Virtual Smartphone over IP技術

NTT情報流通プラットフォーム研究所では，クラウドコンピューティングと仮想化技術の活用により，スマートフォンを用いた高度なセキュリティソリューションや新たな利用形態を実現する技術の研究開発を進めています．本稿では，本提案技術の概要に加え，さまざまな利用シーンについて紹介します．

伊藤 光恭（いとう みつたか）／Eric Y. Chen（エリック チェン）／楠本 哲也（くすもと てつや）
NTT情報流通プラットフォーム研究所

本提案技術の背景

近年，スマートフォンが急速に普及し，ノートPCの代わりになりつつあります．Androidをはじめ，プラットフォームのオープン化により開発環境は自由度が高くなっており，さまざまなキラーアプリケーションが提供されています．しかしながら，PCと同様に利用者の安心・安全は自己責任となるため，今後マルウェアや情報漏洩などの脅威が懸念されています．

Virtual Smartphone over IPの概要

Virtual Smartphone over IPは，クラウドと仮想化技術を用いて，スマートフォンの実行環境を仮想的に拡張するシステムです（図1(a)）．ユーザはクラウド（データセンタ）上でスマートフォンの仮想イメージを目的別に作成し，自分専用の実行環境として運用できます．この環境上でモバイルアプリケーションを実行することで，スマートフォン端末本体のローカルデータと仮想スマートフォン環境に収容されたリモートデータを効果的に隔離でき，高度なセキュリティソリューションが実現できます．さらに，演算処理はクラウド上の仮想環境に移すことにより，スマートフォン端末本体の計算力，メモリ，電力供給などの制限から解放され，スマートフォンの新たな利用形態

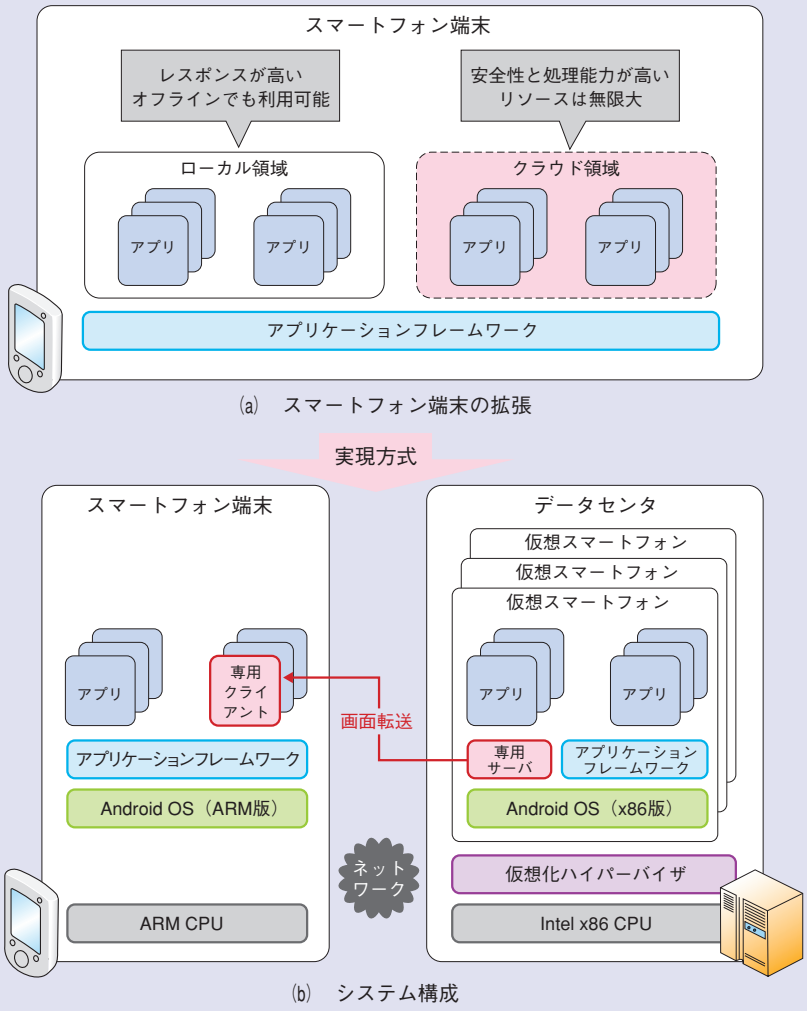


図1　Virtual Smartphone over IPの構成

が実現できます．

本システムは専用サーバプログラム，専用クライアントプログラム，通信プロトコルから構成されます（図1(b)）．サーバプログラムは各仮想スマートフォンにインストールされ，クライアントプログラムはスマートフォン端末にインストールされます．ユーザはクライアントプログラムを通して，仮想スマートフォン上のモバイルアプリケーションをリモートで操作することができます．VNC（Virtual Network Computing）ベースのプロトコルを利用することで，スマートフォン端末から仮想スマートフォンにさまざまなイベントが通知され，その結果画面だけがスマートフォン端末上で更新されます．

