

技術検討作業班の検討事項について

平成30年3月16日

事務局

検討経緯

- 近年、インターネットから操作可能な家電やスマートメーター等の利用が進む等、IoTサービスが広く社会に普及しつつあり、今後、国民生活や企業の社会経済活動に対する影響力は、より一層大きくなっていくものと考えられる。
- こうしたIoTサービスの普及に伴い、それを支える通信ネットワークについても、技術革新による高機能化に加え、設備構成の複雑化や利用形態の多様化が急速に進展している。
- このような中、平成29年12月より、今後導入される様々なIoTサービスを安心して安定的に利用できるネットワーク環境を確保することを目的として、IPネットワーク設備委員会において、現行の電気通信設備の技術基準や関連制度について検証し、IoTの普及に伴うネットワークの高度化や利用形態の多様化を踏まえた電気通信設備に係る技術的条件について検討することとなった。
- さらに、円滑なインターネット利用環境の確保に関する検討会や電気通信事故検証会議における検討を踏まえ、「大規模なインターネット障害発生時の対策」や「IoT機器を含む脆弱な端末設備のセキュリティ対策」についても、平成30年3月より同委員会において追加検討することとなった。

検討事項

「IoTの普及に対応した電気通信設備に係る技術的条件」

答申を予定する時期

平成30年7月頃

(1) IoTに対応した電気通信設備の技術的条件

新たなIoT用無線通信サービスの導入や通信設備のソフトウェア化等の進展により、ネットワーク設備や端末設備の利用が多様化する中、現行の技術基準や情報通信ネットワーク安全・信頼性基準等の有効性を検証し、必要に応じて見直しの検討を行う(IoT機器を含む脆弱な端末設備のセキュリティ対策に係る検討を含む。)

(2) IoTサービスの安全・信頼性を確保するための資格制度等の在り方

IoT時代のネットワーク設備や端末設備の多様化を踏まえ、電気通信主任技術者や工事担任者に求められるスキルや役割等を検証し、資格制度等の在り方について検討を行う。

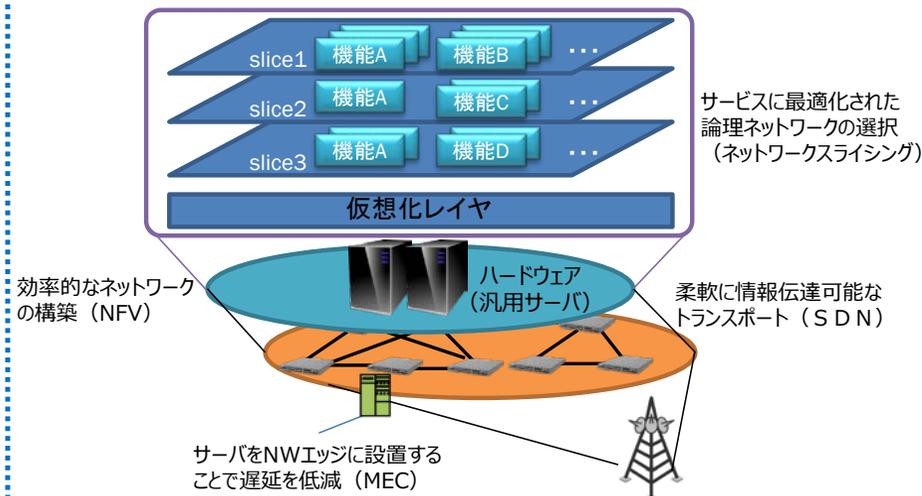
(3) IoT時代における重大事故に関する事故報告等の在り方

今後、IoTサービスが多様化し、従来の設備故障以外を原因とした事故が増加していくことが想定される中、IoT時代における重大事故に関する事故報告の在り方について検討を行う(大規模なインターネット障害発生時の対策に係る検討を含む。)

(4) その他

新たな技術を活用した通信インフラの維持方策や、端末認証の在り方などIoT時代に対応するための課題を整理し、必要な検討を行う。

ネットワーク技術のソフトウェア化等の進展



新たなIoT用無線通信サービス (LPWA等)の開始



技術検討作業班の設置について

- 大規模なインターネット障害発生時の対策については、円滑なインターネット利用環境の確保に関する検討会及び電気通信事故検証会議において方向性の検討を行っていたこと、LPWAの事故報告基準の在り方については、論点がおおむね整理されてきたことから、本委員会の下に設置している技術検討作業班(※)において詳細の検討を進めることとする。

