資料131－1

情報通信審議会　情報通信技術分科会

「ネットワークのIP化に対応した電気通信設備に係る技術的条件」のうち「IoTの普及に対応した電気通信設備に係る技術的条件」に関する検討事項の追加について

平成30年2月13日
IPネットワーク設備委員会

1.　円滑なインターネット利用環境の確保に関する検討について

サイバー攻撃によるインターネットの障害に関する近年の事例

➢ 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	・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、数時間にわたりDNSサーバへの接続障害が発生
2016年8月29日～9月2日	・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、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

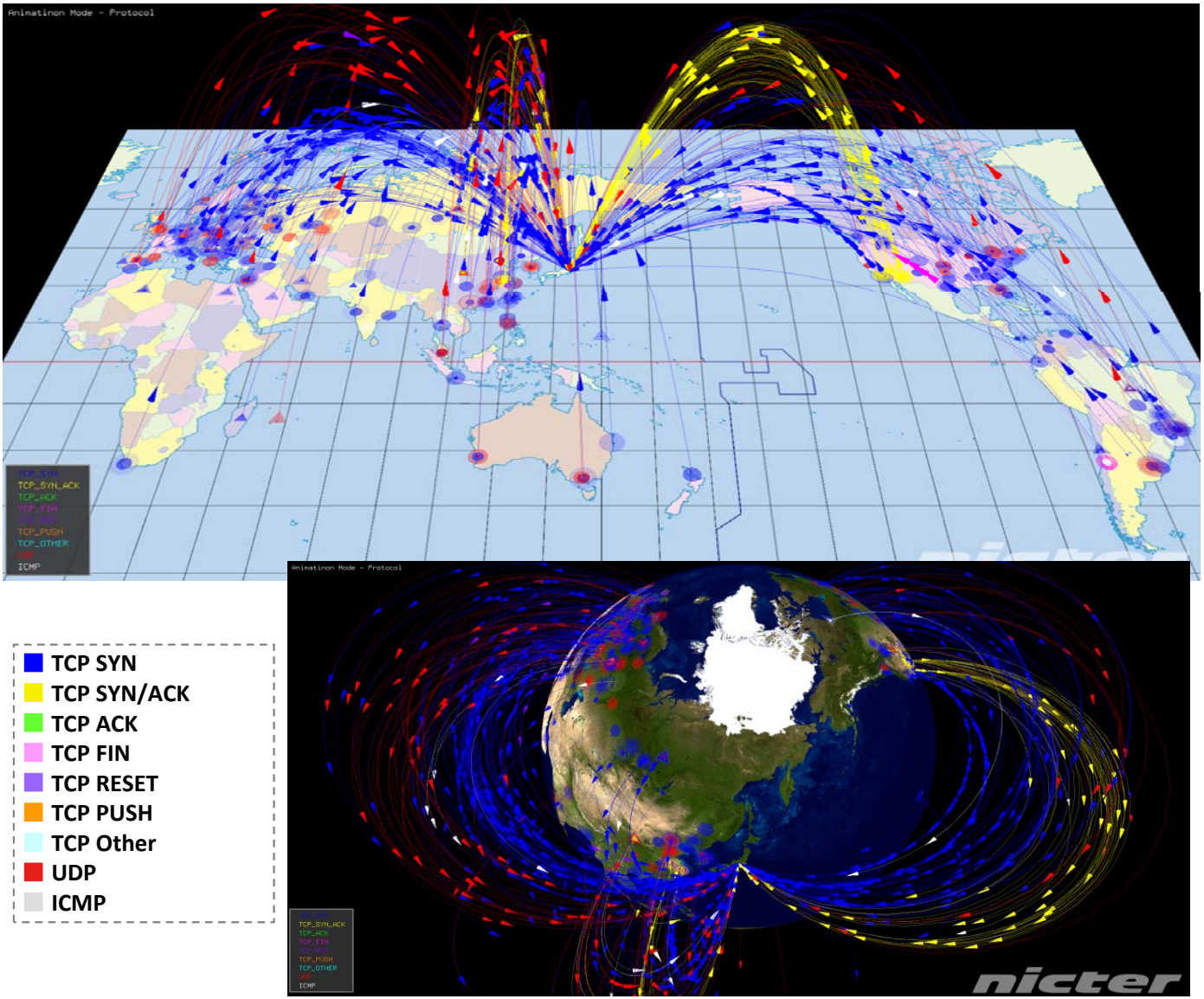
海外

2016年9月13日	【Akamai（米国）】 ・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	【OVH（フランス）】 ・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、最大1.5Tbpsとなる世界最大規模のDDoS攻撃が発生 ・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	【Dyn（米国）】 ・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1.2Tbpsに及ぶとされるDDoS攻撃が発生 ・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

