

# OpenFlowを活用した業務用スマートデバイスのセキュアな通信の実現

才田 好則・飯星 貴裕・森田 弦  
渡邊 義和・狩野 秀一

## 要旨

企業において業務へのスマートデバイスの活用が進んでいるなか、情報漏えいへの対策が急務となっています。クラウドシステム研究所では、スマートデバイスにOpenFlow技術を組み込むことによる、ネットワークとスマートデバイスが連携した柔軟なネットワーク制御機能の研究開発に取り組んでいます。本稿ではこの技術を活用した、スマートデバイスの業務通信の安全化について紹介します。

## キーワード

●OpenFlow ●Software-Defined Networking ●Bring Your Own Device ●Virtual Private Network

## 1. まえがき

スマートフォンやタブレット端末などのスマートデバイスを活用することにより、社内外の多様な場所及び、3G、LTE（Long Term Evolution）、Wi-Fiなどの複数の無線ネットワークを通して、各種業務サービスの活用ができるようになっています。一方でスマートデバイスの業務利用時の課題として、セキュリティ確保が挙げられます。

本稿では、スマートデバイスにおけるセキュリティ課題のうち、通信に関するセキュリティを確保するための技術として、OpenFlowを活用した業務通信の安全化技術を紹介します。

## 2. スマートデバイスのセキュリティ面での課題

従来の携帯電話に対して、スマートデバイスでは表1に示すような機能の拡張が行われており、これによって各種業務サービスを効率的に利用できるようになってきました。

表2は、これらの拡張機能に起因するセキュリティリスクを分類したものであり、表中に挙げた問題への対策が求められます。

本稿ではこれらのセキュリティリスクのうち、特に通信に関わるリスクに対処するための、OpenFlowを活用した技術を紹介します。ストレージに関わるリスクに関しては、他のMDM（Mobile Device Management）ソリューションを用いて保護することで、これらの組み合わせによりスマートデバイスの業務活用をより安全に行うことが可能となります。

表1 スマートデバイスにおける拡張機能

機能	メリット
ストアからのアプリ追加	企業による業務アプリの導入を実現
Wi-Fi	社内外の高速なWi-Fiアクセスポイントを利用可能
テザリング	PCを接続し手軽にインターネットへ接続可能
VPN(Virtual Private Network)	社内ネットワーク環境を社外から利用可能
大画面タッチパネル	よりスマートな操作が可能

表2 スマートデバイスの拡張機能に起因するリスク

機能	アプリ追加	セキュリティリスク			
		不正アクセス	なりすまし	業務効率低下	運用コスト増
Wi-Fi	マルウェア感染による情報漏えい	-	-	業務外アプリの業務時間中の利用	-
	脆弱なアクセスポイントの利用による通信の盗聴	-	-	-	-
VPN	-	不許可端末が許可端末を踏み台にすることによるなりすましアクセス	-	通信量の増大	-
	マルウェアによる社内システムの攻撃	-	-	-	-

## 3. OpenFlowのスマートデバイス通信制御への適用

本章では、OpenFlow技術の概要と、スマートデバイス通信制御への適用方式に関して説明します。

クラウドシステム研究所ではOpenFlowを利用した、ネットワークからのリアルタイムなスマートデバイス通信制御技術の研究を行っています<sup>1)</sup>。これは、ネットワーク全体の状況やサービスの要求に応じて、より柔軟なスマートデバイス通信

## 先端技術研究

### OpenFlowを活用した業務用スマート デバイスのセキュアな通信の実現

制御を行えるようにすることを目的としたものです。

#### 3.1 OpenFlowの概要

OpenFlowは以下の特徴を持ったネットワーク制御技術であり、ソフトウェアによる柔軟なネットワーク管理、運用制御、容易な機能追加を可能にします。

##### (1) 集中制御型の制御

OpenFlowのネットワークは図1に示すとおり、ネットワークの経路を制御する「OpenFlow Controller（以下、OFC）」と、OFCから与えられたパケット処理規則に従って実際にパケットを処理する「OpenFlow Switch（以下、OFS）」で構成されており、ネットワークに配置されたOFCが複数のOFSを制御する“集中制御型ネットワーク”となっています。

##### (2) 細かな粒度＝フロー単位での制御

OpenFlowでは、データリンク層からトランスポート層までのプロトコル情報を組み合わせた「フロー」と呼ぶ単位で通信を管理しています。そのため、従来のOSI階層モデルに従った層ごとの情報に基づく通信制御に比べ、より細かな粒度での通信制御が可能です。