※「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運営方針」に基づき、平成17年11月に設置。

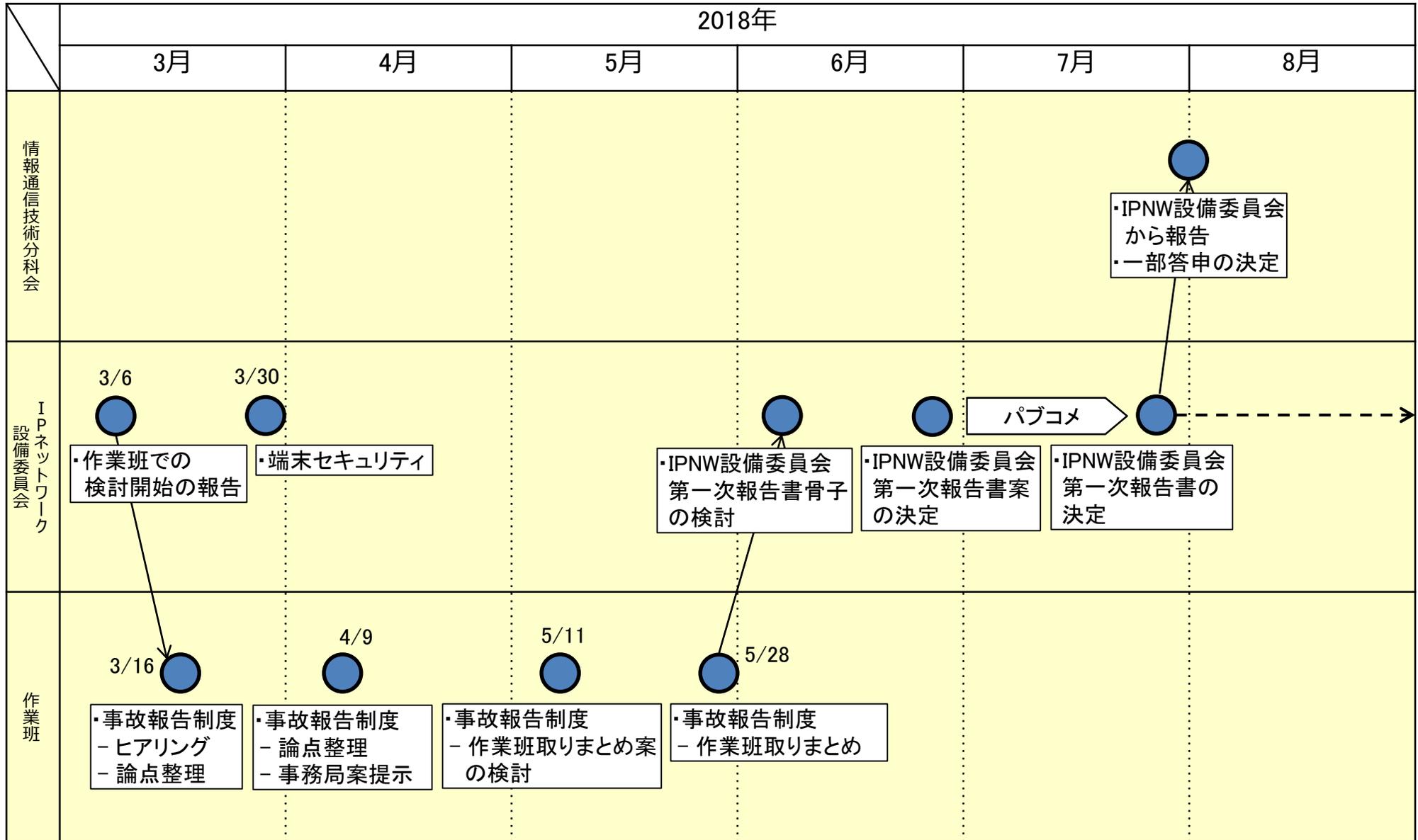
- 検討課題の性質に鑑み、技術検討作業班は、学識経験者、関係事業者及び関係事業者団体等からの参加を得ることとし、次ページのと通りの構成とする。

IPネットワーク設備委員会における検討課題の取扱いについて

- 今後、IPネットワーク設備委員会において論点が整理された検討課題については、同じく本委員会の下に設置している技術検討作業班において詳細の検討を進めることとする。

