資料34－2－2

技術検討作業班報告骨子（案）
- IoT機器を含む端末設備のセキュリティ対策について -

平成30年6月7日

IPネットワーク設備委員会
技術検討作業班
事務局

「IoTの普及に対応した電気通信設備に係る技術的条件」に係る検討事項

（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。

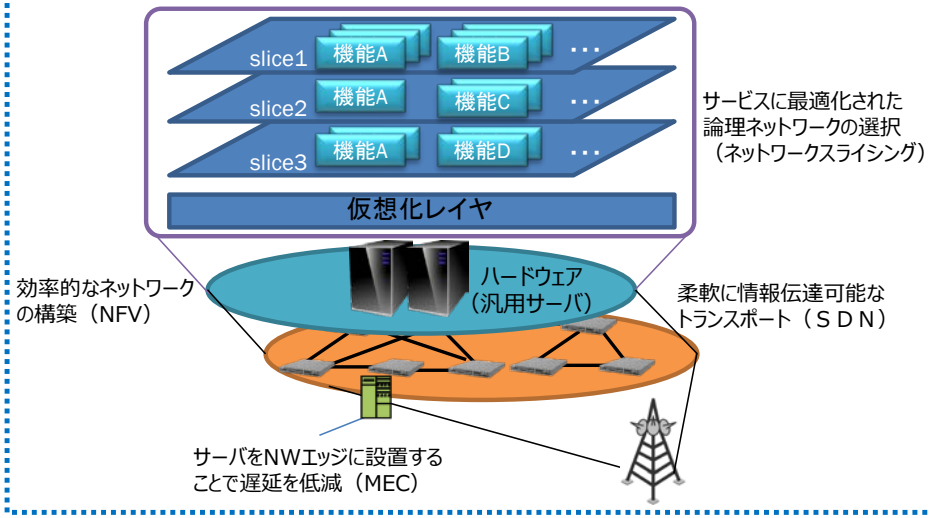
（3） IoT時代における重大事故に関する事故報告等の在り方

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。）。

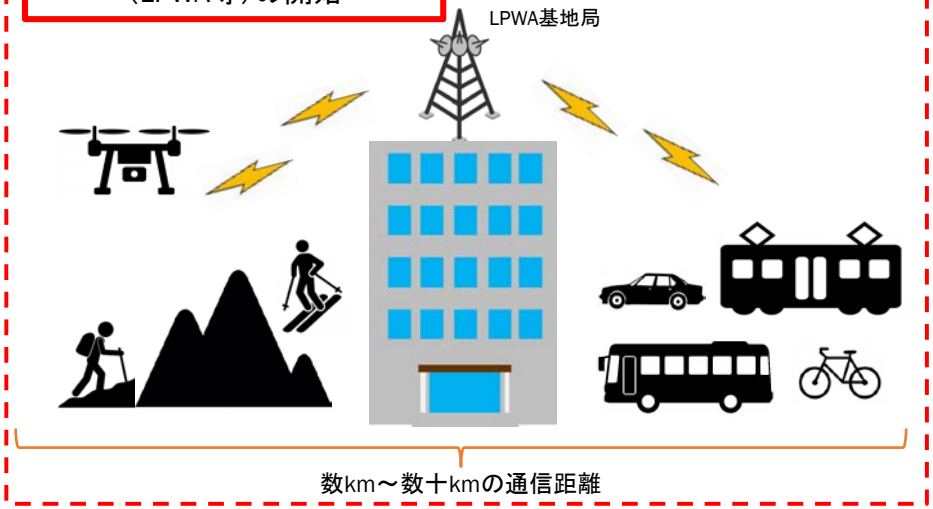
（4） その他

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



IoT機器を含む端末設備のセキュリティ対策に係る検討経過

（1）IPネットワーク設備委員会での検討

第36回（平成30年3月6日）

・「円滑なインターネット利用環境の確保に関する検討会　対応の方向性」を踏まえ、委員会における検討事項の追加を行うとともに、IoT機器を含む端末設備のセキュリティ対策について関係者からヒアリングを行った。

第37回（平成30年3月30日）

・ IoT機器を含む端末設備のセキュリティ対策について関係者からヒアリングを行った。

第38回（平成30年4月27日）

・ IoT機器を含む端末設備のセキュリティ対策について関係者からヒアリングを行うとともに、技術検討作業班において具体的な内容の検討を行うことを決定した。

（2）技術検討作業班での検討

第33回（平成30年5月10日）

・ IoT機器を含む端末設備のセキュリティ対策について検討を行った。

第34回（平成30年6月7日）

・ 技術検討作業班におけるこれまでの検討の取りまとめを行い、委員会への報告書（案）について検討を行った。

IoT機器を含む端末設備のセキュリティ対策に係る検討の目的

■ 近年、Webカメラやルーター等のIoT機器が乗っ取られ、DDoS攻撃等のサイバー攻撃に悪用され、インターネットに障害を及ぼすような事案が増加。

■ このような中、情報通信ネットワークの安全・信頼性を確保するためには、IoT機器を含む端末設備の技術基準にセキュリティ対策を追加することについて検討を行うことが必要。

