# Android 端末をターゲットとしたボットによる被害防止策の検討

戸田　尚希*，鈴木　秀和，渡邊　晃(名城大学)

Consideration of Measures to Prevent Damage from Bots on Android terminals

Naoki Toda, Hidekazu Suzuki, Akira Watanabe (Meijo University)

## 1.　はじめに

近年のスマートフォンの普及に伴い，Android 端末をターゲットとしたボットが登場している．今後のさらなる普及を考えると，Android 端末をターゲットとしたボット対策は重要な課題であると考えられる．

本稿では，Android 端末でユーザが行う特徴的な操作に着目し，ユーザによる操作か，ボットによる操作かを判断して通信の遮断やユーザへの警告を行うことにより，Android 端末におけるボットによる被害を防止する方法を検討した．

## 2.　Android 端末で動作するボット

Android 端末で動作するボットは PC の場合と同様に，複数の感染した Android 端末同士でボットネットを構成し，攻撃者（Herder）の命令に従って様々な被害を引き起こす．

Android 端末に感染したボットはバックグラウンドで動作し，Herder により指定されたサーバに定期的にアクセスして Herder からの命令を待ち受ける．サーバ経由で Herder からの命令を受けたボットは，その命令に従って Android 端末の位置情報や，保存されている個人情報をサーバに送信する．他にも，勝手に Herder の意図する Web サイトにアクセスしたり，DoS 攻撃を行うことでバッテリの消耗が激しくなる等の被害を受ける可能性がある（Fig.1.）．

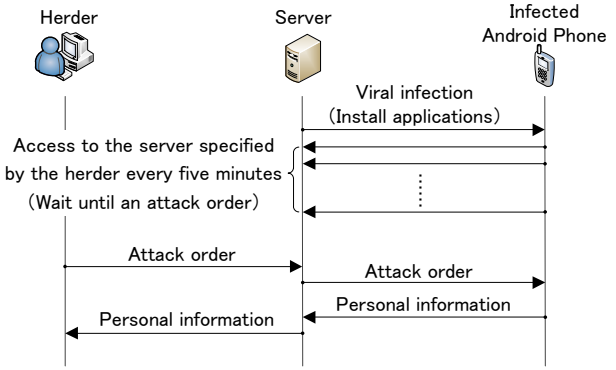



Fig.1. Operation overview of Android bots.

Herder は複数のサーバに接続しているため，仮に 1 つのサーバを停止出来たとしても他のサーバを介して命令を送り続けることが出来る．このため，ボット対策をサーバに対して施すことは，難しいとされている．また，Android 端末が感染するのを完全に防止する対策は PC の場合と同様に困難である．そこでボットの感染は避けられないことを想定し，2 次被害を防止する方法について検討した．

## 3.　Android 端末でユーザが行う特徴的な操作

ボットによる操作とユーザが行う操作には以下のような違いが存在する．メール送信時の送信ボタンを押す操作，Web 閲覧時のブラウザボタンを押す操作，検索時の入力操作がボットにはできないユーザ特有の操作である．従って，Android 端末がネットワークにアクセスする際，直前にこれらの操作があったかどうかにより区別できる．

## 4.　2 次被害の防止対策

ボットによる被害の中に不正なメール送信やネットワークアクセスが挙げられる．メール送信の際には，メール送信ボタンを押す操作の有無により正規の操作であるかを判断する．また，ネットワークアクセスの際には，ブラウザボタンを押す操作の有無及び，検索の際の入力操作の有無により，正規の操作であるかを判断する．ボットによる操作であると判断された場合，オープンソースのアプリケーションである「DroidWall」を利用してボットが内包されたアプリケーションの 3G，Wi-Fi 通信を遮断する．また，ユーザに対してアラームを提示し，通信を遮断したアプリケーションのアンインストールを促す警告を出す（Fig.2.）．

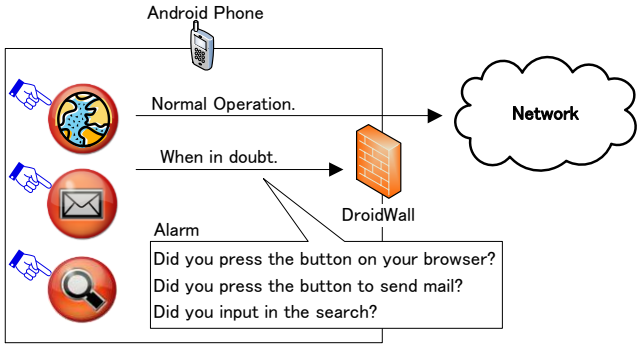



Fig.2. Principle of the proposed system.