- (主任) 内田 真人 早稲田大学 基幹理工学部 情報理工学科 教授 ※敬称略
- 大内 良久 KDDI株式会社 技術統括本部 運用本部 運用品質管理部 部長
- 岡田 昌己 エヌ・ティ・ティ・コミュニケーションズ株式会社 カスタマサービス部 危機管理室長
- 尾形わかは 東京工業大学 工学院 情報通信系 教授
- 小畑 和則 株式会社NTTドコモ R&D戦略部 担当部長
- 木村 孝 一般社団法人 日本インターネットプロバイダー協会 会長補佐
- 喜安 明彦 一般社団法人 電気通信事業者協会 安全・信頼性協議会 副会長
- 小林 和則 株式会社NTTドコモ 災害対策室長
- 小林 努 株式会社インターネットイニシアティブ サービス基盤本部 副本部長
- 小林真寿美 独立行政法人 国民生活センター 相談情報部 相談第2課 課長
- 高橋 範 株式会社ソラコム 事業開発マネージャー
- 西川 嘉之 UQコミュニケーションズ株式会社 渉外部 部長
- 花石 啓介 日本電信電話株式会社 技術企画部門 災害対策室長 兼 ビジネスプロセス戦略担当 担当部長
- 日比 学 京セラコミュニケーションシステム株式会社 LPWAソリューション事業部 LPWAソリューション部 副責任者
- 福島 敦 株式会社ジュピターテレコム 技術運用本部長補佐
- 堀内 浩規 一般社団法人 日本ケーブルテレビ連盟 理事 兼 通信制度部長
- 松本 佳宏 株式会社ケイ・オプティコム 計画開発グループ グループマネージャー
- 向山 友也 一般社団法人 テレコムサービス協会 技術・サービス委員会委員長
- 矢入 郁子 上智大学 理工学部 情報理工学科 准教授
- 山口 琢也 ソニーネットワークコミュニケーションズ株式会社 ネットワーク基盤事業部門 ネットワーク部 ネットワーク運用課 課長
- 渡部 康雄 ソフトバンク株式会社 技術管理本部 業務管理統括部 技術渉外企画部 部長

今後のスケジュール



(参考)円滑なインターネット利用環境の確保 に関する検討会

➤ 近年、国内外において、大規模なサイバー攻撃によりインターネットに障害が生ずる事例が複数発生

国内

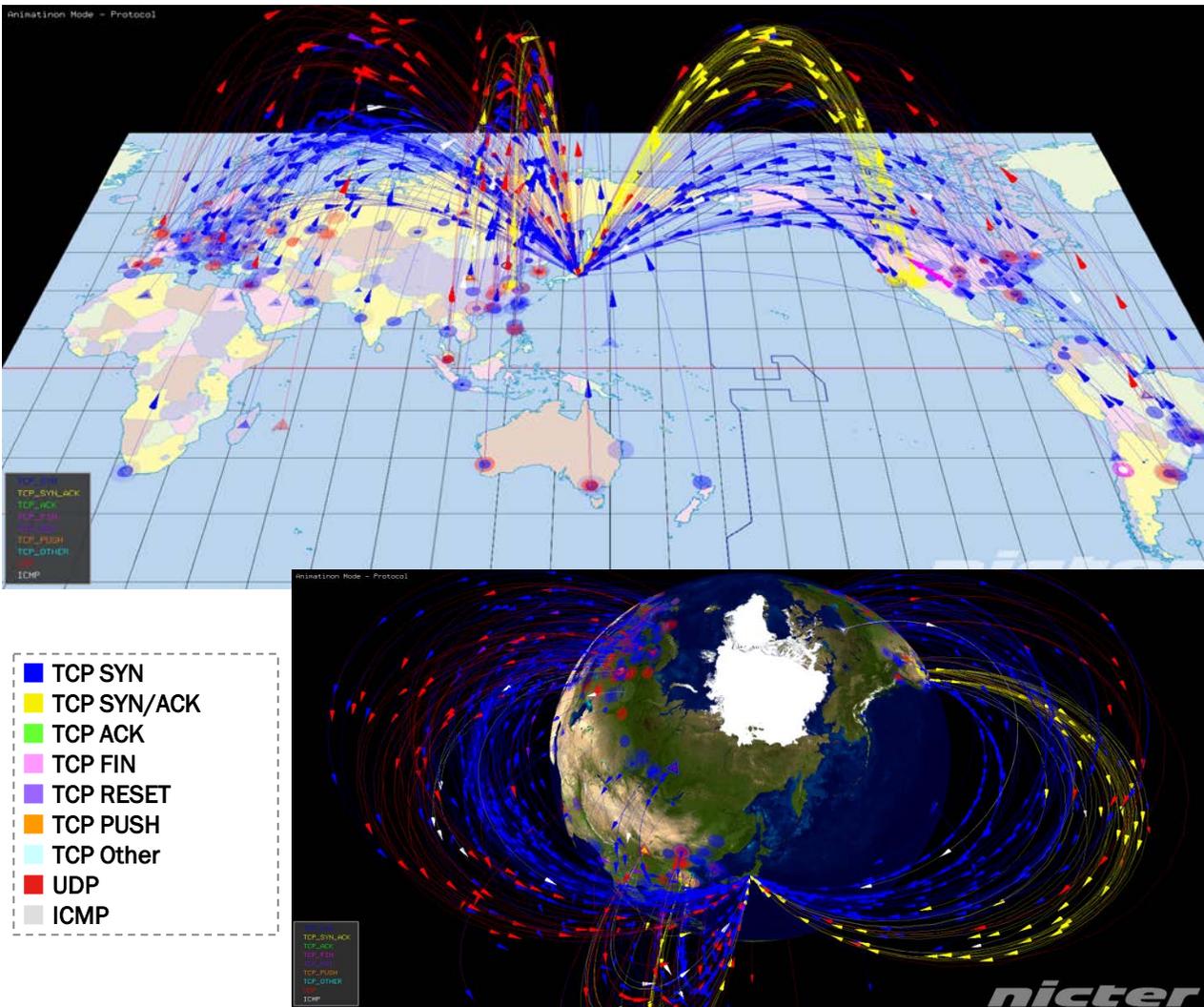
2015年12月14日	<ul style="list-style-type: none"> ・ DNS サーバがDDoS 攻撃を受け、一部の電気通信事業者において、<u>数時間にわたりDNSサーバへの接続障害が発生</u>
2016年8月29日～9月2日	<ul style="list-style-type: none"> ・ 一部の電気通信事業者において、権威DNSサーバ（あるドメイン名に対するIPアドレス等の情報を管理しているDNSサーバ）が外部からのDoS攻撃を受け、<u>ホスティングサービスを中心に大きな障害が断続的に発生</u>

