資料40－1

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6月22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

＜資格制度等の在り方について＞

・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。

・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求められるスキル等について＞

・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。

・LPWA等の新しいサービス形態を踏まえた電気通信主任技術者等の資格者の配置について、公衆無線LANアクセスサービスを提供する場合と同様に一部を緩和するべきではないか。

・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。

・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

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（続き）

＜工事担任者に求められるスキル等について＞

・工事担任者に係る現行制度の課題として、工事担任者の法的役割が電気通信回線設備への障害防止に重点が置かれて、セキュリティの確保など利用者サイドに立っていないこと、利用者に対して工事担任者であることの提示が義務付けられていないことなどから、利用者は資格の必要性の認識が希薄であること、電気通信工事形態の進展に伴い、試験科目の見直しは行っているが、資格取得後の最新の知識・技能の習得が図れていないことが挙げられる。

・電気通信工事は近年増加傾向にあると考えるが、工事担任者の受験者数は毎年約10％減少していることから、工事担任者に関する工事の実態等を調査し、その原因・解決方策等を検討する必要があるのではないか。

・現在、適合表示端末機器をプラグジャックや無線で接続する場合は、工事担任者による工事・監督が不要となっているが、物理レイヤの接続と上位レイヤの接続が区別されていない。今後、IoTが普及し様々な機器が出てくる中、工事担任者による工事・監督が必要な範囲について検討が必要ではないか。

・現状の解釈では、電気通信事業者の電気通信回線設備と接続する機器の配下にある機器は内線網扱いとなるため、工事担任者が工事・監督を行う必要もなければ、機器が適合表示端末機器である必要もないことになる。

・工事担任者の試験内容は、大学生が勉強すべき内容も多く、制度のアピール方法を見直してもよいのでは。

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。

・現在は利用者数が報告の基準になっているが、今後、LPWAの普及状況等を見ながら、人命に関わる場合など、サービスの重要性を考慮することについても検討していくことが必要。

・事業法に基づく対策を海外事業者が直接行うことは難しいが、国内事業者を通じて連携することや制度を英訳するなどして海外にアピールすることが重要。

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

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（続き）

＜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。

・事故情報をエンドユーザに周知する場合については、ホームページへの掲載のみならず様々なメディアを通じてアプローチしていくことが必要。

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。

これまでの主な議論（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・目的について＞

・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。

・通信事業者は、通信内容を見ることができないため、IoT機器からの大量通信が正常な通信なのか、DDoS攻撃に加担しているものか判断できない。また、マルウェア感染したIoT機器のみ通信を止めることも難しく、できることは非常に限られている。

・どんなに注意喚起を行っても、対策や対応を行わない、あるいはできない利用者が一定割合で存在するため、利用者に対策・対応を求めることは容易ではない。

・サイバー攻撃は、IoT機器自体の被害に留まらず、実社会の基盤をなす他の環境へ広範かつ多大な影響を及ぼす事態につながる。この対策として、まずはIoT機器の脆弱性を塞ぎ、それを維持することが最も肝要である。

・脆弱な端末設備の使用を防ぐためには、技術基準に規定することが効果的ではないか。

＜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。

これまでの主な議論（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。

・マルウェアに感染している機器の種類は、9割以上が不明だが、分かっている範囲ではインターネットカメラ、デジタルビデオレコーダ、ルータ等が多い。また、海外製品が圧倒的に多いが、国内製品においても、ルータ、ゲートウェイ、ネットワークストレージ、太陽光パネル管理システム、電力デマンド監視システムといった感染事例がある。

・現在はグローバルIPアドレスを有する機器へのインターネット側からの直接的攻撃が主流であり、家庭内の機器に攻撃を行うものは5%程度。そのため、インターネット側からアクセス可能なネットワークサービス（Web管理、telnet等）を使用する機器については、特に脆弱性対策が必要。

・IoT機器によるDDoS攻撃等を抑止するためには、インターネットに直接接続される機器のセキュリティ対策が最も重要。特に、ファイアウォールなどがない状態で、グローバルIPアドレスが設定される端末はリスクが高い。

・現状は、グローバルIPアドレスを持っているものが攻撃の対象となっているが、今後は間接的につながる機器まで攻撃が及ぶことになると想定される。また、非定常的に接続される機器であっても、多くの機器が集まれば、非常に大きな影響を及ぼすような問題を引き起こしかねないため、対策を想定していく必要がある。

