ICTサイバーセキュリティ政策分科会での議論

資料７－２

- 総務省では、本年２月より、総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性について検討することを目的として、サイバーセキュリティタスクフォースの下で「**ICTサイバーセキュリティ政策分科会**」（主査：後藤厚宏　情報セキュリティ大学院大学　学長）を開催している。
- 同分科会における議論の一環として、**スマートフォンアプリにおけるセキュリティを確保していく上での課題**等について議論がなされ、第５回会合（４月５日開催）では、**「スマートフォンプライバシーイニシアティブ」にセキュリティの観点を盛り込むべき**とされた。

ICTサイバーセキュリティ政策分科会での議論（抜粋）

○主な報告内容等

- スマホアプリにおけるサイバー脅威は、「スマホアプリの脆弱性（セキュリティホール）」と「不正アプリ（マルウェア）」の２つの観点で考える必要があり、アプリ流通経路の責任において一定のセキュリティ確保が可能。アプリ開発者及びアプリストアは、アプリを提供する際のセキュリティ確保において大きな役割を担っている。（第１回　一般社団法人日本スマートフォンセキュリティ協会）
- アプリのセキュリティやプライバシーを確保するためにはアプリ診断というプロセスが必要。ただし、アプリ診断のみでは十分ではなく、アプリのセキュリティやプライバシーの状態を改善するためには、セキュア設計・開発ガイド（アプリのセキュリティ要件やリスク分析、セキュアコーディングの指針、セキュリティテストの方法などをまとめたもの）のサポートが必要。（第５回　OWASP）
- 利用者情報の保護のためには、アプリ開発者のみならず、アプリストア運営者等の関係者も含めて適切な対応を取ることが重要。英国のDSIT（Department for Science, Innovation & Technology）の「Code of practice for app store operators and app developers」も参考に、「スマートフォンプライバシーイニシアティブ」にセキュリティの観点も盛り込むことが望ましい。（第５回　KDDI株式会社※）

（※）第５回分科会においては、KDDI株式会社より、「スマートフォンプライバシーアウトルックＸ」についても発表があった。