海外

2016年9月13日	<p>【Akamai（米国）】</p> <ul style="list-style-type: none"> ・ サイバーセキュリティ専門ジャーナリストのBrian Krebs氏が運営するブログに対し、Mirai※に感染した約18万台のIoT機器から約620Gbpsに及ぶDDoS攻撃が発生 ・ 同氏に無償でホスティングサービス及びDDoS攻撃緩和サービスを提供していたAkamaiは、サーバーへの負荷に耐えきれず、有料顧客へのサービスを優先するため同氏に対するサービスを停止
2016年9月22日	<p>【OVH（フランス）】</p> <ul style="list-style-type: none"> ・ 自社保有サーバに対し、Mirai※に感染したとされる約14万台以上のIoT機器から、<u>最大1.5Tbpsとなる世界最大規模のDDoS攻撃が発生</u> ・ 南欧諸国からOVHのサーバーを利用するサービスへのアクセスの遅延が発生
2016年10月21日	<p>【Dyn（米国）】</p> <ul style="list-style-type: none"> ・ Dyn社のDNSサーバに対し、Mirai ※に感染し攻撃に関与した約10万台のIoT機器から<u>1.2Tbpsに及ぶとされるDDoS攻撃が発生</u> ・ <u>世界各国の様々な大手顧客サイト（Twitter、Netflix、Spotify、英国政府ウェブサイト等）に数時間にわたりアクセス障害が断続的に発生</u>

