

自然と数理8「情報と数理の世界」

## 第6回 人工知能とロボット3

名古屋市立大学  
システム自然科学研究科  
渡邊 裕司

2013/10/31 人工知能とロボット3 1

### 渡邊担当分「人工知能とロボット」のスケジュール(案)

日付	通算回	講義内容
10/17	第4回	人工知能の概要、基礎的研究
10/24	第5回	ゲーム情報学、生物に学んだ機械学習
10/31	第6回	データマイニング、スマートフォンのセキュリティ
11/7	第7回	サイボーグ、ロボット

授業で用いた資料は、10月28日より下記サイトにて公開  
<http://www.nsc.nagoya-cu.ac.jp/~yuji/lecture/InfoMathWorld/>

2013/10/31 人工知能とロボット3 2

### 今日のお話

- ◆ スマートフォンのセキュリティ
  - ◆ 現状と脅威
  - ◆ 利用者の対策
- ◆ 研究事例
  - ◆ コンピュータセキュリティシンポジウム2012, 2013
  - ◆ 行動的特徴を用いたログイン時以外の認証
    - ◆ タッチ操作に基づく認証
    - ◆ データマイニング
    - ◆ 加速度センサを用いた歩行時の認証

2013/10/31 人工知能とロボット3 3

### スマートフォンのセキュリティ

2013/10/31 人工知能とロボット3 4

### 問1:主に使っている携帯電話は何ですか?

1. Androidスマートフォン
2. iPhoneスマートフォン
3. 従来の携帯電話
4. 携帯電話を持っていない

Nexus 4 by developer.android.com

iPhone 5s by Zach Vega

2013/10/31 人工知能とロボット3 5

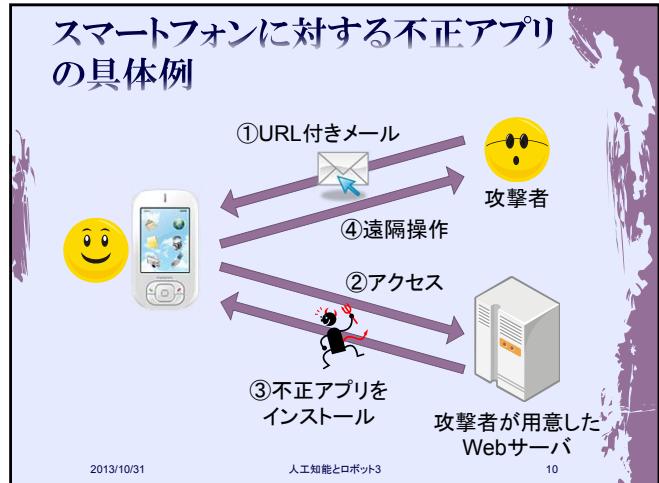
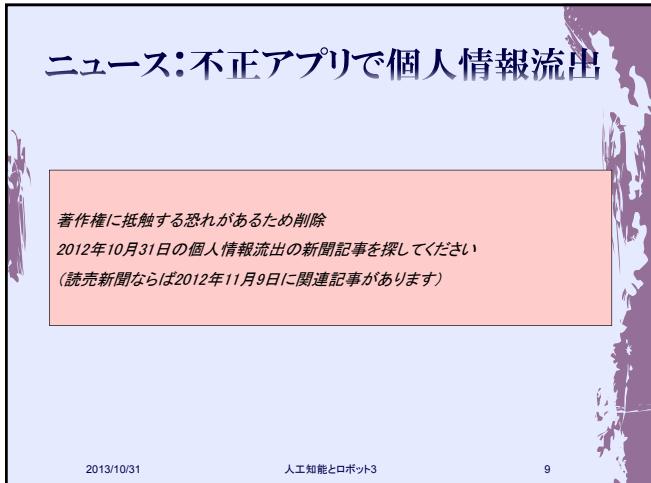
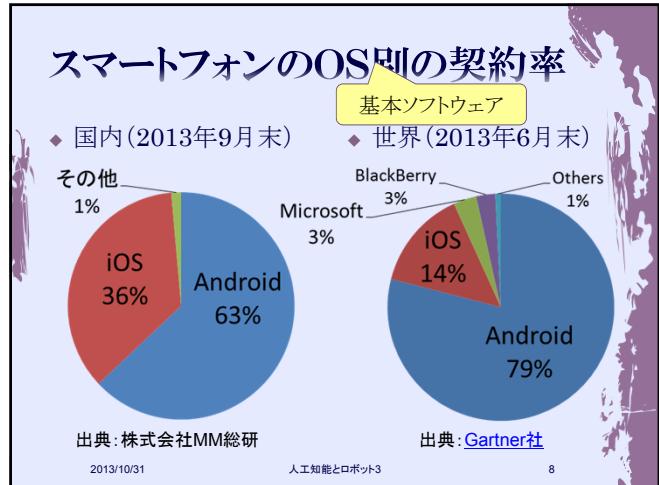
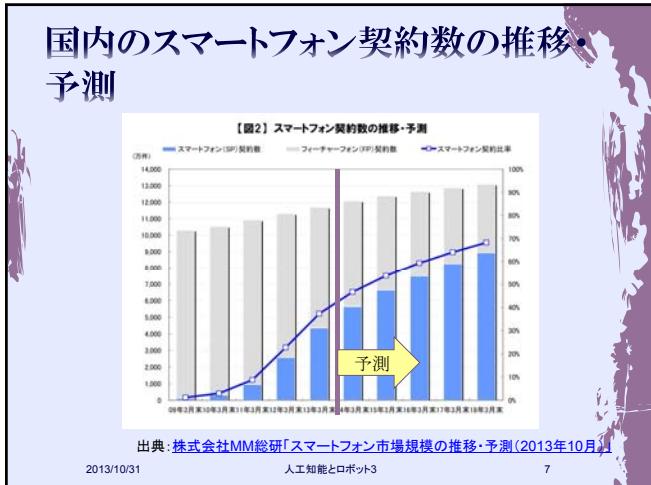
### 国内のスマートフォン出荷台数の推移・予測