## 5.　むすび

Android 端末におけるボット対策として，Android 端末でユーザが行う特徴的な操作を考察した．ネットワークアクセス時の直前にボタン操作がない場合，通信を遮断することで，ボットによる 2 次被害を防止する方法を検討した．今後は，ボタン操作の有無の検出方法を検討し，この方法の有効性を確認するための実装を行う．

文　献

(1)　平田, 他：平成 20 年度電気関係学会東海支部連合大会論文集，講演番号 O-077，2008

# Android端末をターゲットとした ボットによる被害防止策の検討

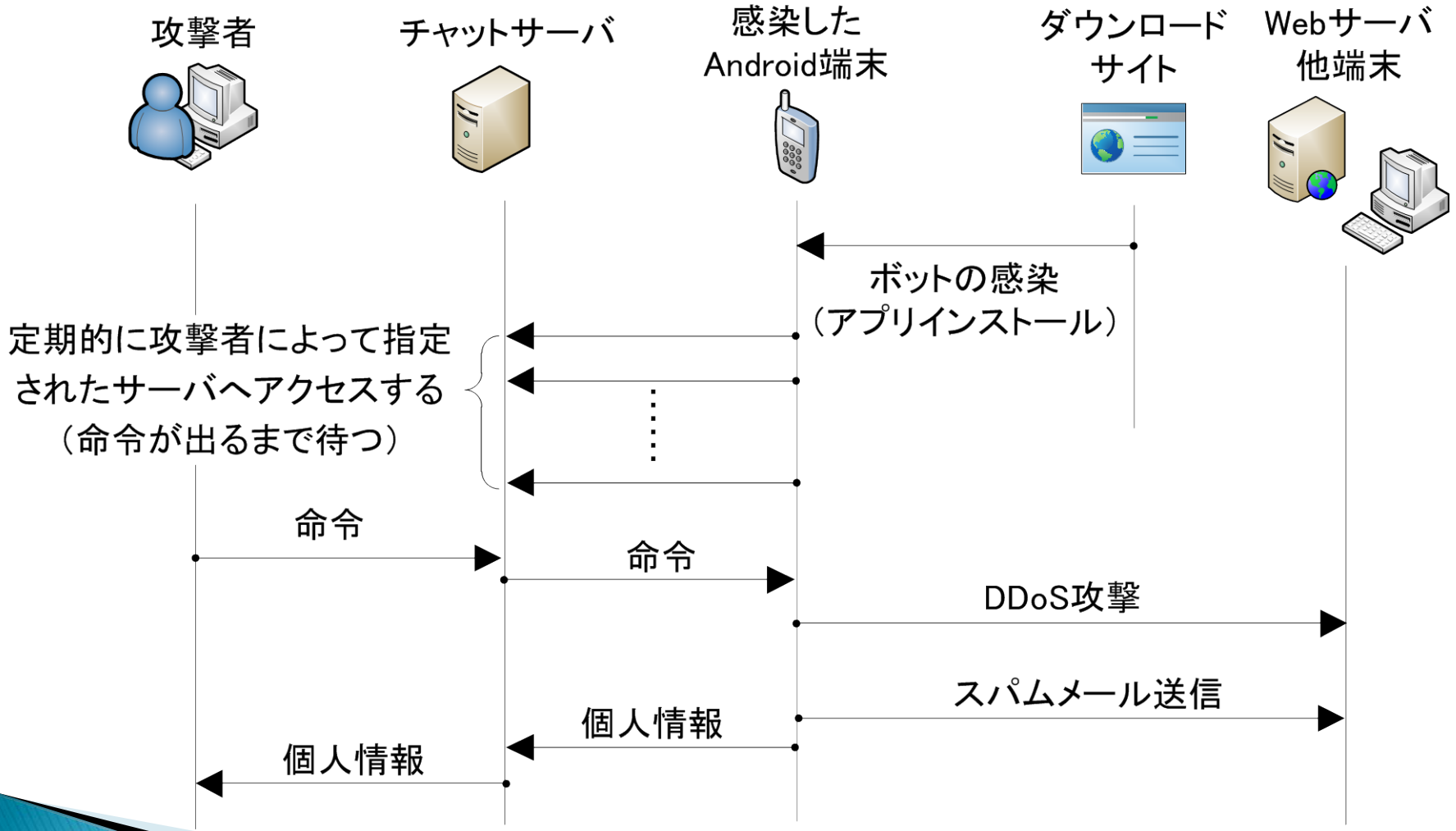
名城大学　理工学部
戸田　尚希，鈴木　秀和，渡邊　晃

# 研究背景

- スマートフォンの普及
- Android OSの脆弱性をついたボットの出現
- ユーザのセキュリティ対策不足

Android端末にボットが
急速に広まる恐れがある