※ IoT機器に自動的に感染し、攻撃者からの指示に応じて感染した機器を踏み台としたDDoS攻撃を実施する等の機能を有するマルウェア

- ▶ 国立研究開発法人 情報通信研究機構 (NICT) では、未使用のIPアドレス30万個 (ダークネット) を活用し、グローバルにサイバー攻撃の状況を観測



- ・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化
- ・色: パケットごとにプロトコル等を表現

1年間で観測されたサイバー攻撃回数

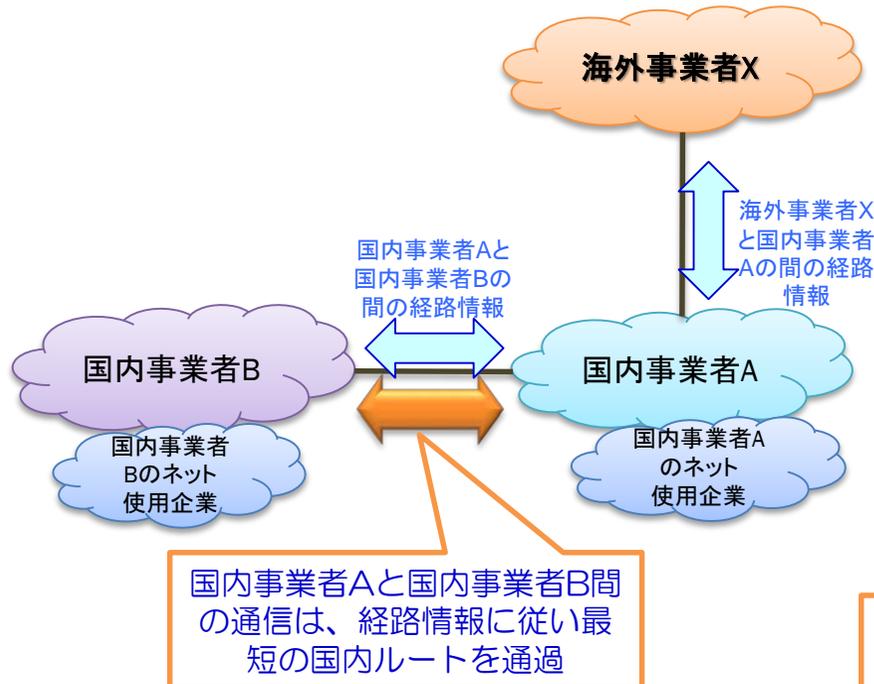
(パケット数(億))

**IoT機器を狙った
攻撃は約5.8倍**

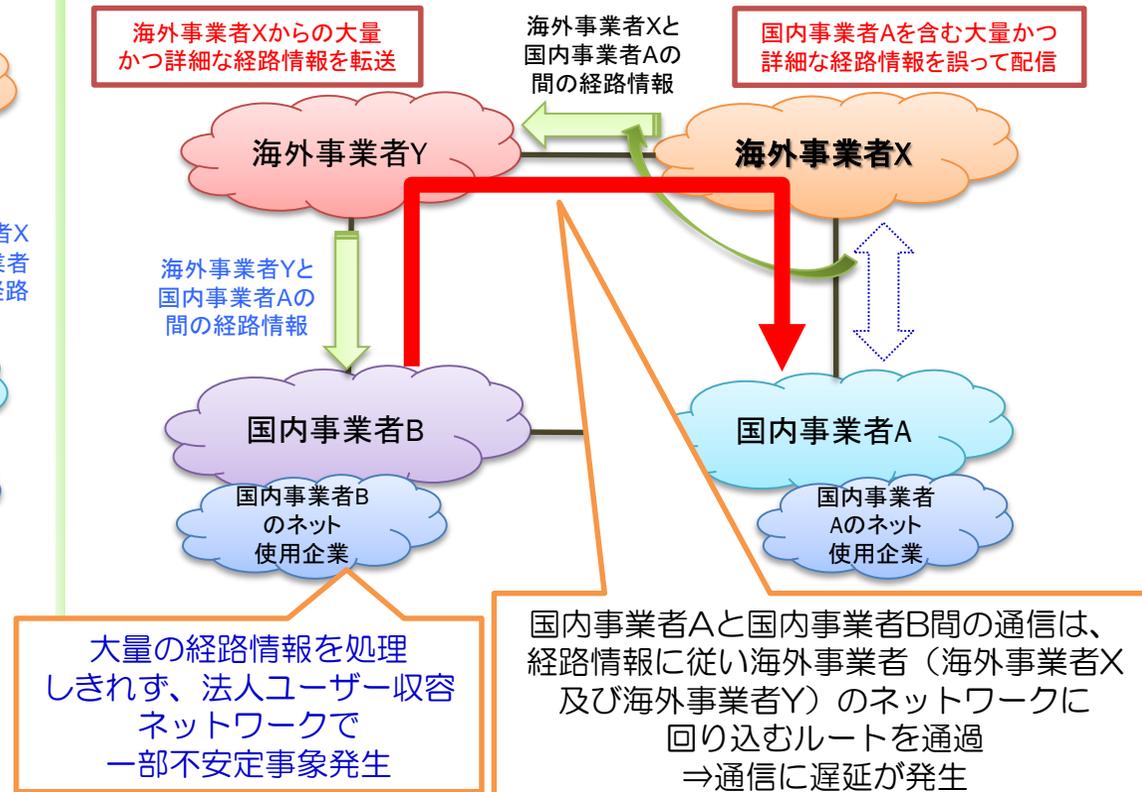


- 昨年8月25日、海外事業者Xが行う通信経路設定の誤りが原因となり、我が国の電気通信事業者（国内事業者A、国内事業者B）の一部の回線や設備に過大な負荷がかかったことにより、インターネットに障害が発生

