参考資料 38－1

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（第 37 回）
議事要旨（案）

１　日時

平成 30 年 3 月 30 日（金）13 時 00 分～15 時 00 分

２　場所

総務省 11 階　共用 1101 会議室

３　出席者（敬称略）

（１）委員会構成員

相田　仁（主査）、会田　容弘、有木　節二、内田　真人、江﨑　浩、大矢　浩、岡野　直樹、片山　泰祥、前田　洋一、松野　敏行、向山　友也、矢入　郁子

（２）プレゼンテーション者

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）

松本　勝之（ソフトバンク株式会社　IT サービス開発本部　セキュリティ事業統括部　セキュリティオペレーションセンター部　サイバーインシデントレスポンス課　課長）

桑田　雅彦（日本電気株式会社　IoT 基盤開発本部　シニアエキスパート）

（３）事務局（総合通信基盤局　電気通信事業部）

古市　裕久（電気通信事業部長）、荻原　直彦（電気通信技術システム課長）、鳥居　秀行（電気通信技術システム課認証分析官）、松井　正幸（安全・信頼性対策室企画官）、道方　孝志（電気通信技術システム課課長補佐）

４　議事

（１）これまでの委員会における主な議論等について

事務局より、資料 37-1 に基づき、これまでの委員会における主な議論等について説明があった。主な質疑応答等は次のとおり。

○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。

○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べきと考える。

（２）利用者が接続する端末設備等の接続の技術基準について

事務局より、資料 37-2 に基づき、利用者が接続する端末設備等の接続の技術基準について説明が

あった。

（３）IoT 機器を含む脆弱な端末設備のセキュリティ対策について

横浜国立大学 吉岡准教授、ソフトバンク及び NEC より、それぞれの説明資料に基づき説明があった。主な質疑応答等は次のとおり。

○資料 37-3 の P.12,13 に管理画面を経由した攻撃が観測された機器として放送受信機とあるが、これはどういったものか。

→有料放送を受信する機器であり、外国製のものが主である。

○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。

→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。メーカーに対し、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。

→JPCERT や NICT が観測した結果は機器メーカーへ提供して情報共有している。この情報を、どの時点でどういった形で公開するかはケース・バイ・ケースである。

○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と考える。

→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。

○資料 37-5 の P.21 に IoT 機器に必要な基本的セキュリティ対策の一つとして、「OS/ファームウェア／アプリ等ソフトウェアの脆弱性対策（更新)」とあるが、そもそも更新ができない機器についてはどのように対策するのか。

→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。

○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と考える。

→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検討が必要。

→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検討が必要。

○IoT 機器へのセキュリティ対策について、どういった対策をすると最も効果的と考えるか。

→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と考える。

→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。

（4）その他

事務局より、次回会合の日程について説明があった。

以上