参考資料 34－2－1

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
技術検討作業班（第 33 回）（端末設備のセキュリティ対策について）
議事要旨（案）

１　日時

平成 30 年 5 月 10 日（木）11 時 00 分～12 時 00 分

２　場所

総務省 11 階　11 階会議室

３　出席者（敬称略）

（１）作業班構成員（端末セキュリティ）

内田　真人（主任）、吉岡　克成（主任代理）、桑田　雅彦、小林　努、阪田　　徹、四ノ宮　大輔、渋谷　香士、高橋　慎一郎、田島　佳武、中野　　学、中村　康洋、西部　喜康、安藤　英治、前田　真弓、福井　晶喜、毛利　政之、松本　勝之、渡部　康雄

（２）事務局（総合通信基盤局　電気通信事業部）

荻原　直彦（電気通信技術システム課長）、鳥居　秀行（電気通信システム課認証分析官）、道方　孝志（電気通信技術システム課課長補佐）、中村　元（電気通信技術システム課企画係長）

４　議事

（３）IoT 機器を含む端末設備のセキュリティ対策の検討

事務局より、資料 33-2-1 に基づき、IoT 機器を含む端末設備のセキュリティ対策の検討について説明があった。主な意見や質疑応答は次のとおり。

○セキュリティ対策について、ファームウェアの更新機能は、利用者が更新をしない場合が多いため、自動更新機能等を具備することが望ましいが、どこまで対策を求めるべきか。
→更新機能を持っていたとしても、誰が責任をもってファームウェアの更新を行うかという課題もある。
→認定の審査にあたっては、更新主体まで確認することは困難と思われる。
→ファームウェア更新に関する認定の審査方法について、更新手段に応じた方法を検討するべき。
→ファームウェアの更新については、主に①ネットワーク経由、②サービスマンによる保守、③リコールによる回収により行われている。

○端末の乗っ取りが行われないような AMP 攻撃による被害も大きいため、こうした攻撃への対策についても検討が必要と思われるが、具体的な基準に落とし込むのは難しいのではないか。
→IoT のセキュリティは様々な取組みで総合的に確保する必要がある。今回の検討では、乗っ取り等を防ぐという観点から端末設備が最低限有すべきセキュリティ機能に絞って議論すべきではないか。

○技術基準適合認定の対象機器の範囲を検討するに当たり、直接接続とはどのレイヤーにおける接続のことであるか明確にすべきではないか。

→現在の端末設備等規則の考え方では、物理的な接続を念頭においている。

→論理的に接続される機器についてはどう考えるべきか。

→例えば、ルーター等における対策や、ネットワーク側での対策ということも考えられるのではないか。

→ルーターや、ネットワーク側で対策することは、技術的にもコスト的にも困難であり、個々の機器で対処していくことが重要と考える。

（3）その他

事務局より、次回会合の日程について、別途連絡するとの説明があった。

以上