【図1】スマートフォン出荷台数の推移・予測

年度	スマートフォン(SP)出荷台数 (万台)	フィーチャーフォン(FP)出荷台数 (万台)	スマートフォン出荷台数比率 (%)
08年度	100	3,500	3%
09年度	200	3,500	5%
10年度	500	3,500	14%
11年度	1,500	4,500	25%
12年度	3,000	4,000	40%
13年度	3,500	4,000	40%
14年度	3,800	4,000	45%
15年度	3,800	4,000	45%
16年度	3,800	4,000	45%
17年度	3,800	4,000	45%

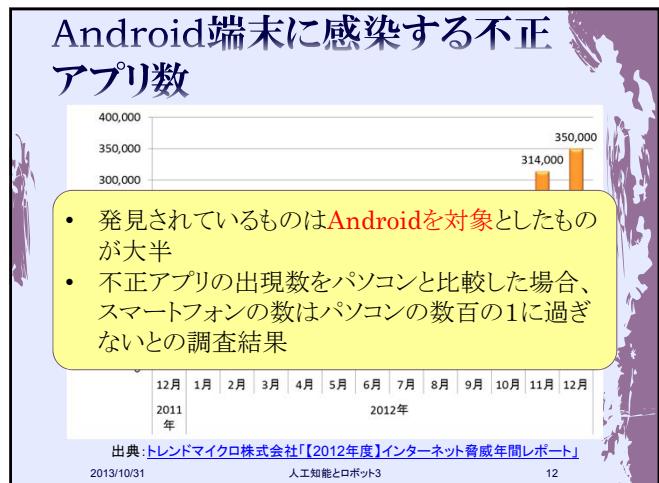
出典:株式会社MM総研「スマートフォン市場規模の推移・予測(2013年10月)」

2013/10/31 人工知能とロボット3 6



## スマホ対象の不正アプリ

発見年月	名称	OS	概要
2009年11月	iKee	iOS	JailbreakしたiPhoneに感染し、勝手に壁紙を変更するワーム
2010年8月	FakePlayer	Android	Androidを狙った初めてのマルウェア。ロシアのプレミアムSMSに勝手に送信する
2010年12月	Geinimi	Android	Androidを狙った初めてのボットウイルス。インストール後、端末内の情報を収集し、サーバからの指令を待つ
2011年2月	DroidDream	Android	OSのぜい弱性を突き、管理者権限を奪取するボットウイルス。起動時に、定期的にサーバと通信し、コマンドやアップデートを実行する
2011年5月	Lightdd	Android	アプリケーション起動なしに端末を監視し、着信や受信、通話の終了などの際に悪性コードを実行し、外部に情報を送信する
2012年1月	FakeTimer	Android	電話番号やメールアドレス等を外部に送信とともに、これらの情報とともに架空の利用料金を請求するポップアップを画面に表示させる



