋内設備 （8項目13対策）	4.電源設備 （7項目16対策）
環境基準 18項目50対策	1.センタの建築 （4項目13対策）	2.通信機器室等 （6項目22対策）	3.空気調和設備 （8項目15対策）	

管理基準・・・ 情報通信ネットワークの設計、施工、維持及び運用の管理の基準 （ 43項目174対策）

方針 9項目9対策	1.全体的・部門横断的な設備管理 （3項目3対策）	2.関係法令等の遵守 （1項目1対策）	3.設備の設計・管理 （2項目2対策）	4.情報セキュリティ管理 （3項目3対策）
体制 18項目45対策	1.J情報通信ネットワークの管理体制 （2項目8対策）	2.各段階における体制 （16項目37対策）		
方法 16項目120対策	1.平常時の取組 （13項目98対策）	2.事故発生時の取組 （2項目16対策）	3.事故収束後の取組 （1項目6対策）	

(1) 情報セキュリティポリシーの策定 → 情報セキュリティポリシー策定のための指針

(2) 危機管理計画の策定 → 危機管理計画策定のための指針