# 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

Dennis Gessner・Joao Girao
Ghassan Karame・Wenting Li

**要　旨**

最近、BYOD（個人所有端末の活用）が大きな関心を集めています。従業員が所有するモバイル端末を企業の業務（例えばEメールを読んだり、ドキュメントを編集するなど）に統合し、それらを活用しようというのが企業の描くBYODのシナリオです。しかし、活用されるべきモバイル端末は企業の管理下にはなく、セキュリティの脅威に対して非常に脆弱であることから、このシナリオには重大なセキュリティ上の懸案事項が生じています。本稿では、この問題への取り組みを紹介し、BYODシステムのユーザビリティとフレキシビリティを損なうことなく、BYODシナリオにおけるセキュリティを強化するためのソリューションを提案します。我々が提案するソリューションでは、端末に搭載されたOSを修正することなく、IT管理者が要求するセキュリティポリシーをリモート管理できるようにしています。

キーワード

●BYOD ●MDM ●モバイルセキュリティ ●データプライバシー

## 1. まえがき

最近、BYOD（Bring Your Own Device：個人所有端末の活用）が大きな注目を集めています。BYODとは、従業員が個人的に所有するスマートフォン、タブレット、PCやノートブックなどの端末を企業の業務で利用しようという取り組みです。このソリューションが可能にするのは、企業においては（1）従業員のために企業専用端末を購入する必要がなくなりコスト削減が図れる、従業員においては（2）自分の使用する端末を自ら選択できるというフレキシビリティを享受できる、ということです。

このように明確な利点がある一方で、BYODには深刻な課題も生じています。それは企業の発信・保有するデータ及び従業員の個人端末に保存または表示されるデータのセキュリティ問題です。より具体的に言うと、従業員が自分の端末を100％コントロールしようとする場合、従業員の個人端末上にある企業の機密情報やセキュリティ情報、重要情報へのアクセスの安全性を確保する策はかなり限られてしまうという問題です。

これは、従業員の使用する端末は企業が提供する、という従来のケースとは大きく異なります。従来であれば、企業のIT担当者は、端末のカーネルとOSに必要な修正を加えて、企業が求めるセキュリティポリシーを従業員が無視できないようにすることが可能でした。例えば企業は、特定のOS設定を認証し、認証されたマイクロカーネルと端末上のTPM（Trusted Platform Module）チップを利用してバイナリの正しい実行を保証することができました。

BYODのシナリオでは、このようなソリューションは利用できません。端末が企業のものでなければ、従業員の所有する個人端末に搭載されたカーネルを、企業が修正することは当然正当化できないためです。

そしてこの事実は、「どうすれば、モバイル端末の状態やOSの修正を最小限に抑えながら、端末にセキュリティポリシーを適用できるか」という、セキュリティ上の課題を導き出すことになります。

しかもこの問題への対応は、端末設定を（意図的に、もしくは偶然に）修正してセキュリティポリシーを回避してしまう端末の所有者や従業員が存在する可能性を考慮すると、更に困難になります。

例えば、マルウェアや悪意のあるアプリケーションによる潜在的脅威の下でも、機密情報を端末に保存するときは必ず暗号化され、通信は信頼できる事前承認された対象とだけ行

うなど、企業はこうしたことが保証されることを期待しているのです。

本稿では、この問題に取り組み、端末を変更しなくても、BYOD環境で安全に利用できるモバイル端末を実現するためのソリューションを検討します。最初に、我々の検討で採用する攻撃者のモデルを明確にし、BYOD環境下でアプリケーションの実行と情報アクセスをセキュアに実現する際の課題について簡潔に述べます。続いて、企業アプリケーションの実行環境を強化したり、隔離したりするためのソリューションを提示します。最後に、アプリケーションの隔離を活用したり、ユーザーフレンドリーなMDM（Mobile Device Management）レイヤと連携したりする、補完的なポリシー管理とポリシー実施レイヤについて述べます。

