# スマートデバイスにおける利用者情報の活用とセキュリティ対策の両立
## －NFC／Felica・カメラ・GPS 機能の利用とセキュリティ対策について－
## アブストラクト

1. 研究の背景・問題意識

昨今スマートデバイスの普及が著しく、企業において業務への活用が進んでいるが、活用事例を調べていくと、用途が情報閲覧に偏っており、想定とは異なる事実が分かってきた。具体的には、スマートデバイスの利用者情報（電話・アドレス帳データ、通信履歴・位置情報等、個人を識別するデータ）やＧＰＳ・カメラといったスマートデバイス特有機能については、業務への活用が進んでいない状況であった。当分科会では、その活用状況から、各企業とも利用者情報や特有機能の利用について、本格的な検討ができず、セキュリティ面の不安を抱えた状態と想定した。

2. 研究アプローチ／研究の進め方

ユーザ企業が直面すると思われるセキュリティ面の不安・問題要素についてメンバで議論した。

(1)「リスクを定量評価することが難しい」
(2)「リスク全体像の把握が難しい」
(3)「リスク検討時の負担が大きい」

以上 3 点が挙げられ、これらを利用者情報・特有機能の活用とセキュリティ対策の両立において、解決すべき課題とした。具体策として、ユーザ企業の担当者が簡易な操作で、リスクを大枠で把握し、定量評価できることをコンセプトとした“リスク把握支援ツール”を作成することとした。

研究はこのツール開発を中心に「特有機能等の基本調査」、「ツールのプロトタイプ作成」、「所属企業へのアンケート、ツール改善」、「検証」の順で行った。

3. 研究成果と想定効果

基本調査の後、ツール仕様についてメンバで議論した。その結果、”ユーザ企業の担当者（初級者）の利用”、”上流工程におけるセキュリティ面の不安を解消すること”を前提条件として定義した。それらを前提として、「①リスク発見シート」、「②悪用／脆弱性事例集」、「③セキュリティ関連規格・ガイドライン一覧」、「④スマートデバイス特有機能の特性」を作成することとした。

（1）①リスク発見シートについて

導入を検討している利用シーンおよび利用機能のリスクを簡易に定量評価するためのシートである。利用シーンの選択のみという少ない入力情報から利用機能・リスク・対策に関する情報を提供する。特徴は、以下の３点である。

1）取り扱う表現・文言の簡易化、操作の容易性など、ユーザの IT スキルに依存しないよう「ユーザビリティ」に配慮していること
2）情報の正当性を確保するため、官公庁・セキュリティ関連団体が発行するドキュメントの定義（リスク計算式、各事象の発生可能性、業種・利用機能）を活用していること
3）利用シーンは、分科会メンバ全員で企業導入事例を収集、146 社分の事例を利用シーンの選択肢として活用していること

リスクの定量化方法は、ISMS、JSSEC、JNSA のドキュメントを活用し「資産価値・発生可能性・リスク値」の仕様を決定した。ツールのプロトタイプを作成し、所属企業のユーザによる試験利用後、アンケートを実施（１０社２３名）。以下の改善点を導出し、改善版を作成した。

・結果表記－情報量多く・大枠把握が難しい＞　出力情報の集約・マトリクスによる視覚表現
・リスク値－根拠不明確　＞　計算値・計算式を表示
・網羅性　－全体が網羅されているか不明　＞　JSSEC ガイドラインの機能体系に表記を統一

（2）②悪用／脆弱性事例集について

スマートデバイスの仕組みを悪用した事件や研究者等によって認識された脆弱性を一覧にした。特徴は、以下の２点である。

１）攻撃に高度な技術が必要な脆弱性を含めたこと
２）報道等がされている悪用事例を改めて確認できること

これにより、中長期的な観点から対策要否の判断を支援できると想定している。

（3）③セキュリティ関連規格・ガイドライン一覧について

ユーザが関連ドキュメントを探す負担の削減を目的として作成したガイド資料である。JSSEC、MCPC、総務省等、セキュリティ関連で頻出するドキュメント３７種の概要を把握しやすいよう、３カテゴリ（a.種類：ガイド、報告書等、b.想定読者：c.記載分野）で分類、マトリクス化した。また、別表で個人情報保護法等、セキュリティ関連の１０法令を概要・抵触行為等の要素で整理した。

（4）④スマートデバイス特有機能の特性

ＰＣとの機能の差異から、NFC/Felica・カメラ・GPS の特性を整理したものである。特性を理解することで、各機能に内在するリスクへの対策要否、対策内容を適切に判断できると想定している。

4.　検証

当分科会で掲げた課題に対し、作成したツール群の有効性について、アンケート（１０社２３名）、およびヒアリング（７社１０名）結果を参考に、課題に対する解決状況を検証した。

課題 1「リスクを定量評価することが難しい」
【解決の試み】リスクの定量化
【出来たこと】リスク値算出の考え方を整理、対応の優先順位が分かるよう数値化
【未解決事項】リスク値に要求される絶対的評価に応えられていない

課題 2「リスク全体像の把握が難しい」
【解決の試み】ユーザの選択肢から想定リスクを大枠レベルで導出する
【出来たこと】利用シーンの選択のみで、セキュリティ事象等を導出する方式の開発
【未解決事項】利用シーン・機能・セキュリティ事象に関する情報が実務レベルに未到達

課題 3「リスク検討時の負担が大きい」
【解決の試み】簡易な操作でリスクを大枠で把握できるツール作成
【出来たこと】利用シーンの選択のみで、セキュリティ事象等を導出するツールの開発
【未解決事項】スキルが異なるユーザに対する出力結果の考慮（簡易性⇔情報量、専門性）

また、当成果物についてベンダのセキュリティ関連部門に所属する方に意見を伺った。当分科会で検討した課題、成果物の狙いやリスク関連の定量化の考え方等について、強い賛同を得ることができた。

5.　考察

”上流工程におけるセキュリティ面の不安を解消する”という目的に対し、作成した各成果物は、「リスクの定量化」、「リスク全体像の把握」、「リスク検討時の負担削減」のそれぞれにおいて、アンケートで約８割の共感を得ており、取り組みの方向性は正しかったと考えている。ただし、算出したリスク値の納得度が低いなど、一部は実務で活用できるレベルまで引き上げることができなかった。今後、ますますスマートデバイスの多機能化、利用シーンの多様化が進み、それに伴いリスク評価に対する重要度は増していくと想定される。セキュリティ関連団体・ベンダ企業には、是非その技術力・見識・経験をもって、ユーザ側上流工程におけるセキュリティの要求定義（RFI/RFP）の手順標準化と、それら手順を広くユーザ企業に展開する手段の構築・模索を期待する。ユーザ企業には、企業内で不足する情報を積極的に外部発信し、セキュリティ関連団体・ベンダ企業と連携し、セキュリティの要求定義における標準化の推進を期待したい。なお、当分科会の成果が標準化に向けての第一歩になれば幸いである。