■ このため、技術検討作業班において、主に端末設備の接続の技術基準に追加すべきセキュリティ対策の内容及び技術基準適合認定等の対象機器の範囲について検討を行ったもの。

検討の目的

・端末設備の接続の技術基準の原則である、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさないといった観点から、大規模DDoS攻撃等のサイバー攻撃を抑止するため、IoT機器を含む端末設備がマルウェアに大量感染する事態を防止すること等を目的とするセキュリティ対策を技術基準に追加することについて検討を行った。

・なお、上記に加え、本年５月に電気通信事業法等が改正され、電気通信事業者による情報共有体制などの新たな取組みが導入されることとなっている。

・また、IoTセキュリティを確保するためには、これらの対策だけではなく、ガイドラインの活用や周知啓発など総合的な対策が必要であり、それらについてはIoT推進コンソーシアム等の場において引き続き検討され、必要な対策が実施されていく必要がある。

技術検討作業班における検討結果（端末設備のセキュリティ対策）について

作業班における検討結果

（１）端末設備の接続の技術基準に追加すべきセキュリティ対策の内容

・インターネットプロトコルを使用する端末設備であって、電気通信回線を介して接続することにより当該設備に備えられた電気通信の送受信に係る機能を操作可能なものについては、大量感染を防ぐための最低限のセキュリティ要件として、アクセス制御機能、アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能及びファームウェアの更新機能、又はそれと同等以上の機能が必要。

【アクセス制御機能】
・当該端末が不正に操作されないことを目的として、当該操作の前にアクセス制御を行うことが必要。

【アクセス制御の際に使用するID/ﾊﾟｽﾜｰﾄﾞの適切な設定を促す等の機能】
・アクセス制御を識別符号によって行う場合は、当該識別符号が他人から容易に推測できないものとして設定されることを目的として、当該端末の利用者に対し当該識別符号について初期値の変更を促す（二以上の識別符号の組み合わせによるものの場合はいずれか一つの識別符号が対象。以下同じ。）、識別符号の初期値について機器毎に別のものを付す、又はそれに準じる措置を行うことが必要。

【ファームウェアの更新機能】
・端末に記憶されている当該電気通信の送受信の機能に係るソフトウェアの更新が可能であることが必要。当該更新は安全かつ自動で行われることが推奨されるが、IoT機器は多種多様であり、更新の手法は機器の種別毎に異なることから、安全かつ自動の更新までは要件とはしない。
・端末への電力供給が停止した場合であっても、当該更新されたソフトウェアや変更されたアクセス制御の設定内容を維持することが必要。

【同等以上の機能】
・CC認証などの国際標準に基づくセキュリティ認証を取得した複合機など、上記の機能と同等以上のセキュリティ機能を有すると認められるものについては、当該セキュリティ要件を満足するものとみなす。

・なお、PCやスマートフォン等、アンチウィルスソフト等のソフトウェアを導入する等、利用者が任意の方法により必要に応じて随時かつ容易に必要な対策を行うことが可能な設備については、当該セキュリティ要件の規定の対象外とする。

技術検討作業班における検討結果（端末設備のセキュリティ対策）について

作業班における検討結果

（２）技術基準適合認定等の対象機器の範囲

・現状、技術基準適合認定等は、基本的に電気通信回線設備に直接接続される端末機器を対象に実施している。

・セキュリティ要件が追加された場合においても、ネットワーク側からサイバー攻撃を受けた際に乗っ取られるリスクが高いのは、電気通信事業者の電気通信回線設備に直接接続される端末機器であることから、技術基準適合認定等の対象は、従来と同様に電気通信回線設備に直接接続される端末機器とする。

・直接接続される機器とは、電気通信回線設備に物理的かつ技術的に直接接続可能な端末機器を指すが、その中でも恒常的に既認定機器を介して接続する機器※については、技術基準適合認定等の対象外とする。

※ 屋外に持ち出して電気通信事業者の回線設備に直接接続して使用することを全く想定していない機器（例：大型白物家電等）

この場合、

－利用者が認定を取得していない機器を誤って直接接続しないようにするため、例えば、取扱説明書等において、①当該機器は既認定機器に接続する必要があることや、②電気通信事業者の電気通信回線設備に直接接続する場合には、電気通信事業者による検査が義務付けられていることを記載すること等をガイドライン等により明示することについて検討する必要がある。

－認定を取得していない機器の乗っ取りを防ぐためには、IoT機器メーカやIoTシステム/サービス提供者等において、IoTセキュリティガイドライン等に基づき、直接接続される既認定機器における対策も含む適切なセキュリティ対策を検討・実施する必要がある。

－今後、端末機器の接続が多様化することが想定されるが、認定が必要な機器の範囲等については、機器メーカ等が判断できるように、ガイドライン等により明示することについて検討する必要がある。