## 2. 関連研究

今日のマーケットには、BYODを支援する製品が多数存在します。これらの製品には、端末の仮想化を基礎とするもの[1) 2)]と、EメールやVPNなどの特定の業務プロセスに対応する専用アプリケーションを提供するもの[3) 4)]があります。他には、企業ネットワークへのリモート接続を提供する製品も存在します。

ただし、これらのソリューションの多くは、搭載OSの修正を必要とする、あるいは受動的な攻撃者（弱攻撃）しか考慮していない、という欠点があります。前述したように、ある従業員のOSを修正することは、(1) 従業員が自身の端末にアップデートをインストールできなくなる、(2) 従業員の同意が必要になる、という点などを考慮すると、必ずしも魅力的なソリューションではありません。

一方、修正を行わない既存ソリューションでは、攻撃者が（例えば悪意のあるアプリケーションなどを利用して）企業とモバイル端末間の通信を傍受して機密資料（例えば暗号鍵や機密Eメール）を取得したり、モバイル端末になりすましたり、認証情報を偽造したりするMITM（中間者攻撃）に対して脆弱であるという問題があります。

TEE（Trusted Execution Environment）[8)]をサポートするシステムでは、システムのブート時にシステムコンポーネントを静的に測定することで信頼の連鎖を構築します。この信頼の連鎖はCore Root of Trustから始まり、端末上で実行されているOSの測定を含んでいます。これらの測定により、OS（またはその他のコンポーネント）で改変が行われたかどうかを判定することが容易になります。またこれらの測定は、端末がリモート対象に対してソフトウェアの真正性を証明するためのリモート証明にも利用することが可能です。

TNC（Trusted Network Connect）も、TPMチップを活用した同様なアプローチ[9)]を採用しています。このソリューションでは、測定の正しさに応じて、ネットワークスイッチがネットワークへのアクセスの許可または拒否を判断します。

## 3. 攻撃者モデル

まず、我々の想定するBYOD設定における、特有の基本的な攻撃者モデルを説明します。攻撃者の関心は、(1) アプリケーションの実行フローを（例えばコードのインジェクション、改変または悪意のあるコードの実行などによって）逸脱させること、(2) 秘密（例えば暗号鍵）または機密情報（例えば機密Eメール、メッセージなど）を取得すること、にあると仮定しています。

上記の目的のため、モバイル端末に悪意のあるアプリケーションをインストールしようとするリモート環境やローカル環境の攻撃者を想定しました。こうした攻撃者は、アプリケーションに付与されている許諾範囲に応じてリソース（例えばインターネット、連絡先など）にアクセスが可能です。この場合、攻撃者は2種類以上のアプリケーションをインストールして企業の機密情報を共謀して取得します。この例としては、権限昇格攻撃や、公開もしくは秘密の通信路を利用した共謀攻撃[7)]が含まれます。

攻撃者はまた、端末に外部周辺機器を接続することも可能です。この場合には、企業サービスにログインするための秘密鍵の取得のみに関心があり、更にモバイル端末のディスク領域全体にアクセスすることが可能な攻撃者を我々は想定しています。

ただし、攻撃者が端末のファームウェアにマルウェアをインストールしたり、低速/高速バスにアクセスしたり、OSに侵入したりといったケースは想定していません。我々の知る限り、このような攻撃の回避に利用できる唯一の有効なメカニズムは、完全準同型関数を併用したトラステッドコンピューティングを用いることであろうと考えます[6)]。

## 4. システムデザインとアーキテクチャ

本章では、モバイル端末を使った改ざん行為を困難にする方法として、アプリケーションの実行を隔離するためのソリューションについて述べます。

### 4.1 概要

マーケットに現存する他のBYODソリューションとは対照的に、我々は以下で、モバイル端末に保存されている情報のセキュリティに「最大限」の保証を実現しつつ、BYODの活用を可能にするソリューションを提示します。

また、我々の提案は企業が保有している機密と見なされるアプリケーション/情報に対してのみ影響を及ぼすので、モバイル端末の所有者に不利益をもたらすことはありません。

### 4.2 アーキテクチャ

我々のソリューションは、モバイル端末内のユーザーアプリケーション領域内に、アプリケーションコンテナをインストールすることで実現するものです（**図1**）。このアプリケーションコンテナは、アプリケーションからシステムへのネイティブ及びJavaのファンクションコールに関連したインターセプターのセットで構成されています。