## 問2:スマートフォンのセキュリティ対策をしていますか?

- 対策している
- 対策していないが、直ぐにでも対策をする予定
- 対策していないが、条件によって検討したい
- 分からない

2013/10/31 人工知能とロボット3 13

## 問3:スマートフォンのセキュリティ対策をしない理由は何ですか?

- 必要だと思うが、実際に何をすればよいか分からない
- 必要だと思うが、対策をするほどは気にしていない
- 必要だと思うが、お金を払ってまで対策したくない
- 必要だとは思わない
- セキュリティ対策をする理由が分からない
- その他

2013/10/31 人工知能とロボット3 14

## スマートフォンの情報セキュリティに関する利用者の意識

状況	割合
対策している	38.5%
対策していないが、直ぐにでも対策をする予定	49.9%
対策していないが、条件によって検討したい	8.1%
分からない	3.4%

理由	割合
必要だと思うが、実際に何をすればよいか分からない	42.9%
必要だと思うが、対策をするほどは気にしていない	25.3%
必要だと思うが、お金を払ってまで対策したくない	20.8%
必要だとは思わない	5.1%
セキュリティ対策をする理由が分からない	1.5%
その他	4.4%

出典: 総務省スマートフォン・クラウドセキュリティ研究会最終報告  
株式会社ネットマイル「スマートフォンのセキュリティに関する調査」

2013/10/31 人工知能とロボット3 15

## 平成24年7月27日掲載の政府広報

平成24年7月27日掲載

OutLine

- スマートフォンを安心・安全に使うために情報セキュリティ対策をしましょう
- 必要な知識
- 実際の操作
- コラム

2013/10/31 人工知能とロボット3 16

## スマートフォントと携帯電話との相違

- 使いたいアプリケーションを自由にインストール可能
- タッチパネルを搭載した製品が多い
- 通信キャリアのネットワークだけでなく無線LANを経由した通信も可能
- 端末メーカ、OS提供業者、通信キャリア、アプリケーション提供業者が混在した水平展開型のサービス

2013/10/31 人工知能とロボット3 17

## スマートフォンのビジネスモデル

従来の携帯電話市場

スマートフォン市場

スマートフォンは

- ・従来の携帯電話の延長
- ・高機能な携帯電話端末

ではない！！

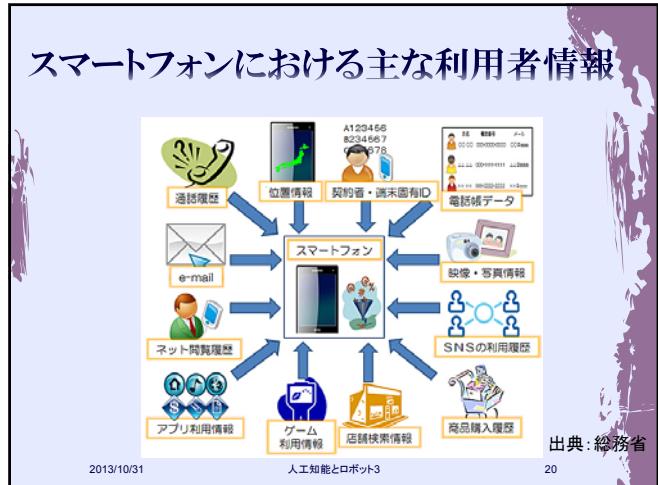
出典: 総務省

2013/10/31 人工知能とロボット3 18

## スマートフォントとパソコンの相違

- ◆ 電話、カメラ、GPS等のデバイスを搭載  
プライバシー問題
- ◆ 小型で処理能力が限られるためセキュリティに割けるリソースが少ない  
→アプリケーションを制限された範囲でのみ動作させるアクセス制限(サンドボックス)の使用  
→OSの設計としては、一般的にパソコンより安全性が高い

2013/10/31 人工知能とロボット3 19



## スマートフォン情報セキュリティ3か条

1. OS(基本ソフト)を更新
  - ◆ 更新の際には、機能の追加修正のほかに、せい弱性の修正
  - ◆ 古いOSではウイルス感染や情報漏えいの危険性が高い
2. ウイルス対策ソフトの利用を確認
  - ◆ ウイルスの混入したアプリケーションが発見
  - ◆ 携帯電話会社などが提供するウイルス対策ソフトを導入
3. アプリケーション(アプリ)の入手に注意
  - ◆ アプリの事前審査を十分に行っていないアプリ提供サイトでは、ウイルスの混入したアプリが発見
  - ◆ 安全性の審査を行っている提供サイトを利用
  - ◆ インストールの際にはアプリの機能や利用条件に注意

出典: 総務省(配布資料)

