資料37－1

これまでの委員会における主な議論等について

平成30年3月30日
事務局

IPネットワーク設備委員会におけるこれまでの主な議論

1. 基本的な考え方

・IoTサービスは、現行の制度ではデータ伝送役務に該当するが、データ伝送役務の中でもサービス等の実態に合わせ、さらに基準等を区分けするということも考えられる。

・ネットワークの仮想化・ソフトウェア化の進展に伴い、ソフトウェア制御によるリソース運用が物理装置を共有する別の論理ネットワークに影響を与える可能性があり、責任の所在等があいまいになる可能性がある。

・ネットワークの仮想化技術の進展により、ハードウェアの汎用化が進むことが期待される一方、ソフトウェアの複雑化により、設定ミス等のリスクが懸念される。

・従来の電気通信サービスは、人の利用を前提とした制度設計になっている。一方、IoT時代の電気通信サービスは、数時間サービスが停止しても大きな影響がないようなモノ向けのサービスや、人の利用を想定していても用途が限定されたサービスが増えると考えられるため、必要に応じて制度の見直しの検討を行うことが重要。

・バーチャルキャリアが提供する役務の区間には、MVNOとなる区間もあれば、利用者により回線が共有される区間もある。また、専用線的に役務が提供される一方で、クラウドにもつながる役務区間があるなど、注目する区間により基準の考え方が変わってくる。

・グローバルプラットフォームプレイヤー等が国内のサービスに影響を与える場合があり、国内法では担保できない可能性もあるので注意が必要。

IPネットワーク設備委員会におけるこれまでの主な議論

2.　IoTに対応した電気通信設備の技術的条件

＜LPWAネットワーク設備の安定運用のための対策について＞

・コア設備がサイバー攻撃を受けると危険であり、冗長・自動復旧等の対策が重要。

・コア設備は、複数のデータセンターで運用され、仮に災害により、一部のデータセンターが停止したとしても、サービスは停止しない仕組みとなっている。仮想化技術を活用し、サーバーの自動交換による障害復旧も可能。

・他事業者から卸電気通信役務を受けている区間について監視を行っており、障害の把握は可能。

・IoTデバイスの要件によって、求められるセキュリティーレベルが異なるため、事業者としては、提供するサービスのセキュリティーレベルや適した用途などをSLA(Service Level Agreement:サービス品質保証)化して提供することや、セキュリティオプションの選択肢を提供することが重要。

・LPWAの特性（用途、通信頻度、機器数、影響度など）を考慮し、法令の適用範囲等について検討が必要。

・アンライセンスバンドを利用するため意図しない障害が発生する。そのため、利用者には、アプリケーション層以上で、リトライやデータの再送を行うこと等により品質を確保することを求めている。また、このようなサービスについては、期待されるサービスレベルに即したガイドライン等を設定する必要がある。

・外部から直接LoRaデバイスに通信を行うことは不可能としており、セキュリティーのリスクは限定的。

＜端末設備のセキュリティ対策について＞

・現在は電気的特性などを規定する端末設備の技術基準に、セキュリティ対策の要件を追加することを検討すべき。

IPネットワーク設備委員会におけるこれまでの主な議論

3. 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

・ネットワークの仮想化の進展に伴い、ソフトウェア人材やセキュリティ技術を十分に持った技術者が必要。

・技術領域は多岐にわたり、従来の伝送線路、交換といったカテゴリでは区分できない技術も増加。

・電気通信主任技術者等の資格者の配置については、LPWA等の新しいサービス形態を踏まえた整理が必要ではないか。

・電気通信主任技術者については、ネットワークの仮想化技術等の新たなスキルが必要。

・現状のニーズを踏まえながら資格制度の内容や試験項目等の設計を行うことが必要。

・現場でIP機器の設定ができるような資格が、間違いなく今後重要になってくるのではないか。

・電気通信主任技術者には、ISMS（情報セキュリティマネジメントシステム）認証の取得等の一定のセキュリティ資格や水準を求めていくべきではないか。

IPネットワーク設備委員会におけるこれまでの主な議論

4. IoT時代における重大事故に関する事故報告等の在り方

＜想定される事故について（主にLPWA関係）＞

・LPWAサービスを含む昨今の通信サービスはクラウドベースとなっていることが多く、クラウドサービスにおける障害が容易に全国規模の障害に発展する可能性がある。

・LPWA端末が定期的にデータの送信を行うようにしており、送信されなくなった場合はネットワーク側でアラートがなる仕組みを用意しているため、LPWA端末が故障等した場合の検知は可能。