本来の通信経路



今回の障害時の通信経路



- 総務省では、近年サイバー攻撃等によりインターネットに重大な支障が発生していることを踏まえ、電気通信事業におけるこれらの障害への対処を促進することを目的として、「円滑なインターネット利用環境の確保に関する検討会」を以下のとおり開催。

目的

- 近年、増加するIoT機器を悪用したサイバー攻撃等によりインターネットに重大な障害が発生している。さらに、2020年の東京オリンピック・パラリンピック競技大会に際して日本に対する大規模なサイバー攻撃の発生が懸念されている。このため、電気通信事業においてインターネットの障害を防ぐ適切な対策が講ぜられるための方策について検討を行う。

検討事項

- (1) 電気通信事業者によるサイバー攻撃等に起因したインターネットの障害の防止措置
- (2) 電気通信事業者等によるインターネットの障害に関する情報共有の在り方
- (3) IoT機器を含む脆弱な端末設備への対策
- (4) その他

検討会構成員 (○:座長)

遠藤 信博	日本電気株式会社 代表取締役会長
佐伯 仁志	東京大学大学院 法学政治学研究科 教授
佐々木良一(○)	東京電機大学 未来科学部 教授
宍戸 常寿	東京大学大学院 法学政治学研究科 教授
長田 三紀	全国地域婦人団体連絡協議会 事務局長
藤本 正代	富士ゼロックス株式会社 パートナー、 情報セキュリティ大学院大学 客員教授
森 亮二	英知法律事務所 弁護士
吉岡 克成	横浜国立大学大学院環境情報研究院 先端科学高等研究院 准教授

- 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。

1 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。

2 電気通信事業者によるDDoS攻撃等に対する防止措置の推進

- 【対策】
- ・ 攻撃の事前予防のための、マルウェア感染の可能性が高い端末利用者に対する注意喚起
 - ・ 指令サーバ*のブラックリスト等を用いたマルウェア感染が疑われる端末等の検知
 - ・ マルウェア感染者等の通信を利用した未知の指令サーバの検知

※ マルウェア感染端末にサイバー攻撃を命令する機器で、このような機器と通信する端末はマルウェア感染が疑われる。

【課題と今後の対応】 通信の秘密等との観点から、具体的な実施方法や留意すべき事項等について精査。

3 情報共有、分析基盤の構築

【対策】 第三者機関を中心とした情報共有基盤を構築

- ∴ ①IoT機器の増加に伴い個別の情報共有が困難となっているため、情報共有の結節点が必要
- ②情報を集約して集中的に分析、検証することで、対策の実効性向上が可能

【課題と今後の対応】

通信の秘密に該当する情報を関係者間で共有することから、実施に向けて具体的な体制等を検討し、裏付けとなる法制度を整備。

IPネットワーク設備委員会において追加検討

4 IoT機器を含む脆弱な端末設備のセキュリティ対策

【対策】 IoT機器等の端末設備において、基本的なセキュリティ対策を実施

【課題と今後の対応】

国際競争力確保等の観点も踏まえ、IoTサービスや機器の普及の阻害とならないよう、諸外国の検討状況等を踏まえた上で関係者から広く意見聴取し、検討。

IPネットワーク設備委員会において追加検討

5 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ルータの設定につき規定するとともに、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を検討。