2013/10/31 人工知能とロボット3 21

## 携帯電話会社のウイルス対策ソフト

著作権に抵触する恐れがあるため削除  
各携帯電話会社が提供しているウイルス対策ソフトを探してください

2013/10/31 人工知能とロボット3 22

## アプリケーション提供サイト

アプリケーション提供サイト			提供アプリケーション		
運営者	名称	種別	提供対象	登録数	事前審査
Apple	App Store	配信	iPhone, iPad	約58.5万 (平成24年2月)	あり
Google	Google Play	配信	Android	45万以上 (平成24年3月)	なし
NTTドコモ	dマーケット	紹介	NTTドコモのAndroid	約1,000 (平成24年3月)	あり
KDDI	au Market	配信	KDDIのAndroid	約7,500 (平成24年4月)	あり
ソフトバンクモバイル	@アプリ	紹介	ソフトバンクモバイルのAndroid	約2,000 (平成24年4月)	あり

出典: 総務省

2013/10/31 人工知能とロボット3 23

## Google Play™の安全への取り組み

- ◆ ユーザからの指摘を受けて迅速に悪性アプリを駆除
- ◆ 悪性アプリの事前審査、定期検査を担う“Bouncer”的導入
- ◆ 開発者登録としてクレジットカードの登録、\$25の支払い

一定の安全性は確保、しかし...

出典: KDDI研究所 竹森敬祐、「スマートフォンとセキュリティ」、平成24年第1回学術情報基盤オーブンフォーラム資料、2012/07/04

2013/10/31 人工知能とロボット3 24

## スマートフォンプライバシーガイド

- ◆ スマートフォンのサービス構造を知る
    - ◆ 従来の携帯電話と違い水平展開型のサービス
  - ◆ アプリの信頼性に関する情報を自ら入手し理解するよう努める
    - ◆ 利用者も受け身ではなく、アプリケーションの機能や評判、提供者など、アプリケーションの信頼性に関する情報を自ら入手し、理解に努める
    - ◆ さらに不安ならば、利用を避けることも大切
    - ◆ 例: [LINE](#)、読売新聞「LINEのシステム変更&設定 2013年版まとめ」
  - ◆ 利用者情報の許諾画面等を確認する(次のスライド)!!

2013/10/31

人工知能とロボット3

25

## 利用者情報の利用許諾画面の例

#### ＜Android OS搭載スマートフォンでアプリをダウンロードする場合＞



(※Google Playから入手したアプリをもとに総務省作成)

出典: 総務省

26

## その他の対策

- ◆ 盗難・紛失時に不正利用されないようにするために  
→従来の携帯電話と同様にパスワードなどで端末にロック  
→リモートロック、リモート検索、リモートワイプも併用
  - ◆ iOSとAndroidでの制限を解除しないこと
  - ◆ 制限: アプリケーション、テザリング、カスタマイズ
  - ◆ 方法: iOSではJailbreak(脱獄)、Androidではroot化
  - ◆ 理由: 不正プログラムが感染しやすく、メーカサポートが受けられなく可能性が増大

2013/10/31

人工知能とロボット3

27

## 行動的特徴を用いたログイン時以外の認証

## 当研究室での最新研究事例

2013/10/31

人工知能とロボット3

28

コンピュータセキュリティシンポジウム  
CSS2012



2013/10/31

人工知能とロボット3

29

## CSS2012の写真



2013/10/31

人工知能とロボット3

30

## CSS2012のプログラム(1日目)

### 日程表

日時	時間	会場1 小ホール	会場2 国際 会議場	会場3 501 会議室	会場4 601 会議室	会場5 多目的 ホール	会場6 401 会議室	デモ会場 3階 ホール
10月 30日 (火)	09:30- 12:00	MWS Cup 優 勝/MWSハン ズオン	—	—	—	—	—	—
	13:00- 14:20	1A1 Androidセ キュリティ (静的 解析)	1B1 Androidセ キュリティ (1)	1C1 秘密分散・ 共通鍵暗 号(1)	1D1 個人情報・ プライバシ 保護(1)	—	—	—
	14:40- 16:00	1A2 Androidセ キュリティ (動的 解析)	1B2 Androidセ キュリティ (2)	1C2 秘密分散・ 共通鍵暗 号(2)	1D2 個人情報・ プライバシ 保護(2)	—	—	デモ
	16:10- 17:10	—	特別講演 1	—	—	—	—	—
	17:20- 18:20	MWS Cup 講評	—	—	—	CSSx2.0	—	—
	18:30- 21:00	—	—	—	—	—	—	—