※ 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

IoT機器を狙った攻撃が急増（NICTERによる観測）

➢ 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

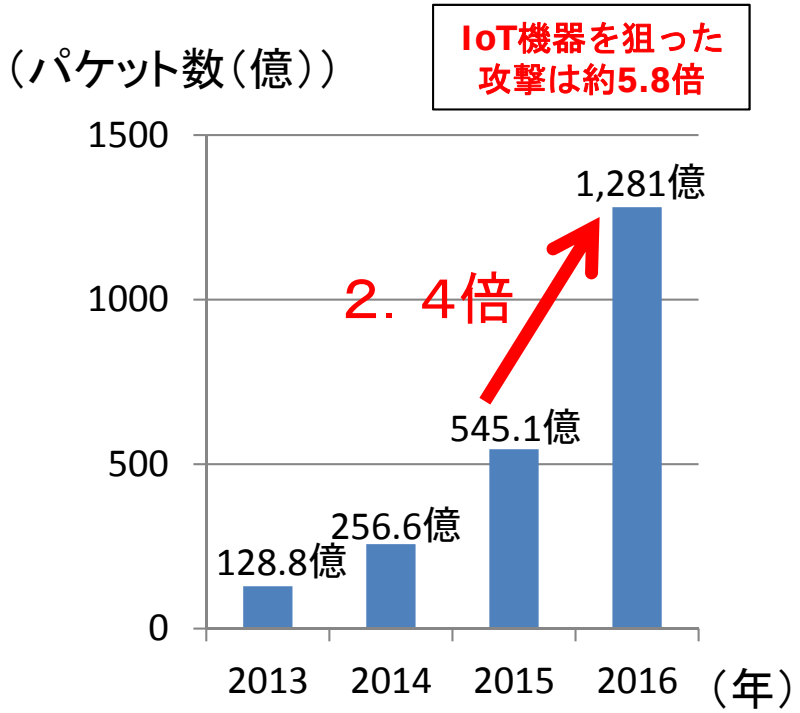


- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

・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

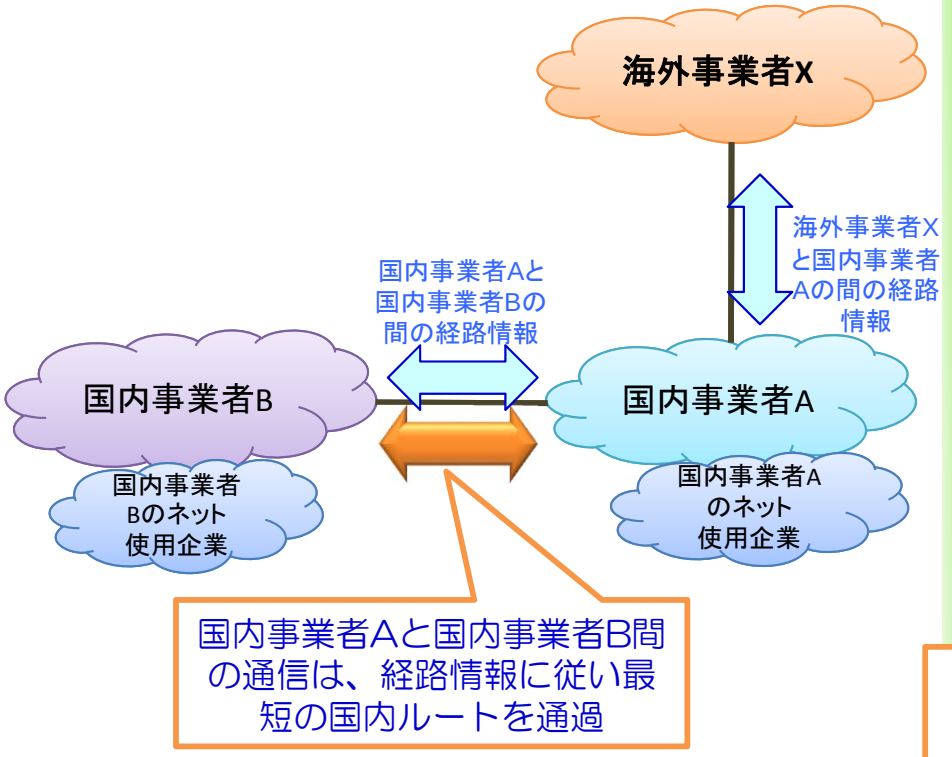
１年間で観測されたサイバー攻撃回数



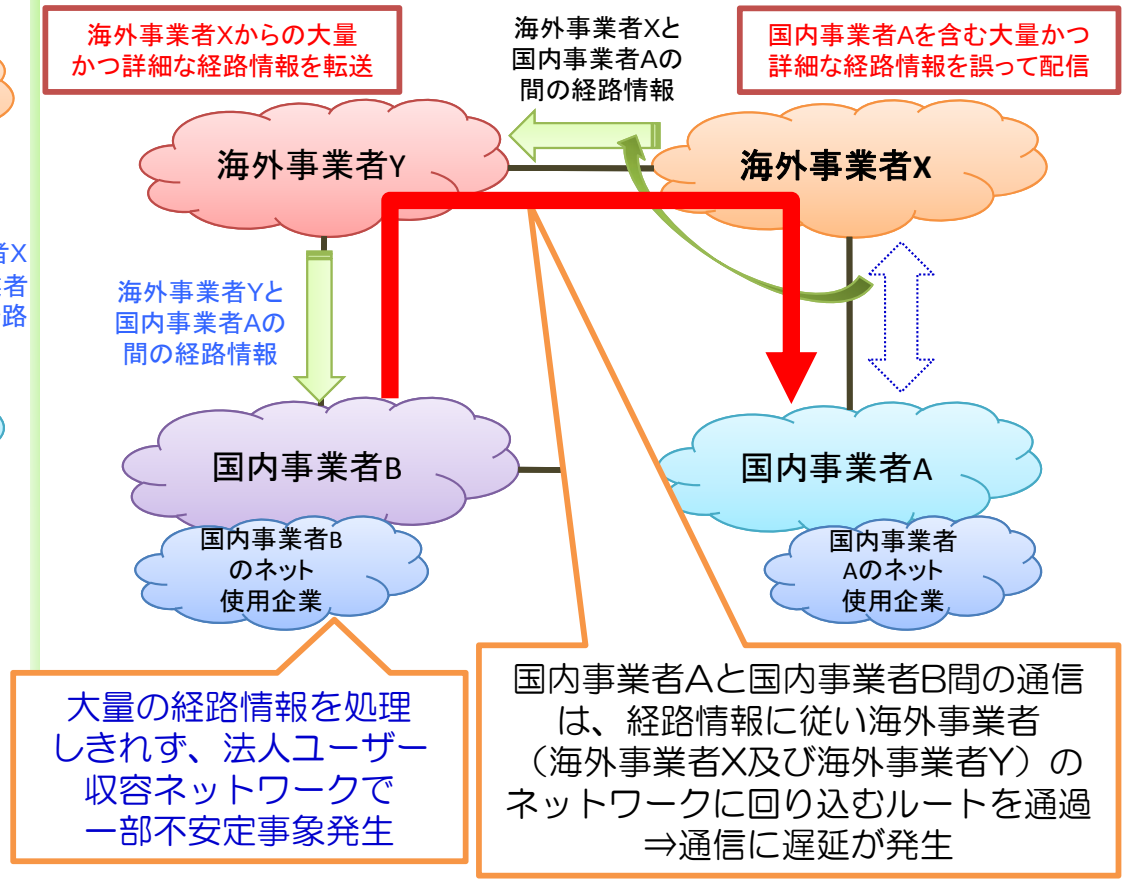
昨年8月に発生した大規模なインターネット接続障害

- 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



今回の障害時の通信経路



円滑なインターネット利用環境の確保に関する検討会

➢ 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

「対応の方向性」概要 - ①

➢ 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。

「対応の方向性」概要 - ②

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。

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。

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。

2. IPネットワーク設備委員会における追加検討について

「IoTの普及に対応した電気通信設備に係る技術的条件」の追加検討

追加検討について

○　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、昨年末より、IPネットワーク設備委員会において、「IoTの普及に対応した電気通信設備に係る技術的条件」の検討を開始。

○　「円滑なインターネット利用環境の確保に関する検討会」で示された対応の方向性のうち、「IoT機器を含む脆弱な端末設備のセキュリティ対策」、「大規模なインターネット障害発生時の対策」について、「IoTの普及に対応した電気通信設備に係る技術的条件」の中で検討を行うことが適当と考えられる。

IPネットワーク設備委員会における検討事項

IoT機器を含む脆弱な端末設備のセキュリティ対策を追加検討

（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。

（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。

大規模なインターネット障害発生時の対策を追加検討

（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。

（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。

今後の検討スケジュール