##### (3) ソフトウェアによる柔軟な制御

従来のネットワークでは専用の機器で行っていたネットワーク制御を、OpenFlowではOFCで保持するパケット

処理規則の変更で対応できます。これにより、(2)に挙げたフロー単位の制御と合わせ、ソフトウェアによる柔軟なネットワーク管理、運用制御、新規機能の追加を実現できます。

#### 3.2 OpenFlowのスマートデバイス通信制御への適用

クラウドシステム研究所では、このOpenFlowの技術をスマートデバイスに適用することで、OFCから、OFSソフトウェアを搭載したスマートデバイスの通信を制御する方式の研究試作を進めています。

その際、図2のa)とb)に示す2つの適用形態を想定しています。

図2のa)は、ネットワークにOFCを配置した場合、図2のb)はスマートデバイスにOFCを配置した場合で、いずれかのOFCによって、スマートデバイスのOFSを制御します。いずれの構成においても、スマートデバイスにOFSを搭載することで、制御単位であるフローの情報からスマートデバイス上で通信を行っているアプリケーションを特定することが可能となり、この情報をを利用して、アプリケーション単位での3G、Wi-Fiといった無線通信経路の選択、または通信の拒絶などの制御を行うことが可能となります。

一方でOFCの配置位置の違いにより、それぞれ次のような

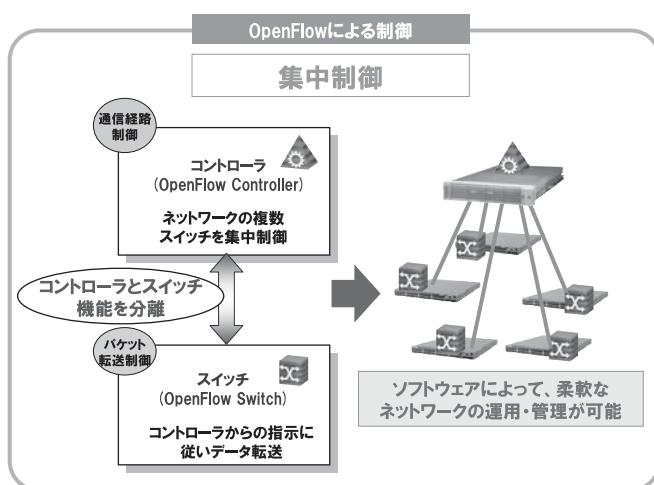


図1 OpenFlowのコンセプト

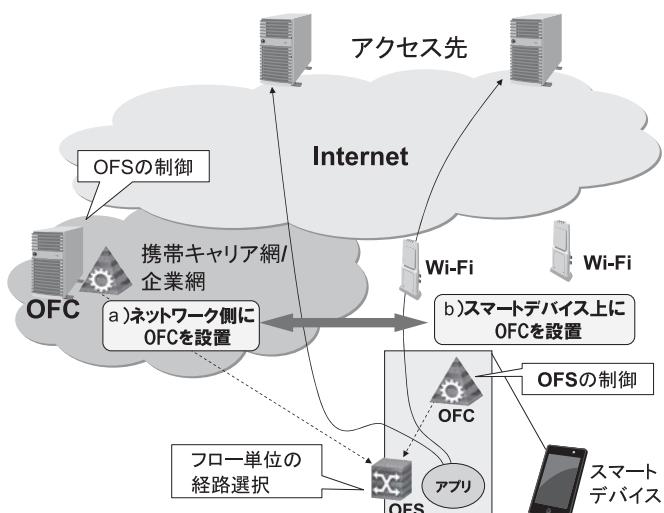


図2 スマートデバイス通信制御の構成

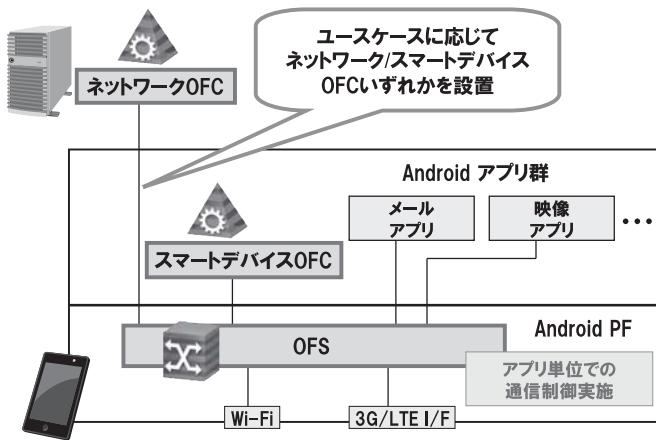


図3 Androidスマートフォン上の試作構成

特徴があります。

#### ・ ネットワークにOFCを配置する場合

携帯キャリア網や企業網にOFCを配置することで、配下の全スマートデバイスの通信を集中制御可能となります。

#### ・ スマートデバイスにOFCを配置する場合

スマートデバイス単体だけで動作可能となり導入が容易になりますが、スマートデバイス全体の集中制御を行う際には、別途MDMシステムなどとの連携が必要になります。

クラウドシステム研究所では現在、図3に示すような構成で、Androidスマートフォン上での研究試作を進めています。ネットワークOFCとスマートデバイスOFCに関しては、ユースケースに応じてどちらか一方を設置してOFSを制御します。