(参考)電気通信事故の報告に係る関連制度

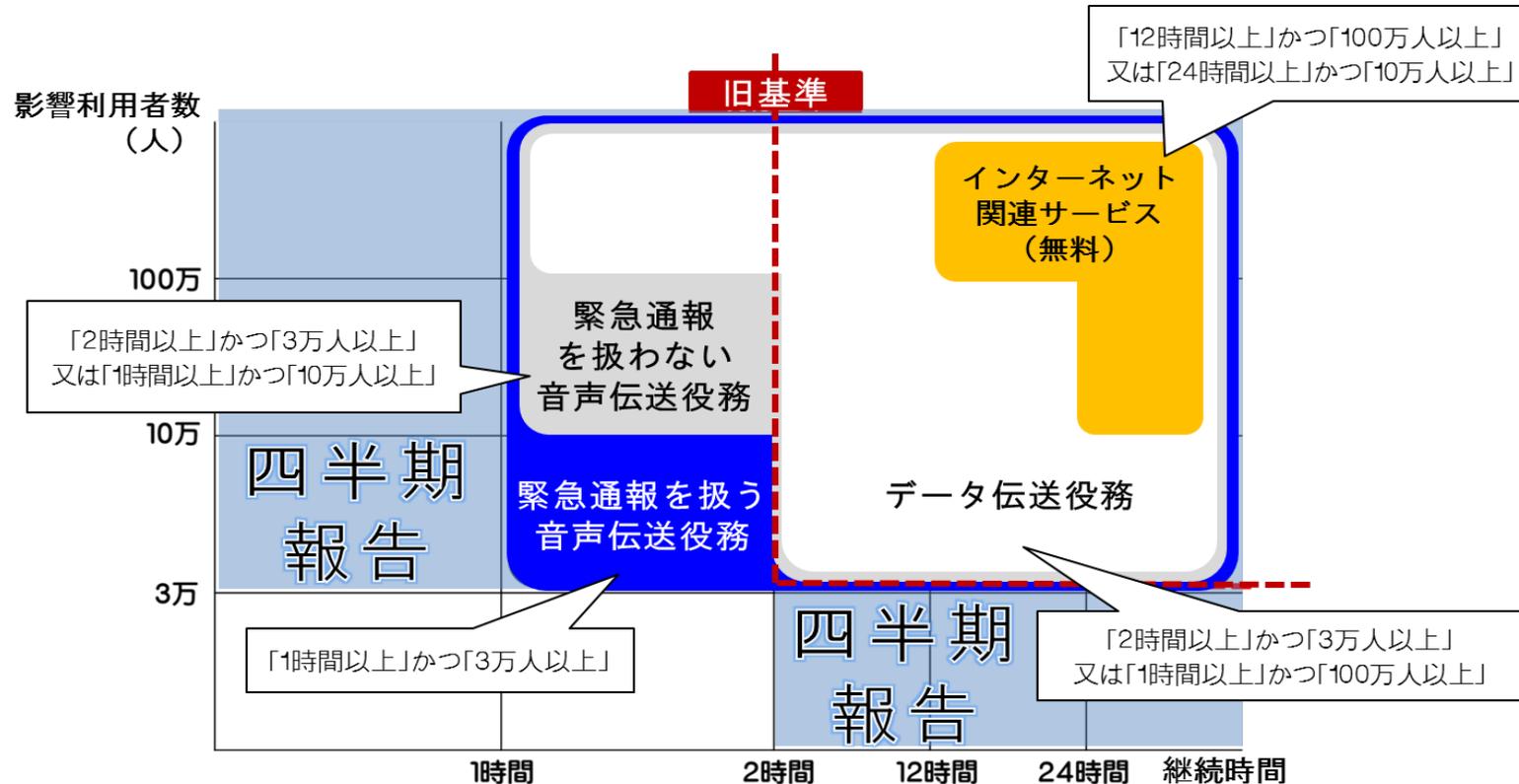
○ 通信サービスを提供する上での基盤となる電気通信設備について、サービス中断等の事故が発生した場合、国民生活や社会経済活動に深刻な影響を与えかねないため、安全・信頼性確保に関する制度を設けている。

強制基準	技術基準	<p><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)</p> <p><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、電氣的条件、責任の分界 等)</p>
	管理規程	<p><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</p>
ガイドライン	安全・信頼性基準	<p><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</p>
監督責任	電気通信設備統括管理者	<p><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</p>
	電気通信主任技術者	<p><事業用電気通信設備の「工事、維持・運用」を監督> 電気通信事業者は資格者証の交付を受けている者を選任し事業用電気通信設備に関して監督させる</p>
	工事担任者	<p><端末設備等の「接続の工事」を実施等> 利用者は資格者証の交付を受けている者に端末設備等の接続に係る工事を実施又は実地で監督させる</p>
報告義務	事故報告	<p><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</p>

- 電気通信事業は、社会経済活動に必要なサービスを提供する公共性の高い事業であり、継続的・安定的なサービス提供が求められる。
- そのため、全ての電気通信事業者に対し、一定の規模を超える事故が生じたときは、重大事故として総務大臣への報告義務を課しており、総務省において、必要に応じて再発を防止するための適切な措置を講ずることとしている。

総務省への報告義務のある電気通信事故は、次の二つに大別。

- ① **重大な事故**：サービスごとの**影響利用者数・継続時間の基準**※に該当する事故 → 事故後30日以内に報告書を提出
- ② **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



○ 全ての電気通信事業者に対して、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・信頼性に関するガイドライン*を策定している。 ※「情報通信ネットワーク安全・信頼性基準」(昭和62年郵政省告示第73号)

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)

