第6章

Androidに存在するセキュリティ問題と対応策

濱口 遵一郎

セキュリティの問題は，ほかのOSと同様，Androidにも存在する．AndroidはLinuxベースOSであることからユーザ単位での権限設定やプロセス単位で隔離された保護機能は存在するが，それでも現在の攻撃レベルからすると不十分だ．そこで各種セキュリティ・ソフトウェアによるデータの保護が必要になる．

ここでは米国Mocana社のMocana DSF for Androidを例に，Androidに存在するセキュリティ問題とその対応策について見ていく．（編集部）

Android携帯電話の急激な普及にも関わらず，企業で採用が進んでいない理由の一つとして，Androidには企業向けセキュリティ・ツールが欠けている点があります．同様に，米国Apple社のiPhoneも強固なセキュリティ機能を装備していないため，エンタープライズ市場においてカナダRIM社のBlackberryほど採用されていません．

米国Mocana（以下モカナ）社のMocana DSF for Androidは，開発者がエンタープライズ・グレードのセキュリティをAndroidデバイスとアプリケーションに実装できるソフトウェア・パッケージです．モジュラ設計されており，必要な機能コンポーネントだけを必要なときのみ使用し，簡単に機能追加や拡張ができます．実装に当たり，暗号技術の専門家である必要はありません．

1．スマートフォンのセキュリティについて

どこでもインターネットにつながる便利さと大容量ストレージにより，ユーザはスマートフォンに重要な企業・個人情報を入れて持ち歩くようになりました．個人とビジネス・デバイスの境目が次第になくなりつつあります．

ユーザが意識することはないかもしれませんが，重要なビジネス・データや個人情報を保持しているため，時としてスマートフォンは知的財産の一部と考えられることもあります．これらの情報が所有者の承認を得ずに公開された場合，漏洩した企業への責任は非常に重くのしかかってきます．

一方，スマートフォンのセキュリティは，ユーザに快適に使ってもらえるよう高速かつ高スケーラブルでなくてはなりません．さらに，バッテリ消費を抑えるため，モバイル・デバイスとサービスのセキュリティはCPUを効率良く使わなければなりません．爆発的なモバイル・ワイヤレス市場の成長により，業界標準は急速な進化を続けています．つまり，現時点のセキュリティ要件と急速に進化する将来のセキュリティ要件に対応できる，拡張可能なセキュリティ・フレームワークがスマートフォン開発者にとって必要になるのです．

● 狙われやすい携帯端末

ハッカーやマルウェアを書くプログラマにとって，スマートフォンは攻撃しやすいターゲットです．彼らのターゲットは企業ネットワークに接続するパソコン以外のデバイスに比重が移りつつあります．多くのユーザがネットワークを使うアプリケーション，メールやWebブラウザ，IM（インスタント・メッセンジャ）などを使うと気軽にディジタル・データをダウンロードできます．そのため，Android端末のようなモバイル・デバイスは，パソコンと同じようにネットワークの脆弱性（せいじゃくせい）を晒（さら）す危険を常に伴っています．

2．Androidに存在するセキュリティ問題

● Androidはユーザ権限ベースのセキュリティ

米国Google社はAndroidのセキュリティ・モデルについて，「大半のアプリケーションとシステムのセキュリティはアプリケーションのユーザ・グループIDなどのLinux

KEYWORD——セキュリティ，Mocana DSF for Android，マルウェア