・無線のインターフェースを持つIoT機器については、公衆無線通信サービスに影響を及ぼす可能性があり、セキュリティ対策をしっかり行うことが必要。

・端末設備のセキュリティ対策については、電気通信事業者の回線設備に障害を与えない、他の利用者に迷惑を及ぼさないという技術基準の原則の枠内で規定できるのではないか。この場合、これまでの認定の考え方を踏襲すると、認定対象は直接接続されうる機器に限られるが、セキュリティ対策についても同様の考え方として問題ないか。

・セキュリティ対策の対象となる機器を明確化すべき。また、既存製品への対応についても検討が必要ではないか。

これまでの主な議論（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。

・製品に使われているソフトウェアやライブラリを把握することで新規に発見される脆弱性への迅速な対応が可能。また、強制アップデートやユーザ通知、簡易なユーザインタフェースなどによりアップデートを徹底させる仕組みが必要。

・管理画面は不用意にインターネット側からアクセスできる仕様にしないこと。インターネット側からのアクセスが必要な機器については、デフォルトパスワードの使用禁止などユーザに適切な設定を促すことが必要。

これまでの主な議論（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（続き）＞

・アクセス制限がない機器、ハードコーディングされたIDとパスワードを持っている機器、既知の脆弱性が埋め込まれている機器等の出荷を極力避けるべき。また、出荷後のセキュリティの維持のため、脆弱性の修正ができる機能を出荷前から埋め込んでおくことが必要。

・セキュリティの基本的な対策として、暗号化、そのための鍵管理、暗号を用いた主体認証、メッセージ認証、改ざん検知等が内部対策としては重要であり、乗っ取りを防ぐという観点では、アクセス制御、必要最小限のアクセス権の設定等が重要。さらに、乗っ取られた場合の対処として、迅速な異常の検知、対処や状況の可視化が必要。IoT機器の持っている機能等に応じて、こうしたセキュリティ対策を選択して適用する必要がある。

・IoTシステムの構築に当たっては、セキュリティゲートウェイによりインターネット側に影響を及ぼさないようにすることが非常に重要であり、ガイドラインの整備等も含めてその考え方を普及させていく必要がある。

・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とする意見に賛同。サイバーセキュリティに関しては状況の変化が早いため、このような方針が適切であると考える。

・脆弱性対策ができない機器についても仮想的にパッチを適用した状態にする対策などを活用する必要がある。また、ネットワーク側に問題を引き起こすような機器はつないでも通信ができないように強制設定できるような仕組みが必要。

・セキュリティ対策を技術基準適合認定等で担保する場合、どこまでの対策を行うべきか明確にすべき。

・今まで、技術基準適合認定等は一度取得すれば永久に有効だったが、非常に大きな脆弱性が見つかったときに、認定の取り消しといった考え方があり得るのか。また、ネットワーク機能がソフトウェアで実現する場合、そのソフトウェアを入れ替えた際には、認定のとり直しが必要ではないか、その場合、認証番号の表示のあり方はどうあるべきか。

・現状のサイバー攻撃に関しては、既知の脆弱性への対応や適切なID・パスワードの設定といった対策により大抵の攻撃は防げるのではないか。

・現在のサイバー攻撃に対しては、比較的簡単な方法で大方の脅威に対処することが可能。

・セキュリティ対策について、技術的にはアップデートが必ず必要であることは間違いない。

これまでの主な議論（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（続き）＞

・インターネットに直接接続する場合もあれば、セキュアなルータを介して接続するような場合など、製品の特性あるいはネットワークへの接続状態によって、脅威やリスクが異なるという点を踏まえて検討を行う必要がある。

・端末設備のセキュリティ対策については、個々の端末の可用性を損なわずに電気通信事業者のネットワークや他の利用者に迷惑を与えるケースが増加すると考えられ、そうした観点も踏まえた検討が重要。