今回，x86プラットフォームで動作する仮想スマートフォン端末を，ARM（Advanced RISC Machines）プラットフォームのAndroidデバイスからリモート制御することで，このコンセプトの実現に成功しました．Android OSを選んだ理由は，オープンソースとしてx86とARMプラットフォームの両方が利用可能である点，およびAndroidの拡張性の利点があります．また，このシステムはハイブリッドなプラットフォームにも拡張可能です．例えば，iモードやWindows Mobileの利用ユーザが仮想スマートフォンにアクセスし，Androidアプリケーションをユーザ端末で利用できるようになります．

利用イメージ

本システムの利用イメージを述べます（**図2**）．前提として，本システムではスマートフォン端末やPC端末にあるWebブラウザから事前にユーザ登録を行うものとします．登録ユーザは本システムのサービスサイトから専用クライアントプログラムをダウンロードし，ユーザ自身のスマートフォン端末にインストールします．次に，この専用クライアントプログラムにより，あらかじめ用意された仮想スマートフォンテンプレート（CPU性能，メモリ，ストレージ容量，利用機能などが事前に設定されたもの）の中からクラウド上で新しいイメージを生成し，スマートフォン端末からクラウドコンピューティング環境でモバイルアプリケーションを実行します．

ここではユーザのニーズに合わせたいくつかの利用シーンを紹介します．

■アプリケーションの評価

スマートフォン端末の内部リソースから分離され，アクセスを厳重に制限された仮想スマートフォンを用いることで，提供元不明のモバイルアプリケーションを安全に実行，およびテストすることができます．この利用方法は「サンドボックス」と呼ばれ，ユーザ自身のスマートフォン端末でモバイルアプリケーションを実行せず，仮想環境から利用可能なリソースにのみアクセスするといった利用方法です．特にAndroidマーケット以外で提供される，信頼性の低いモバイルアプリケーションによる被害を最小限に抑えるため，ネットワークとデータへのアクセスを制限することで，セキュリティの向上が可能です．

■情報漏洩対策

近年では，シンクライアント技術は情報漏洩対策として注目されています．本システムでも，ユーザのスマートフォ

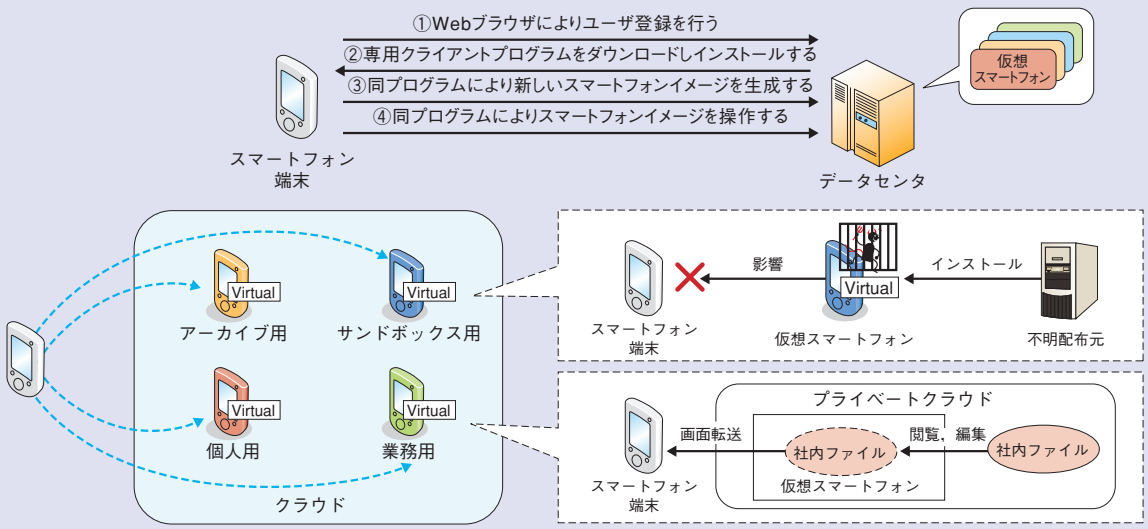


図2　利用イメージ

ン端末には仮想スマートフォンからの画面描写情報だけが送られるため，データファイルは安全なデータセンタから流出することはありません．これにより端末本体の盗難や紛失に対する物理的セキュリティリスクを格段に抑えられます．操作面でも，データセンタ側の仮想環境をスマートフォン端末の小型画面に最適化しているため，スマートフォン端末で実行するローカルアプリと同じ感覚で利用できます．