## 4. スマートデバイスの業務通信の安全化への応用

スマートデバイス上の業務アプリケーションの通信を安全にする、OpenFlowを用いたスマートデバイス通信制御技術の適用例を示します。

#### (1) 企業ポリシーに従った、通信網の自動選択

ネットワーク側からスマートデバイスに対して、通信の安全性、コストを元に3G、Wi-Fiのいずれかの利用を指示できます。Wi-Fiに関しては、接続するWi-Fiアクセスポイント単位の指定も行うことができます。

#### (2) アプリケーションの利用要件に合った通信網の選択

スマートデバイス上で動作するアプリケーションの要件（通信の安全性、接続性、帯域）及び、ユーザーの状況（業務時間内/外、オフィス内/外、接続経路）に応じた通信網の自動選択を行います。

#### (3) 業務通信のVPNへの自動振り分け

特定アプリケーションの通信や、特定サイトへの通信に対して、自動的にVPN通信を利用するように柔軟に制御可能です。

#### (4) 許可された通信以外の、マルウェア通信の遮断

あらかじめホワイトリストとして指定されたサーバアドレス以外の通信に対して、ユーザーへの通知や、遮断を行うことができます。

これらを実現するためのシステム構成を図4に示します。

このシステムは、第3章で説明したネットワーク側からスマートデバイスの通信制御指示を行うOFC及び、OFCの指示によってスマートデバイス上で通信制御動作を行うOFSから構成されます。これにより、以下の機能を実現します。

#### ・ アプリケーション単位、通信先単位の経路制御

OFCからの指示によって、アプリケーション単位、通信先単位で、3G、Wi-Fi、VPN接続のいずれかの無線通信手段の利用を指定可能です。

#### ・ OFCからの指示のない宛先に対する通信の検知、遮断

スマートデバイス上で動作するマルウェアが、許可された通信先以外に通信を行うのを検知し、ユーザーや管理者に通知及び遮断することができます。

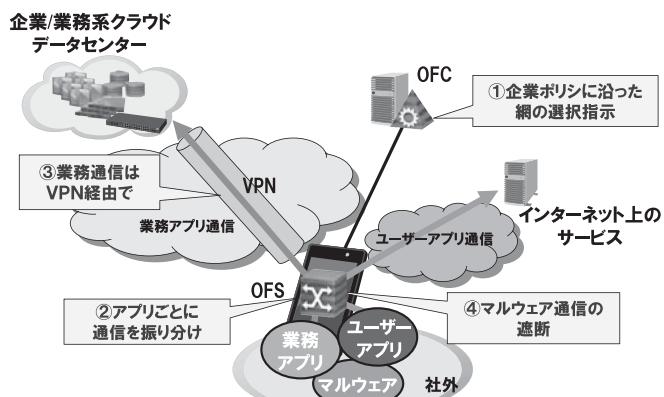


図4 業務通信セキュア化のシステム構成

## 先端技術研究

### OpenFlowを活用した業務用スマート デバイスのセキュアな通信の実現

#### ・ スマートデバイス上の制御アプリケーションとの連携

OFCをスマートデバイス上のアプリケーションから制御するためのAPI (Application Programming Interface) を提供することにより、例えばスマートデバイスの各種コントロール（位置、時間、利用可能ネットワーク）による通信制御機能の切り替えが可能です。