・CC認証でも有効期限の導入について議論になっているところ、認定の有効期限について検討したほうが良いのではないか。

・白物家電やセンサーデバイスなどは10年以上使用する場合もあり得るという点を考慮すべき。

・将来的には機器ではなく、システムを対象としてセキュリティを担保する仕組みを検討する必要があるのではないか。

・IPAではネットワークカメラについて、現場で調達し得る範囲の最小限の要件をチェックリスト化しており、こうしたチェックリストの第三者評価のような仕組みがあれば効果的と考えられる。

これまでの主な議論（端末設備のセキュリティ対策関係）

＜セキュリティ対策に関する関係者間の情報共有・連携について＞

・販売時に脆弱なIoT機器や、サポート期間の切れた後に脆弱性の発見されたIoT機器が接続されたままになってしまうと、インターネットを利用するありとあらゆるものに迷惑がかかる。例えば、サポート期間を明確化できないか。

・ネットワークに接続された機器の脆弱性が悪用された際、通信事業者において異常を検知しても原因が分からないことがある。そのため、通信事業者に情報を共有頂くことはできないか。

・情報共有について、JPCERTやNICTが観測した結果は機器メーカーへ提供している。この情報を、どの時点でどういった形で情報公開をするかはケース・バイ・ケースになっている。

・バグが見つかった際、オンラインアップデート機能が備わっていたため助かったという事例がよくある。一方、オンラインアップデート機能がなく、既に流通した機器の回収が困難なため相当苦労した事例も聞いている。メーカに対し、きちんとセキュリティ対策をとらないと、かえって手間となることを共有することが重要。

・セキュリティ対策の役割分担について、エンドユーザに対策を期待するのは実効的に難しいため、IoT機器、IoTシステム/サービス、及び公衆電気通信サービスの提供者が役割分担して対策を実施するのが現実解であると考える。

・端末側とネットワーク側の対策について、どこで責任を切り分けて役割分担していくかを明確にする必要がある。

・機器の利用者にもリスクを認識させるような手立てが必要ではないか。

・脆弱性が見つかった際、ユーザに通知する仕組みなどを検討してはどうか。

これまでの主な議論（端末設備のセキュリティ対策関係）

＜セキュリティ対策に関する国際動向について＞

・米国においては、初期設定及び自動ソフトウェアの更新機能などの重要性を指摘するとともに、機器の大半は国外に存在するため、国際的に認められた標準に基づくセキュリティの向上が重要とする、「ボットネット等の脅威に対するインターネットの強固性と通信のエコシステムの強化」に関する報告書案を公表し、現在、最終的な報告書を取りまとめているところ。

・欧州においては、ICT機器やサービスに対し、既知の脆弱性を含まないソフトウェアが提供され、安全にソフトウェア更新がおこなわれることを保証する等を目的として、「ICTサイバーセキュリティ認証に関する規則案」が公表され、引き続きEUの議会で検討が行われているところ。

・グローバル対応との整合性を図る際には、日本からも積極的に提案を行っていくべきではないか。

＜国際標準に基づくセキュリティ認証について＞

・CC認証は、世界28カ国で受け入れられている認証制度であり、複合機の例では、他の利用者による不正な操作や通信データの盗聴・改ざん、管理機能への不正なアクセス等を脅威として想定し、識別・認証・権限付与やアクセス制御、ファームウェアに電子署名を付すといった高信頼な通信等のセキュリティ機能を保証。また、セキュリティ機能自体の脆弱性評定も実施。

・CC認証を取得した機器のアップデートにより認証した機能に影響がある場合、再度認証を取得する必要があるが、複合機の例では、毎年新機種が出ており、既存の認証機器をアップデートするより都度認証を取得することが一般的。

＜他法令との関係について＞

・修正不能な脆弱性が発見された場合の製造物責任法との関係はどうなっているか。1年も経たないうちに深刻なバグが見つかった際、黙っていると製造物責任法に反していることになるのではないか。同様に明らかに甚大な影響を及ぼすようなバグが見つかった場合、本来ならリコールをかけ、ファームウェアをアップデートするということが必要になるのではないか。

・IoT機器がマルウェアに感染し、通信事業者の通信サービスに影響を与えた場合、一般的には直ちに一般消費者の生命に危害を与えるとは考えにくいため、消費生活用製品安全法に基づくリコールの対象には該当しない。

・IoT機器は、製造物責任法の対象となり得るため、製造物の欠陥により他人の生命、身体、財産権を侵害した場合には損害賠償を請求できる可能性がある。