また，企業内の情報セキュリティの観点においても，本システムを用いることで社員はデータを端末本体にコピーするための承認や権限を必要とすることなく，データを参照することが可能となります．さらに，企業にとっても機密データを集中管理することができ，情報管理の効率化を図ることが可能となります．

■モバイルアプリの高速化

Androidがx86，ARMプラットフォームの両方で同じJavaベースのAndroidアプリケーションフレームワークを利用しているため，x86，ARMプラットフォーム間ではモバイルアプリケーションのポータビリティがあります．通常のAndroidアプリケーションはARMプラットフォームでの利用を想定していますが，x86の仮想スマートフォンからデータセンタ側のリソースを利用することにより，同じモバイルアプリケーションのパフォーマンスを劇的に向上することができます（**図3**）．これらの結果から，計算量が大きいモバイルアプリケーションは，仮想スマートフォン上で動作させ，演算結果を表示する画面情報だけを端末本体に送信するという形態が，今回のシステムに適していると考えられます．

また，計算処理の大部分を，仮想スマートフォンで実行し，スマートフォン端末は結果の画面を表示することで，端末本体のバッテリ消費を節約することにも役立つと考えられます．

■その他

その他の利用シーンとして，例えば，ユーザはあまり利用しないアプリケーションを仮想スマートフォンの中に移動させることもできます．また，仮想スマートフォンはクラウドコンピューティング環境に存在し，常にオンラインであるため，開発者はスマートフォン端末で実現が難しかったサーバライクなモバイルアプリケーションを開発することもできます．

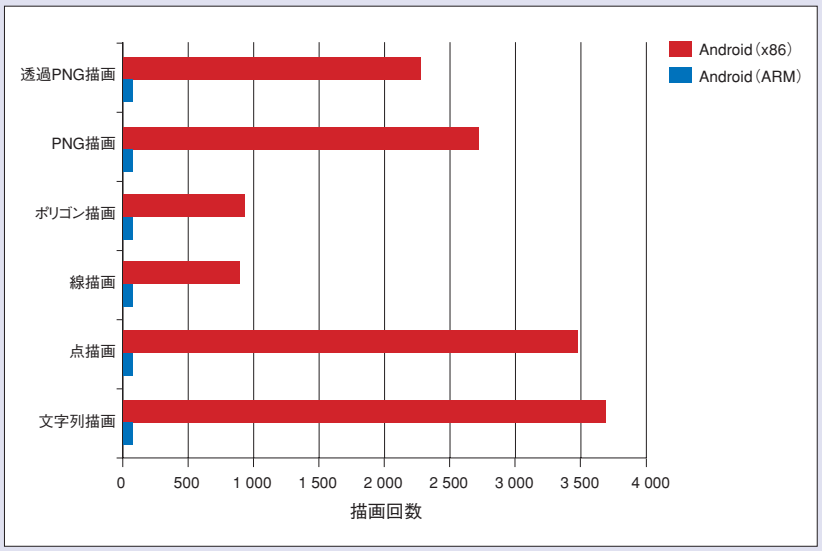
Androidマーケットではユーザはアプリケーションを評価して，24時間以内であれば購入したアプリケーションを返却できます．しかしながら，アンインストールした後も不要なファイル（apkファイル等）は残ってしまいます．ユーザは仮想スマートフォンを利用することで，不要なファイルが自分のスマートフォン端末に残るのを防ぐことができます．

本システムの特徴

仮想スマートフォン上で動作するモバイルアプリケーションをスマートフォン端末でシームレスに実行できることが重要だと考えます．これを実現するために，本システムで採用した主な技術の特徴について概要を紹介します．