# ボットとは


攻撃者
チャットサーバ
感染した
Android端末
ダウンロード
サイト
Webサーバ
他端末
ボットの感染
（アプリインストール）
定期的に攻撃者によって指定
されたサーバへアクセスする
（命令が出るまで待つ）
命令
命令
DDoS攻撃
スパムメール送信
個人情報
個人情報

# 既存技術

- ウイルス対策アプリ
  - ウイルスバスター
  - ノートン
  - MacAfee

ウイルス定義ファイルを利用したパターン・マッチングが主流

新種や亜種のウイルスに対応出来ない

# ユーザによる対策

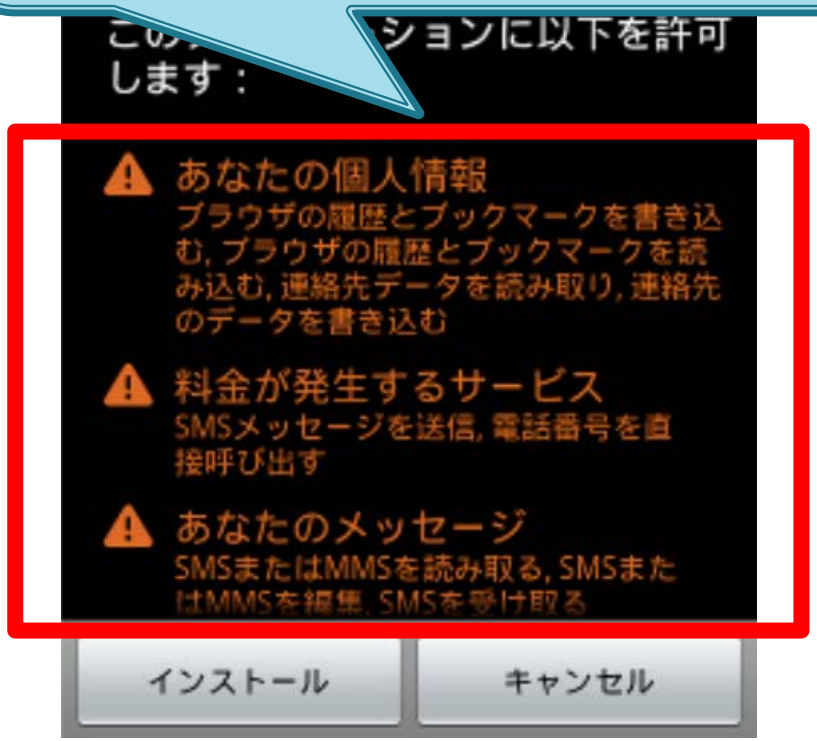
- Android Market以外のダウンロードサイトからアプリを入手しない
- 提供元不明のアプリはインストールしない設定をする
  - 野良アプリのインストールが阻止できる
- ウイルス対策アプリを導入する
- アプリインストール時のアクセス許可を確認する