＜事故報告の基準について（主にLPWA関係）＞

・LPWAサービスはアンライセンスバンドを利用しており、意図しない障害の発生を防ぐことは困難。そのため、重要度の高い通信には使用されないと思われる。事故報告の基準は、こうしたLPWAサービスの特性（用途、通信頻度、機器数、影響度など）を考慮したものとすべき。

・重大事故に関する報告基準のうち、役務停止による影響利用者数の基準については利用者数が契約者数であれば現状のままで良いが、通信頻度等を踏まえると役務停止の時間の基準については議論が必要。

・利用者数や時間といった基準ではなく、サーバ等のコアネットワークの故障等が発生した際に報告を求めるのが良いのではないか。

・LPWAサービスのようなアンライセンスバンドを利用するサービスについて、外部原因による通信障害と設備故障等による事故をどのように線引きするべきか、検討が必要。

＜事故情報の共有について＞

・他事業者に起因する事故に関する情報共有体制の構築について検討が必要。

IPネットワーク設備委員会におけるこれまでの主な議論

5. その他

＜最新技術を活用した電気通信設備の維持・管理＞

・レーザー、車載カメラ、ドローン等、様々な手段で設備情報を自動収集するとともに、AI技術などを活用してインフラ設備の劣化を自動診断している。

・労働人口減少に伴い、技術の高度化・複合化、AI/ロボットなどの最新技術の活用がより一層必要。

・高所作業や災害対応等にドローン等を活用することで安全性、業務効率をあげることが重要。

前回の委員会における主な議論（端末設備のセキュリティ対策関係）

＜端末設備のセキュリティ対策の必要性について＞

・近年の「Mirai」等による大規模DDoS攻撃を抑止するためには、攻撃の踏み台となるIoT機器がマルウェアに大量感染しないような対策を取ることが重要。

・IoT機器の利用者は、IoT機器が目的どおり動作している限り、攻撃の踏み台となっていることを認知することができないため、脆弱性やソフトウェアのアップデート状況の確認を怠りがちとなる。

・脆弱性の発見されたルータ等を通信事業者がレンタルしている場合は、比較的速やかな対策を取ることが可能だが、売り切り型の場合はユーザへの周知が難しく、対策が進まないといった側面がある。過去の事例では脆弱性のある機器を約80%減らすのに約3年を要した。

＜端末設備のセキュリティ対策を検討する上で考慮すべき事項＞

・DDoS攻撃等は、グローバルに行われるということを認識する必要がある。

・IoT機器は様々な種類のものがあるため、関連各分野の意見を十分に聴取し、協議・検討を進めるべき。

・短期的な対策と中長期的な対策とを考えていく必要がある。

＜セキュリティ対策を求める端末設備の範囲について＞

・IPを使用する全ての機器に対し、セキュリティ対策を求めることが理想的ではあるが、現実的には、セキュリティ対策を行うことが効率的な機器の範囲を明確にし、その範囲で効果的な対策を検討すべきではないか。

・ホームルータ、インターネットカメラ、インターネット家電等のインターネット接続の境界に設置されたり、インターネットと直接通信が可能な機器のセキュリティを確保することが急務。

前回の委員会における主な議論（端末設備のセキュリティ対策関係）

＜セキュリティ対策の内容について＞

・IoT機器には、安価で簡易的なものから高価で高機能なものがあり、一律に高いセキュリティ対策を求めることは難しい。バランスのとれた対策を検討する必要がある。

・不適切な設定や利用者に認知されていない脆弱性を悪用したサイバー攻撃が多いため、パソコンやスマートフォンで通常行われている対策を行うことでIoT機器でも大半の攻撃を防ぐことが可能。

・セキュリティ対策については、ファームウェアの脆弱性が見つかったときのバージョンアップや初期利用時のID・パスワードの変更等の推奨が考えられる。

・機器の機能として、第一に不正アクセスを防ぐ認証機能の実装が必要。また、ファームウェアのアップデート等のセキュリティホール検出時の対処の機能が必要。さらに、こうした機器仕様による対策に加え、適切なパスワードの使用促進等の運用時における対策も重要。

・グローバル市場への展開や国際競争力確保といった観点から、国際標準への準拠を目指すべきだが、IoT機器のセキュリティに関する国際標準は未確立。

・コスト増につながる第三者認証はその必要性を十分吟味すべきであり、国際標準に移行できるよう、指針・ガイドラインに沿った自主規制や、ベンダーによる自己適合宣言といった形を基本とすることが当面は望ましいのではないか。