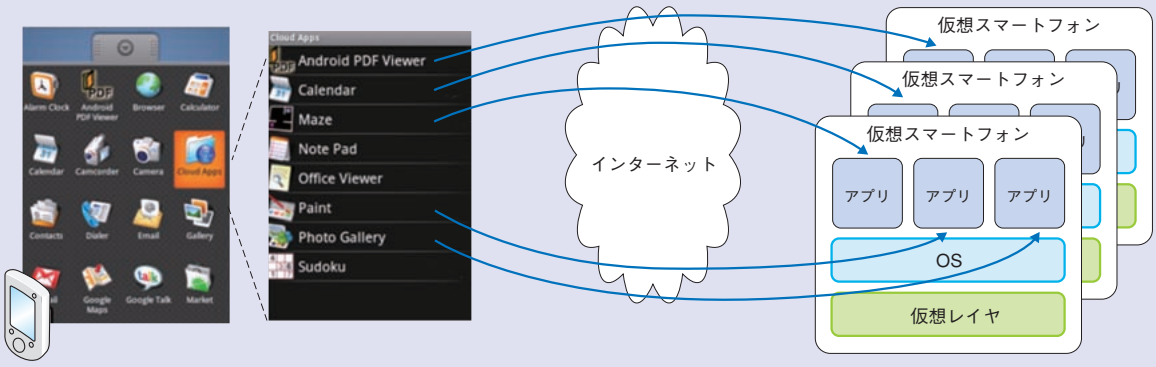
■拡張入力デバイス

多くのスマートフォンはGPS，磁気センサ，加速度センサ，温度センサといったさまざまな入力デバイスを備えています．従来のVNCを利用したシンクライアントソリューションでは，入力デバイスとしてキーボードとマウスしかサポートしていませんが，本システムではスマートフォン端末のストレージや，新しい入力デバイスをサポートしています．これらのスマートフォン端末の入力デバイスはあたかも仮想スマートフォン上に実際にあるように見えるため，モバイルアプリケーションはクラウ

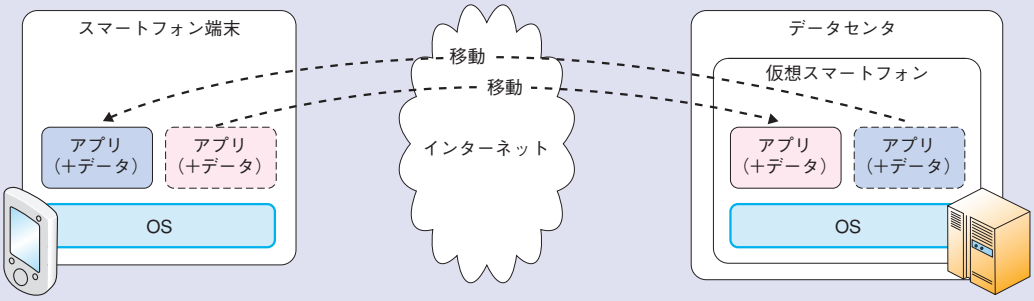


※ラスターワークス社の「SmartPhoneBench」による測定結果
※値が大きいほど処理性能が高い
※Android（x86）はDELL Precision M6300とESXi上で実行した
※Android（ARM）はAndroid Dev Phone 2で実行した

図3　Android（x86版）とAndroid（ARM版）の性能比較



(a)　ショートカット機能



(b)　アプリケーション移動

図 4　本システムの特徴

ド上でもローカル環境と同様に実行できます．

■GUIの統合

本システムは，スマートフォン端末と仮想スマートフォン間でのコピー&ペースト等，ユーザがスマートフォン端末上のアプリケーションを利用しているかのように，クラウドコンピューティング環境のアプリケーションを実行することが可能となります．また，ユーザはスマートフォン端末上のショートカットを利用することで，最小限の手順で仮想スマートフォン上のアプリケーションを実行することができます（**図 4**）．さらに各ショートカットは異なる仮想スマートフォンに結び付けることも可能で，これにより，ユーザは1つのメニューリストの中から，複数の仮想スマートフォンに存在するアプリケーションに即座にリモートアクセスできるようになります．

■アプリケーション移動

本システムは，コピープロテクトがかかっていないモバイルアプリケーションとそれに関連するデータをスマートフォン端末とクラウド上の仮想スマートフォン間で移動できるため，従来のシンクライアントソリューションよりも自由度が高く，リモート環境とローカル環境の壁をなくしてさらに統合できます．

今後の取り組み

NTT情報流通プラットフォーム研究所では，開発者向けAndroid端末（Dev Phone）を用いてプロトタイプを実装してきました．本稿に記述したいくつかの特徴を商用向けのAndroid端末として実現するには，ファームウェアのカスタマイズが必要です．今後はこれらの特徴を組み込むために，通信キャリアと端末メーカが密に協力することが必要と考えています．

(左から) Eric Y. Chen/ 伊藤　光恭/ 楠本　哲也

NTT情報流通プラットフォーム研究所では，今後もモバイルクラウド技術の研究開発を通じて，安心・安全なネットワークの実現を目指していきます．

◆問い合わせ先
NTT情報流通プラットフォーム研究所
セキュアコミュニケーション基盤プロジェクト
TEL　0422-59-3347
FAX　0422-59-5660
E-mail　eric.chen@lab.ntt.co.jp