2013/10/31

人工知能とロボット3

31

## 背景

- ◆ スマートフォンの爆発的な普及
- ◆ スマートフォンにはアドレス帳など多くの重要な個人情報
- ◆ これらの個人情報を不正使用者から守ることが必要



正規ユーザー



不正使用者

### ユーザ認証システム

- ◆ パスワード認証(IDとパスワードを利用)
- ◆ バイオメトリクス認証(身体的特徴・行動的特徴を利用)

2013/10/31

人工知能とロボット3

33

## 身体的特徴を利用したバイオメトリクス認証

- ◆ 指紋や静脈、網膜を利用
- ◆ 利点
  - ◆ ユーザ間の差が明確であるため、ユーザ識別が容易
  - ◆ 時間的変化に強い
- ◆ 問題点
  - ◆ 認証時に専用の読み取り機が必要
  - ◆ 身体的特徴の損失(怪我など)
  - ◆ ユーザ情報が一度漏洩すると、不正ユーザの侵入を防止することが困難
  - ◆ ログイン後の頻繁な認証はわずらわしい



2013/10/31

人工知能とロボット3

35

## CSS2012のプログラム(2, 3日目)

日時	時間	会場1 MWS(DIM)	会場2 MWS(特別 セッション)	会場3 MWS(特別 セッション)	会場4 MWS(特別 セッション)	会場5 MWS(特別 セッション)	会場6 MWS(特別 セッション)	会場7 MWS(特別 セッション)	会場8 MWS(特別 セッション)
10月 31日 (水)	08:40- 12:00	2A1 ユビキタス セキュリティ	2B1 暗号プロト コル(1)	2D1 コードレス セキュリティ 保護(1)	2D2 コードレス セキュリティ 保護(2)	2E1 セキュリティ評 価・監査	—	—	—
	10:20- 11:20	2A2 MWS(特別 セッション)	2B2 暗号プロト コル(2)	2D3 暗号理論 (1)	2D4 暗号理論 (2)	2E2 匿名化方 式(1)	—	—	デモ
	13:00- 14:20	2A3 ネットワー ク監視・通 信(1)	2B3 ネットワー ク監視・通 信(2)	2D5 匿名化方 式(2)	2D6 匿名化方 式(3)	2E3 心理学と トラスト	—	—	デモ
	14:40- 16:00	2A4 MWS(特別 セッション)	2B4 ネットワー ク監視・通 信(3)	2D7 匿名化方 式(4)	2D8 匿名化方 式(5)	2E4 セキュリティ評 価・監査	—	—	デモセッ ション
	18:10- 17:10	—	—	—	—	—	—	—	—
	17:20- 18:00	特別講演 2	—	—	—	—	—	—	—
11月 1日 (木)	08:40- 10:00	3A1 MWS(通信 解説)	3B1 コンピュータ ネットワーク セキュリティ	3C1 暗号ハッカ ーク(1)	3D1 認証・バイ オメトリク ス(1)	3E1 セキュリティ 評価・監 査	MWS ハンズ オン	—	—
	10:20- 11:20	—	3B2 Webメー リセキュリ ティ	3C2 暗号シス テム実装	3D2 認証・バイ オメトリク ス(2)	3E2 セキュリティ 評価・監 査	—	—	—
	19:00- 21:00	—	—	—	—	—	—	—	—

2013/10/31

人工知能とロボット3

32

## パスワード認証

ユーザIDとパスワードが一致 ➔ 正規ユーザー

- ◆ 利点
  - ◆ 導入が容易
  - ◆ 正しいパスワードならば認証に失敗しない
- ◆ 問題点
  - ◆ パスワードが外部に漏洩すると容易に不正使用可能
  - ◆ パスワード認証はログイン時に一度だけ行うことが多く、ログイン時以外には正規ユーザーだけでなく不正使用者も自由にアクセス可能



2013/10/31

人工知能とロボット3

34

## 行動的特徴によるバイオメトリクス認証

### 行動的特徴によるバイオメトリクス認証

- ◆ パソコンでは1990年代から個人の操作の特徴や癖を用いた行動的特徴によるバイオメトリクス認証の広範な研究
  - ◆ キー操作、マウス操作、コマンド列
- ◆ 利点
  - ◆ 指紋読み取り機など特別な装置が不要
  - ◆ ログイン時以外も継続的に監視が可能
- ◆ 問題点
  - ◆ ユーザの作業、心理状態、時間変化の影響を受けやすい
  - ◆ 識別すべき人数が増加するにつれて認証精度が悪化