このコンテナでは、アプリケーション外部への、つまりライブラリやシステムコールに対するファンクションコールを、我々のスタブに置き換えてアプリケーションをロードします。次に、我々のスタブは、例えば暗号を使用したフラッシュメモリへの書き込み実行のような追加機能を提供するだけでなく、端末コンテキスト及びポリシーに基づいて、コールの実行を許可または拒否することも可能にします。同じアプリケーションをこのコンテナの外部で実行することもできますが、その場合、そのアプリケーションから企業ネットワークまたは端末内部の暗号化データにアクセスすることはできません。

我々のアプリケーションコンテナは、長期秘密鍵が攻撃者側に漏えいしないことを保証するように、注意深く構成したセキュリティプロトコルと併せて使用されます。長期秘密鍵は、SIMカードやSDカードなどの不正改ざん防止式（耐タンパ）記憶装置に恒久的に保管することを想定しています。これらの鍵が記憶装置の外部に出ることは絶対になく、その他のどのような対象物にも暴露されることはありません。

我々のソリューションは、各セッションの開始時に企業サーバとの間で一時的な短命セッション鍵を使ってネゴシエートを行うセキュリティアルゴリズムを内蔵しています。これにより、 (1) 攻撃者がモバイル端末のOSに侵入できた

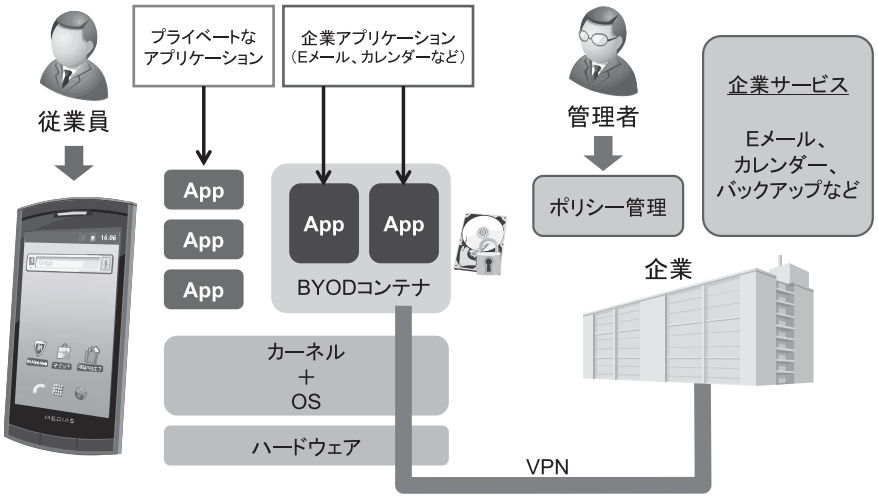


図1　BYODアーキテクチャと展開の様子

としても長期鍵は取得できないこと、及び（2）セッションごとに新規のセッション鍵が発行されるため、システム内にいる攻撃者の優位性は時間的制限を受けることが保証されています。

このように、我々の提案するアーキテクチャは、システムのセキュリティとユーザビリティとの間のトレードオフ関係をもたらします。このアプリケーションコンテナ内では、リモートによるワイプやデータストレージのセキュア化、詳細なポリシー管理など、多数のサービスが提供できるという特長があります。このアーキテクチャは、いかなる他のアプリケーションを実行する際の使用感に影響することもなく、またモバイル端末のプライベートな機能を制限することなく、実現することが可能です。

### 4.3 BYODポリシー管理

我々のソリューションの中心は、市販されているあらゆるモバイル端末に対応可能なポリシーベースの管理です。これにより我々のソリューションは、企業が必要とするセキュリティレベルに応じた最適化をモバイル端末内で行えるモジュラーな手段を提供し、企業が求めるセキュリティレベルの達成に欠かせないセキュリティ機能を、IT管理者がリモートから起動することを可能にします。同時に、システム内の端末