・コピー複合機の場合、オフィス向けの高級機種では、ISO／IEC15408のCC（Common Criteria）認証を取得している例が多い。

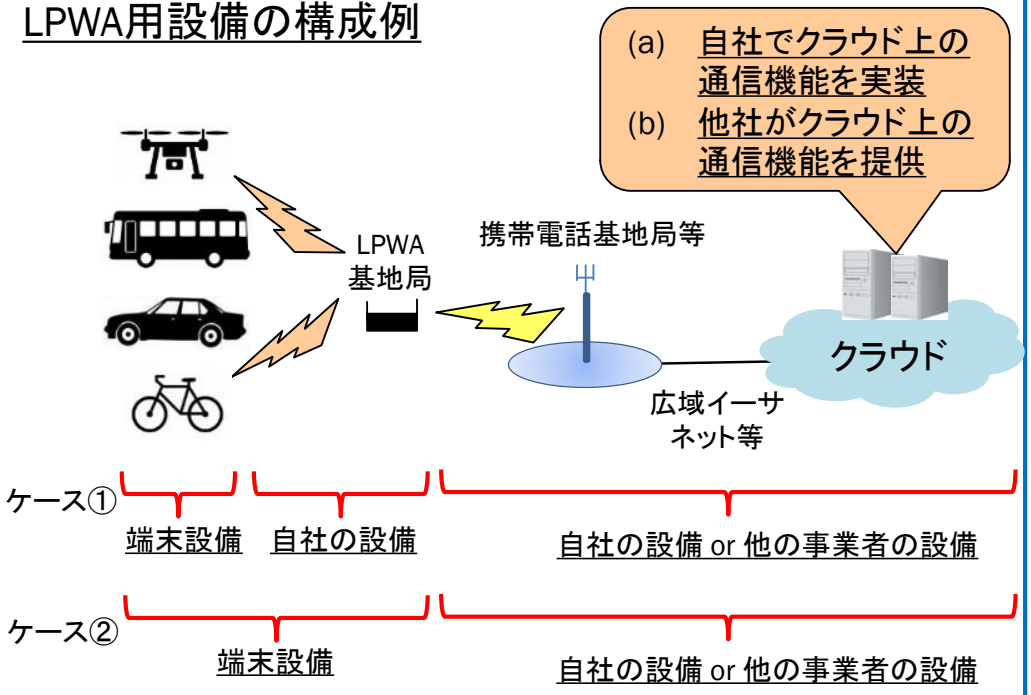
・ファームウェアのアップデート機能については、悪用されてしまうと当該機能がセキュリティホールになり得るという指摘もある。

LPWAサービスの技術基準の適用について

LPWA用設備に適用される主な技術基準

① 役務提供に係る機能に重大な支障を及ぼす故障(電源停止等)の検知
② 交換設備の異常ふくそう対策
③ 耐震対策
④ 屋外設備の気象変化等の外部環境変化への対策
⑤ 役務提供に重大な支障を及ぼすおそれのある設備の分散設置
⑥ 利用者の通信内容を蓄積する設備の防護措置

LPWA用設備の構成例



論点

1. LPWAサービスでは、センサー情報等を集約するクラウド設備に故障があった場合、役務の提供に重大な支障を及ぼすこととなる。

2. LPWA事業者は、クラウド事業者が提供するハードウェアやOS等のプラットフォーム上において通信機能を実装し、役務を提供することが考えられるが、責任の分界や技術基準への適合についてはどのように考えればよいか。

→ クラウド上の通信機能を実装するLPWA事業者に対し、技術基準への適合維持義務が課されるべきではないか。
→ 異常ふくそう対策や設備の分散設置等の技術基準の適合については、プラットフォームの機能を活用することが認められるのではないか。
→ 電源停止の検知等の物理的な措置については、クラウド事業者において対応していることを確認する必要があるのではないか。

3. 一方、他の事業者がクラウド上の通信機能を提供している場合は、当該他の事業者が技術基準に適合していることをLPWA事業者において確認する必要があるのではないか。また、クラウド上の通信機能に異常があった場合には、LPWA事業者が検知できる仕組みが必要ではないか。

4. クラウド上の通信機能を利用するLPWAサービスは、簡易かつ無線局免許を要しない設備のみを用いて提供することが可能であり、設備の故障等が発生したとしても、その復旧は容易と考えられる。このような場合に、電気通信主任技術者の選任要件はどのようにあるべきか。

※原則、電気通信設備を直接管理する事業場ごとの選任かつ都道府県ごとの選任が必要。(アクセスポイントのみを設置して公衆無線LANアクセスサービスを提供する場合等を除く。)

5. LPWA基地局に使用する機器は端末設備にもネットワーク設備にもなり得るが、その場合の技術基準の適用をどう考えるか。