Android™端末のアプリ管理
～ホワイトリスト方式による端末保護～

竹森敬祐† 川端秀明† 磯原隆将† 窪田歩† 池野潤一††
†KDDI 研究所 ††KDDI

あらまし Android™端末の特徴は、誰もが自由にアプリの開発・公開を行え、ユーザは Market プレイスからアプリをダウンロード･インストールして端末の高機能化を図れる点にある。しかし、Market プレイスにマルウェアが掲載されることもあり、誤って感染してしまう恐れがある。Android™端末のインシデントの殆どは、このアプリのインストールによって生じる。

そこで本展示では、安全性の求められる法人向け端末の保護策として、安全性を確認したアプリだけを予めホワイトリスト化しておき、業務用端末にアプリがインストールされるタイミングで、これと一致しないアプリを駆除するフレームワークをデモする。我々は 1000 台規模の実証実験を行い、業務で不必要なアプリの侵入を阻止できること、端末状態を管理できること確認し、Android™端末の法人利用の目処を得た。

デモ 図 1 に、デモシステムの構成を示す。

① 管理者は、業務向けアプリを Market プレイスから管理用端末にインストールする。
② このアプリを起動･操作することで､安全性を評価するための挙動ログを収集する。
③ 収集された挙動ログやアプリ本体を、安全性を評価するセンタ局へ送付する。
④ センタ局では、アプリ本体から得られるパーミッションに対する静的解析と、挙動ログに対する動的解析を行い、それぞれ潜在脅威と顕在脅威を評価する[1][2]。そして、脅威の低いアプリを認定することで、ホワイトリストを作成する。
⑤ 業務用端末は、一定周期でホワイトリストをセンタ局から取得する。
⑥ 業務用端末で、アプリのインストールを検知すると、ホワイトリストと比較することで、認定の場合にはそのまま、未認定の場合にはアンインストールを実行する。
⑦ 端末所有者によるインストール履歴や端末に組み込まれているアプリ一覧をセンタ局に送付することで、管理者は配布した業務用端末の状態を把握できる。

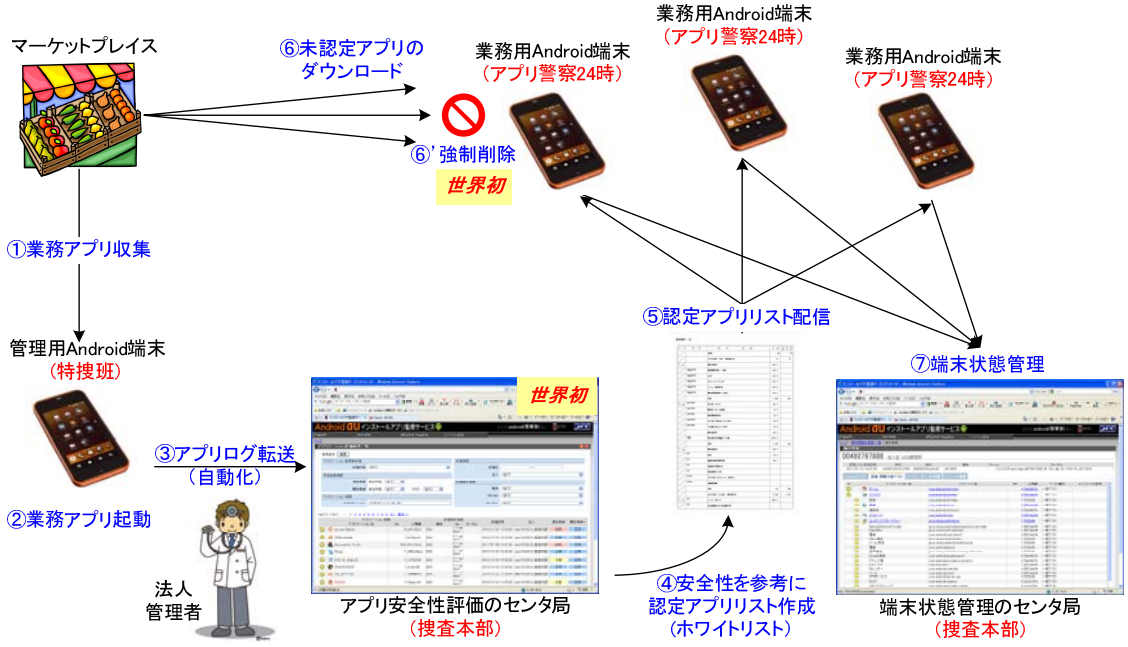

図 1 Android™端末アプリ管理フレームワーク ～アプリ警察 24 時～

[1] 磯原隆将, 竹森敬祐, 窪田歩, 高野智秋,“Android 向けアプリケーションの挙動に注目したマルウェア検知”, IEICE, SCIS, 3B3-2, 2011 年 1 月.

[2] 竹森敬祐, 磯原隆将, 窪田歩, 高野智秋,“Android 携帯電話上での情報漏洩検知”, IEICE, SCIS, 3B3-3, 2011 年 1 月.