技術検討作業班における検討結果（端末設備のセキュリティ対策）について

作業班における検討結果

（３）その他

〇経過措置

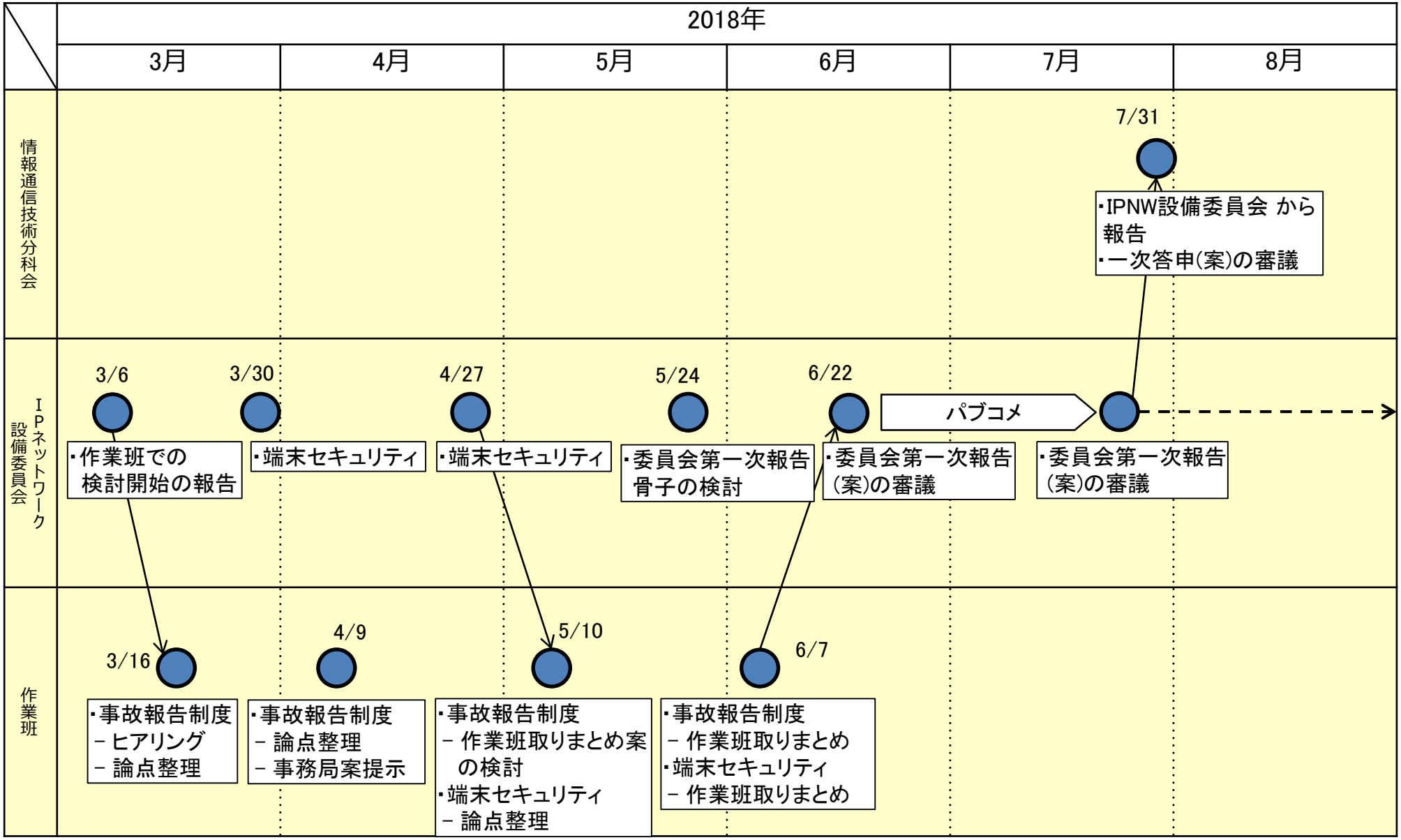
・端末設備の接続の技術基準へのセキュリティ要件の規定の追加が制度化された場合は、一定の期間を設けて施行することとなるが、その期間は1年から2年程度とする。

・従来の制度に基づき、新制度の施行前に取得した技術基準適合認定については、施行後も引き続き有効であり、当該認定に基づく機器も引き続き使用することを可能とする。

〇審査方法

・登録認定機関等によるセキュリティ要件に係る技術基準適合認定の審査方法等については、通信事業者、機器メーカ等が参画可能な場で別途議論を行う必要がある。

今後のスケジュール（案）


2018年
3月
4月
5月
6月
7月
8月
情報通信技術分科会
IPネットワーク設備委員会
作業班
7/31
・IPNW設備委員会 から報告
・一次答申(案)の審議
3/6
・作業班での検討開始の報告
3/30
・端末セキュリティ
4/27
・端末セキュリティ
5/24
・委員会第一次報告骨子の検討
6/22
・委員会第一次報告(案)の審議
パブコメ
・委員会第一次報告(案)の審議
3/16
・事故報告制度
－ヒアリング
－論点整理
4/9
・事故報告制度
－論点整理
－事務局案提示
5/10
・事故報告制度
－作業班取りまとめ案の検討
・端末セキュリティ
－論点整理
6/7
・事故報告制度
－作業班取りまとめ
・端末セキュリティ
－作業班取りまとめ