# アクセス許可確認による感染対策

- アプリのインストール時に表示される
- 表示されるアクセス許可により，不正アプリかどうかを判断する

非常に困難

個人情報，位置情報，
料金が発生するサービス



# 提案方式

ボットの感染を防ぐのは難しい事を
前提とした2次被害の防止策を提案

- ユーザが行う特徴的な操作
  - ユーザによる操作かボットによる操作かを見分ける
- ファイアウォールアプリによる通信制御
  - ボットによる操作と判断された場合の通信の遮断

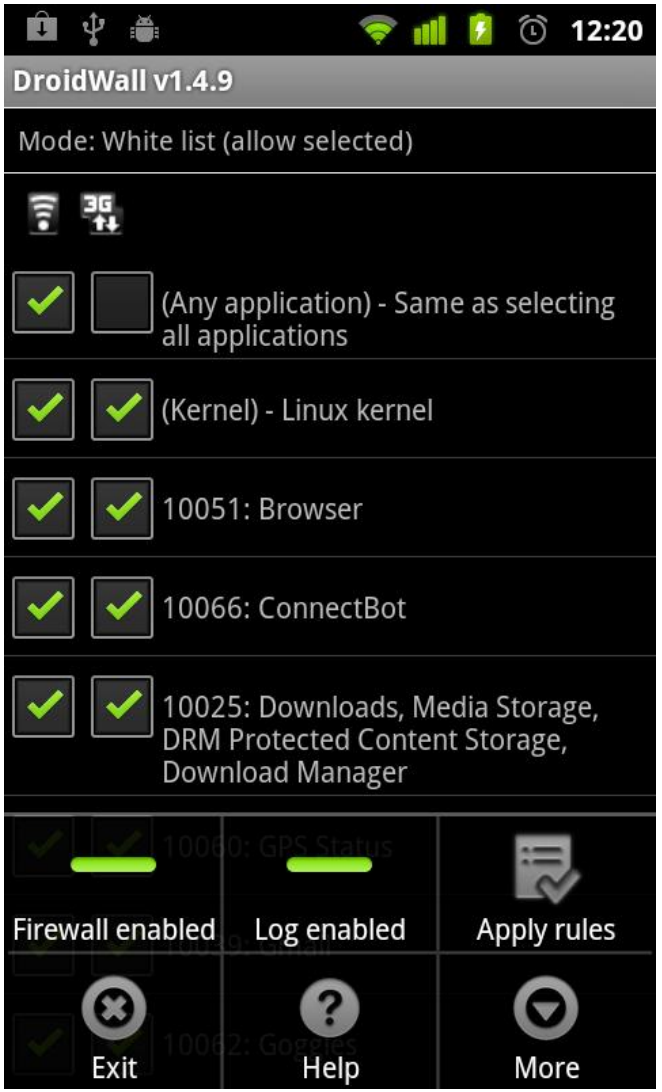
# ユーザが行う特徴的な操作

- メール送信時の送信ボタンを押す操作
- Web閲覧時のブラウザボタンを押す操作
- 検索時の入力操作

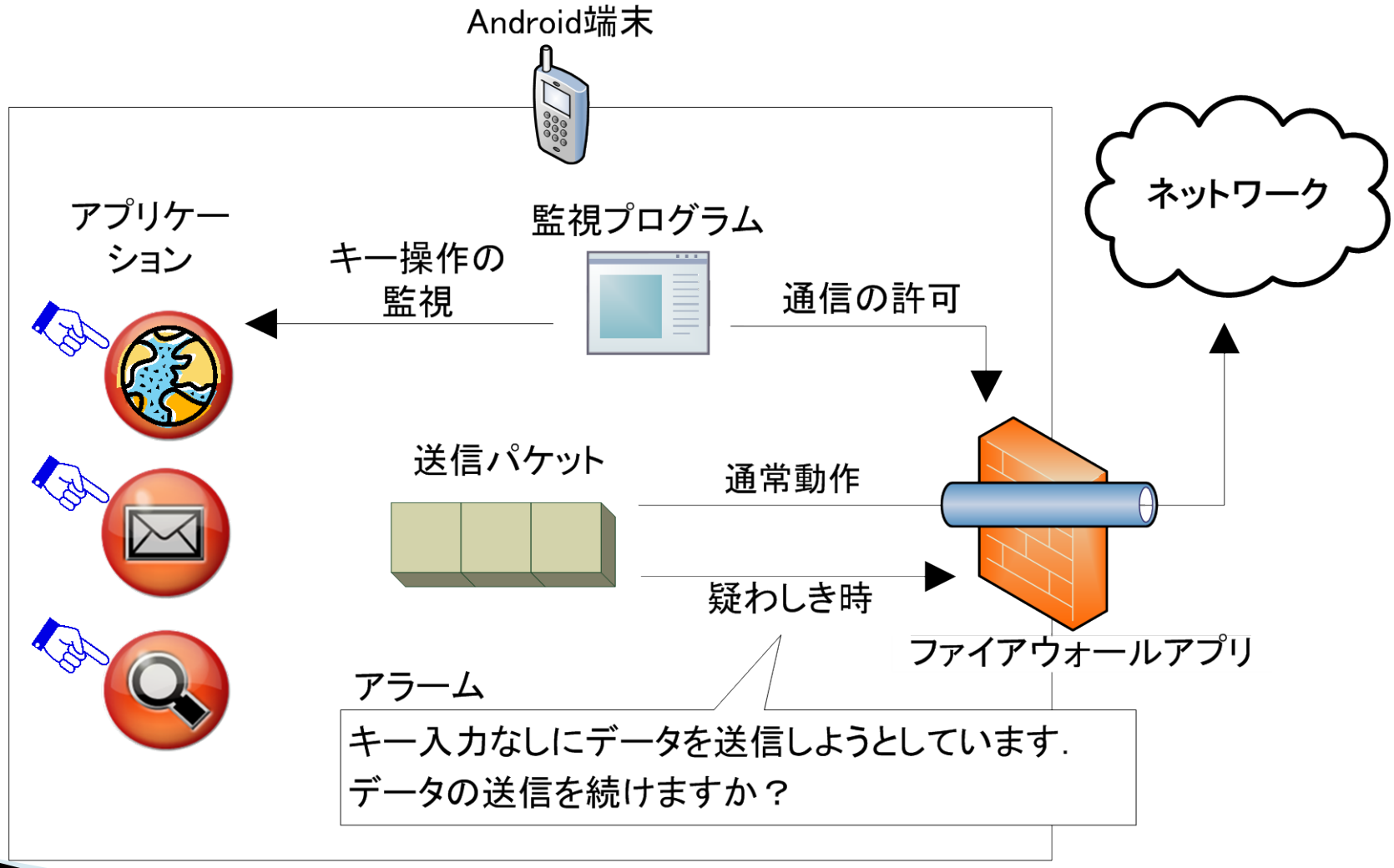
ボットには出来ない操作

# ファイアウォールアプリ

- 「DroidWall」が利用出来るのでは？
- オープンソースのアプリケーション
- iptablesを利用したファイアウォールアプリケーション
- アプリケーション単位で3G,WiFiの通信を制御



# 提案方式の動作


Android端末
ネットワーク
アプリケーション
監視プログラム
キー操作の監視
通信の許可
送信パケット
通常動作
疑わしき時
ファイアウォールアプリ
アラーム
キー入力なしにデータを送信しようとしています．
データの送信を続けますか？

# 提案方式の利点

- 新種・亜種のボット対策に有効
- DDoS攻撃への加担防止やスパムメール送信の防止に有効
- バッテリーの消耗防止に有効

DDoS攻撃：Distributed Denial of Service attack

# まとめ

- ボットによる2次被害の防止策の検討
  - Android端末でのキー操作の有無により，ボットによる操作を検知し，通信制御を行う
- 今後の課題
  - 提案方式の実装と評価