2013/10/31

人工知能とロボット3

36

## スマートフォンにおける行動的特徴による認証

- 携帯電話やスマートフォンにおける行動的特徴による認証の研究も最近始められつつある
  - キー操作
  - 加速度センサ
  - タッチパネル
  - 複数センサ
- ログイン時以外の認証を扱った研究はまだ少ない
  - ログインタスクは全ユーザーに対して共通にできる
  - しかし、ログイン時以外ではタスクはユーザー毎に異なり、認証は難しくなる

2013/10/31 人工知能とロボット3 37

## 研究の最終目的

- 最終目的
 

スマートフォンにおいてタッチパネル、加速度センサなど複数センサから各ユーザーの操作や行動の特徴を抽出し、**ログイン時以外も継続的に認証するシステム**の構築

手始めに

タッチ操作に着目  
 タッチパネル式のスマートフォンでは独特の操作(フリック、タップ、ピンチなど)があり、認証に利用できるかどうか？

2013/10/31 人工知能とロボット3 38

## スマホにおける基本タッチ操作

2013/10/31 人工知能とロボット3 39

## iOS用簡易文章閲覧アプリ

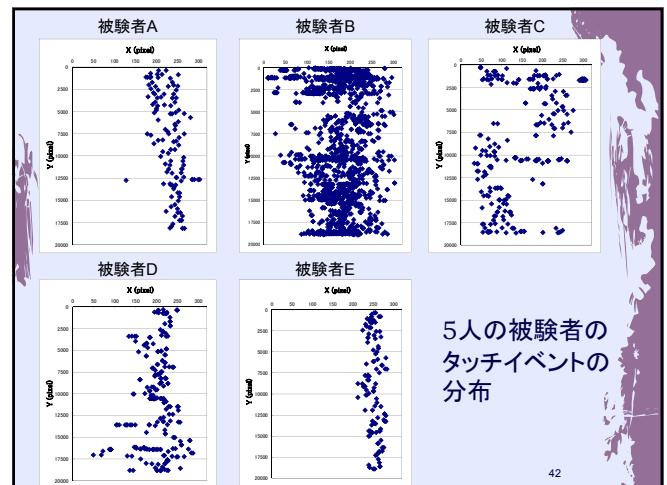
480ピクセル  
320ピクセル  
UITextView Class X [0, 320]  
Y [0, 20000]  
フリック  
縦スクロール  
ドラッグ

2013/10/31 人工知能とロボット3 40

## 操作履歴の取得

- 簡易文章閲覧アプリによって取得される操作履歴は $\{event, (x, y), t\}$ の形式
  - event : 1. 指をタッチした瞬間  
2. 指を動かしたとき  
3. 指を離したとき
  - $(x, y)$  : タッチイベントを検出したときの座標位置
  - $t$  : 検出時刻

2013/10/31 人工知能とロボット3 41



## 操作特徴の抽出

- 操作履歴から基本的な操作特徴を抽出
  - 指のX座標
  - 指の移動距離
  - 指の移動速度
  - 指の移動角度
- オーバーラップさせつつ、10操作単位で各操作特徴の平均値と標準偏差を計算

2013/10/31 人工知能とロボット3 43

## 分類アルゴリズム

- 認証: 本人かそうでないかを分類  
→ 特徴の平均値と標準偏差を分類アルゴリズムを適用
- 分類アルゴリズムとして、加速度センサを用いた既存研究を参考にして、WEKAのデータマイニングソフトから決定木(J48)とニューラルネットワーク(NN)を使用
- 設定はデフォルトのまま、10分割交差検証を使用

2013/10/31 人工知能とロボット3 44

## データマイニング

- データマイニングとは、
  - 大量の整理されていないデータから役に立つと思われる情報を見つけだす手法
  - 例: ネットショッピングで、過去の買い物データをもとに「おすすめ品」を提示
- 機械学習との違い
  - 機械学習と交差する部分が大きく、技法も同じなので混同されやすい
  - 機械学習の目的は、訓練データから学んだ「既知」の特徴に基づく予測
  - データマイニングの目的は、それまで「未知」だったデータの特徴の発見

2013/10/31 人工知能とロボット3 45

## 機械学習

前回資料

- 機械(コンピュータ)が自らの経験から将来使えそうな知識を発見・獲得すること
- 手法
  - 決定木学習
  - ニューラルネットワーク
  - 進化論的計算手法
  - 人工免疫システム
  - 強化学習
  - サポートベクターマシン
  - ベイジアンネットワーク 等