- (1) 情報セキュリティポリシーの策定
- (2) 情報セキュリティポリシーの公表
- (3) 危機管理計画の策定

情報セキュリティポリシー策定のための指針

危機管理計画策定のための指針

体制
18項目45対策

1.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

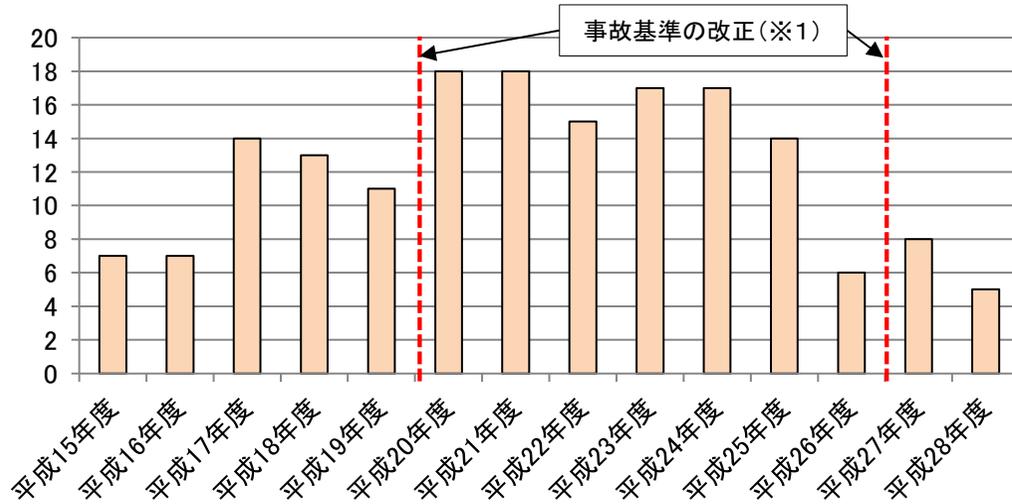
1.平常時の取組
(13項目98対策)

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)

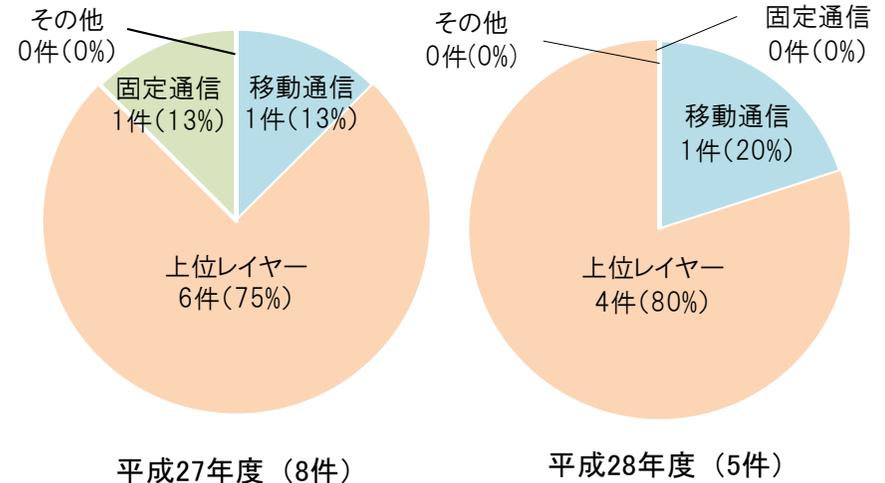
- 平成28年度の電気通信事故(四半期報告)の総件数は6,293件。(前年度比+104件)。
- 重大な事故は、平成25年度までは毎年15件程度発生。平成26年度以降は一桁台。平成28年度に発生した重大な事故は5件(前年度比-3件)。
- 近年の傾向として、上位レイヤーサービス関係の重大事故の割合が高まっている。

<重大な事故の発生件数の推移>



※1 平成20年度の報告分から、電気通信役務の品質が低下した場合も事故に該当することとなり、さらに平成27年度の報告分から、電気通信役務の区分に応じ、重大な事故に該当する基準が定められたことから、年度ごとの推移は単純には比較できない。

サービス別の重大な事故の内訳



「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。」【総務省「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】

電気通信事故検証会議の設置(平成27年5月)

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

課題

● 報告事業者への
フィードバック

● 業界内共有
● 技術基準等へ反映

- 平成27年度電気通信事故に関する検証報告 報告書
http://www.soumu.go.jp/main_content/000431571.pdf
- 平成28年度電気通信事故に関する検証報告 報告書
http://www.soumu.go.jp/main_content/000500038.pdf