以上の機能により、先に挙げたスマートデバイスの業務通信における（1）～（4）の安全化を実現します。

このような通信制御に関わる多様な機能の実現を、OFC及びOFSを中心としたプラットフォーム上に容易に構築できることが、本システムの特徴となります。新規の通信セキュリティリスクに対応する際には、新たに制御ソフトウェアをネットワーク側もしくはスマートデバイス側のOFCに追加することで、即座に対応可能となります。

## 5. むすび

本稿では、OpenFlowによるスマートデバイス通信制御技術を応用した、スマートデバイスの業務通信を安全化するためのシステム例を紹介しました。

クラウドシステム研究所では本技術を元に、サービス単位で最適な通信特性を持つネットワークを動的に構築するための研究開発に取り組んでいます。この研究成果を元に、スマートデバイスを活用した新サービスの創出に努めてまいります。

なお、本研究の一部は、独立行政法人情報通信研究機構（NICT）の委託研究「新世代ネットワークを支えるネットワーク仮想化基盤技術の研究開発」（課題ア）によるものです。

\*LTEは、欧洲電気通信標準協会（ETSI）の登録商標です。

\*Wi-Fiは、Wi-Fi Allianceの登録商標です。

\*OpenFlowは、Open Networking Foundationの商標または登録商標です。

\*Androidは、Google Inc.の商標または登録商標です。

## 執筆者プロフィール

才田 好則  
中央研究所  
クラウドシステム研究所  
主任研究員

飯星 貴裕  
中央研究所  
クラウドシステム研究所  
主任

森田 弦  
中央研究所  
クラウドシステム研究所

渡邊 義和  
中央研究所  
クラウドシステム研究所  
主任

狩野 秀一  
中央研究所  
クラウドシステム研究所  
主任研究員

## 参考文献

- 1) 狩野秀一ほか：事業者による移動端末制御へのOpenFlowの適用、信学技報 Vol.111 No.468 NS2011-201, pp.123-128, 2012.3

# NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。  
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)

NEC Technical Journal(英語)

## Vol.65 No.3 スマートデバイス活用ソリューション特集

スマートデバイス活用ソリューション特集によせて  
スマートデバイス活用に向けたNECグループの取り組み

### ◇ 特集論文

#### サービス基盤

OSやキャリア不問のスマートデバイスの管理・セキュリティソリューション  
スマートデバイスの活用を支えるソリューションと導入事例  
スマートデバイスに最適な認証ソリューション  
スマートデバイスの利活用に貢献する「Smart Mobile Cloud」  
高品質なサービスの構築を支える「BIGLOBE クラウドホスティング」  
スマートデバイス向けコンテンツ配信サービス「Contents Director」  
BYODに最適なスマートデバイス活用基盤「UNIVERGE モバイルポータルサービス」  
スマートデバイスの利用を促進するリモートデスクトップ・ソフトウェア  
スマートデバイス対応アプリケーション開発を効率化する業務システム構築基盤「SystemDirector Enterprise」  
BIGLOBE ホスティングを活用したスマートフォン向けコンテンツ配信基盤サービス

#### スマートデバイス

Android搭載タブレット「LifeTouch」シリーズの概要  
Windows 8搭載 大画面タブレットPC「VersaPro タイプVZ」  
Android搭載タブレット型パネルコンピュータの開発

#### ソリューション

スマートデバイス対応のペーパーレス会議システム「ConforMeeting」  
スマートフォンを活用したBusinessView保守業務ソリューション  
UNIVERGE遠隔相談ソリューションの見守りサービスへの適用  
画像認識サービス「GAZIRU」の紹介  
インストア・コンシェルジュ～究極の接客ソリューション～  
スマートデバイスを活用した業務システム向けテンプレートの開発  
マルチデバイス対応のビデオコミュニケーションクラウドの紹介

#### 先端技術研究

ユーザーフレンドリーなセキュリティ強化BYODソリューションに向けて  
OpenFlowを活用した業務用スマートデバイスのセキュアな通信の実現  
映像投影とジェスチャー入力によるインタラクション技術  
雑音下でも頑健に動作する音声UI技術とその応用

### ◇ 普通論文

大規模災害における移動通信サービスの輻輳解決に向けた取り組み

### ◇ NEC Information

#### C&C ユーザーフォーラム& iEXPO2012

人と地球にやさしい情報社会へ～あらゆる情報を社会の力に～

NEC講演

展示会報告

### NEWS

2012年度C&C賞表彰式典開催



Vol.65 No.3  
(2013年2月)

特集TOP