生物に学んだ

- 決定木学習 ← 脳・神経系
- ニューラルネットワーク ← 遺伝・進化系
- 進化論的計算手法 ← 免疫系

2013/10/31 人工知能とロボット3 46

## ニューロンモデル

$$u_i = \sum_{j=1}^n w_{ij} x_j$$

$$y_i = f(u_i - \theta_i)$$

前回資料

階段関数

シグモイド関数

2013/10/31 人工知能とロボット3 47

## ニューラルネットワーク

前回資料

- 階層型ネットワーク
- 相互結合型ネットワーク

ニューラルネットワークの学習:  
ニューロン間の結合荷重を変更→所望の出力を獲得

2013/10/31 人工知能とロボット3 48

## 決定木の例:ゴルフする?しない?

著作権に抵触する恐れがあるため削除  
以下の「決定木による分類モデルとは?」のページを直接参照ください  
<http://musashi.sourceforge.jp/tutorial/mining/xtclassify/model.html>

2013/10/31 人工知能とロボット3 49

## 予備実験結果

- 被験者は5人(内スマートフォン所持者は4人)
- 作成した簡易文章閲覧アプリをiPod touchで使用してもらい、操作履歴を取得

被験者	検出できたイベント数	検出できた移動距離の数
A	120	7
B	2420	339
C	270	52
D	250	72
E	110	24

2013/10/31 人工知能とロボット3 50

## タッチ操作の結果:FARとFRR

被験者	決定木(J48)		ニューラルネットワーク(NN)	
	FAR (%)	FRR (%)	FAR (%)	FRR (%)
B	18.2	4.5	12.4	4.2
C	0.7	9.3	1.2	7.0
D	4.9	25.4	1.3	14.3
E	0	0	0.2	0
Ave.	5.95	9.8	3.78	6.38

2013/10/31 人工知能とロボット3 51

## 評価指標:FARとFRR

提出用資料

- 他人受入率**(False Acceptance Rate: FAR)
  - 他人を誤って本人として受け入れてしまう割合
$$FAR = \frac{\text{認証システムが受け入れた他人のデータ数}}{\text{他人のデータ数}}$$
- 本人拒否率**(False Rejection Rate: FRR)
  - 本人を誤って他人として拒否してしまう割合
$$FRR = \frac{\text{認証システムが拒否した本人のデータ数}}{\text{本人のデータ数}}$$
- FARとFRRともに小さいほど好ましい認証
  - 指紋認証 FAR 0.0001% FRR 0.001%
  - 顔認証 FAR 0.1% FRR 1%
  - オンライン署名認証 FAR 0.6% FRR 0.2%

2013/10/31 人工知能とロボット3 52

## タッチ操作の結果:FARとFRR

被験者	決定木(J48)		ニューラルネットワーク(NN)	
	FAR (%)	FRR (%)	FAR (%)	FRR (%)
B	18.2	4.5	12.4	4.2
C	0.7	9.3	1.2	7.0
D	4.9	25.4	1.3	14.3
E	0	0	0.2	0
Ave.	5.95	9.8	3.78	6.38

• 被験者によって認証精度がかなり異なる  
• 決定木よりもニューラルネットワークの方が良い精度である

他の認証研究と比較すると、十分に良い精度とは言えない

2013/10/31 人工知能とロボット3 53

## コンピュータセキュリティンボジウム CSS2013



2013年10月31日 人工知能とロボット3 54

## CSS2013の写真



2013/10/31

人工智能とロボット3

55

## CSS2013のプログラム(3日目)

会場						
時間	会場1 国際会議場	会場2 会議室	会場3 会議室	会場4 会議室	会場5 会議室	会場6 会議室
09:30~ 10:50	3A1 M&S(アコ通達4) 11	3B1 会議(アコボイント 会議室)1 22	3C1 会議(アコボイント 会議室)2 23	3D1 会議(アコボイント 会議室)3 24	3E1 会議(アコボイント 会議室)4 25	-
11:00~ 12:20	3A2 M&S(アコ通達4) 12	3B2 会議(アコボイント 会議室)1 26	3C2 会議(アコボイント 会議室)2 27	3D2 会議(アコボイント 会議室)3 28	3E2 会議(アコボイント 会議室)4 29	-
13:20~ 14:40	3A3 M&S(アコ通達4) 13	3B3 会議(アコボイント 会議室)1 30	3C3 会議(アコボイント 会議室)2 31	3D3 会議(アコボイント 会議室)3 32	3E3 会議(アコボイント 会議室)4 33	-
14:50~ 16:10	3A4 M&S (D&S)	3B4 会議(アコボイント 会議室)1 34	3C4 会議(アコボイント 会議室)2 35	3D4 会議(アコボイント 会議室)3 36	3E4 会議(アコボイント 会議室)4 37	-