**図2　BYODアプリケーション、現在のセキュリティ課題の表示画面例**

が増えても対応できる効率性とスケーラビリティも備えています。よって、このソリューションは大企業や中規模の企業のシステムとも容易に統合が可能です。

**図2**に、我々のソリューションで実行中のBYODアプリケーションの例を示します。ここでは、MDMサーバから送られた更新ポリシー（規則）が何回か受信されていることが確認でき、企業のITセキュリティポリシーの侵害がなかったことを安全に推定できます。

## 5. むすび

現在のマーケットには数多くのBYODセキュリティソリューションが存在しますが、それらは多くのセキュリティの脅威に対して脆弱であるか、またはモバイル端末に搭載されているOSの修正を必要とするものです。

本稿では、柔軟でユーザーフレンドリーでありながら、企業での利用に対応したセキュリティを総合的に強化できるソリューションについて述べました。我々の提案したソリューションは、アプリケーションコンテナとモバイル端末の堅牢な記憶装置の利用、更に、モバイル端末の長期鍵及び機密資料の秘密性を保証する、特別に開発した暗号プロトコルとの組み合わせでできています。本稿では、これが、モバイル端末のユーザーレベルアプリケーション空間に単一のアプリケーションをインストールするだけで達成できることを示しました。

我々のソリューションは明らかに、モバイル端末のセキュリティとユーザビリティの両立を提供するものです。我々は、この提案が現在、企業で採用している既存のセキュリティポリシーのほとんどに適用可能であると確信しています。この提案はまた、多数の端末に対応したセキュリティポリシーをリモート管理するIT担当者にとっても、便利でかつ容易な手段となることを約束します。最後に、全てのインストールされたアプリケーション及びデータについて、我々のソリューションは、起動したその時点から、ユーザーをITセキュリティポリシーに従わせることを可能にします。

---

*Javaは、米国及びその他の国におけるOracle Corporation及びその子会社、関連会社の登録商標です。

*SDは、SD-3C,LLCの商標です。

**参考文献**

1) Citrix：Best practices to make BYOD simple and secure, http://docs.media.bitpipe.com/io_10x/io_104481/item_530202/BY - OD%20Best%20Practices%20Guide.pdf, 2012.3
2) VMware：The BYOD Opportunity, http://www.vmware.com/files/pdf/view/VMware-BYOD-Opportunity-Whitepaper.pdf, 2012.7
3) Good Technology：Good for Enterprise Android Version：http://media.www1.good.com/documents/gfe_android_ds.pdf, 2012
4) AirWatch LLC.：Mobile Security：http://www.air-watch.com/solu - tions/mobile-security, 2012
5) Array Networks Inc.：Bring Your Own Device (BYOD), http://www.arraynetworks.com/solutions-byod-bring-your-own-device.html, 2012
6) Craig Gentry：Fully homomorphic encryption using ideal lattices, Proceedings of STOC 2009
7) Claudio Marforio, Hubert Ritzdorf, Aurélien Francillon, and Srdjan Capkun：Analysis of the Communication between Colluding Applications on Modern Smartphones, In Proceedings of ACSAC, 2012
8) Global Platform：The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market, http://www.globalplatform.org/documents/GlobalPlat - form_TEE_White_Paper_Feb2011.pdf, 2011.2
9) Trusted Computing Group：TCG Trusted Network Connect TNC Architecture forInteroperability, http://www.trustedcompu - tinggroup.org/files/resource_files/2884F884-1A4B-B294-D001FAE2E17EA3EB/TNC_Architecture_v1_5_r3-1.pdf, Version 1.5, Revision 3, 2012.5

## 執筆者プロフィール

Dennis Gessner
Research Scientist
NEC Laboratories Europe
NEC Europe Ltd.

Joao Girao
Manager
NEC Laboratories Europe
NEC Europe Ltd.

Ghassan Karame
Research Scientist
NEC Laboratories Europe
NEC Europe Ltd.

Wenting Li
Research Associate
NEC Laboratories Europe
NEC Europe Ltd.

# 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