10月3日(木)

2013/10/31

人工智能とロボット3

56

## CSS2013で発表した最新研究

- ◆ 3D1-1: Android端末におけるタッチ操作の特徴を用いた個人認証に向けたアプリケーションの開発
  - ◆ ◎藤田 奨、渡邊 裕司(名古屋市立大学)
- ◆ 3D1-2: スマートフォンの加速度センサを用いた歩行時の認証に関する一考察
  - ◆ ◎彭 龍、渡邊 裕司(名古屋市立大学)

2013/10/31

人工智能とロボット3

57

## 新アプリケーション

新アプリケーション	旧アプリケーション
Android OS	iOS
マルチタッチ	シングルタッチ
文章閲覧・画像操作・Webブラウジング	文章閲覧
スクリーン上のイベントの取得	テキスト上のイベントの取得

より多くの状況での操作記録を取得することが可能

2013/10/31

人工智能とロボット3

58

## アプリケーションの構成

- ◆ アンケート
  - ◆ 性別・年齢・使用年数
  - ◆ スマートフォンにおけるセキュリティについて
- ◆ 実験1
  - ◆ 画像操作
- ◆ 実験2
  - ◆ 文章閲覧
- ◆ 実験3
  - ◆ Webブラウジング



アプ実験3を押す直後

2013/10/31

人工智能とロボット3

59

## 取得

◆ 新アプリケーション

- ◆ eve  
EventTime=700841, time=1375431195366, x=333, y=65244, y2=233, size=85385, pointerId=1
- ◆ cou  
EventTime=7008181, time=1375431195385, pointerId=1
- ◆ id  
EventTime=7008441, time=1375431195385, pointerId=1
- ◆ (x, y)  
EventTime=7008181, time=1375431195385, pointerId=1
- ◆ poi  
EventTime=7008441, time=1375431195400, pointerId=1
- ◆ dou  
EventTime=7008181, time=1375431195400, pointerId=1
- ◆ pre  
EventTime=7008454, time=1375431195407, pointerId=1
- ◆ size  
EventTime=7008181, time=1375431195407, pointerId=1
- ◆ Eve  
EventTime=7008454, time=1375431195408, pointerId=1
- ◆ tim  
EventTime=7008181, time=1375431195408, pointerId=1
- ◆ tim  
EventTime=7008181, time=1375431195413, pointerId=1
- ◆ 旧アプリケーション
- ◆ イベント

2013/10/31 17:09:29

60

## 予備実験

- デバイス: SONY NW-Z1050
- スクリーンサイズ: 800×480 (4.3インチ)
- 被験者: 2人
- 実験手順:
  - アンケート
  - 基本操作(直線を描く等)
  - 文章を読む
  - Webブラウザを利用し課題を解く

2013/10/31

人工知能とロボット3

61

## 各実験でのピンチ操作の回数

### 追加機能のマルチタッチについて分析

実験	ピンチ操作	被験者A	被験者B
実験1	ピンチイン	17回	16回
	ピンチアウト	14回	16回
実験2	ピンチイン	5回	0回
	ピンチアウト	1回	0回
実験3	ピンチイン	5回	5回
	ピンチアウト	11回	5回

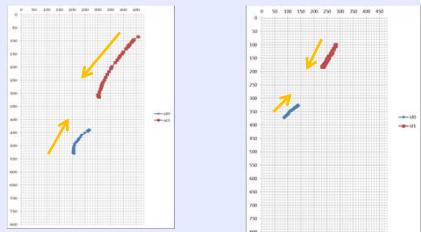
2013/10/31

人工知能とロボット3

62

## ピンチイン操作における特徴の例

### 実験1で得られたプロット



被験者A

被験者B

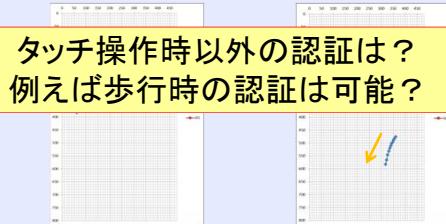
63

2013/10/31

人工知能とロボット3

## ピンチアウト操作における特徴の例

### 実験3で得られたプロット



被験者A

被験者B

64

2013/10/31

人工知能とロボット3

## 加速度センサを用いた既存認証研究

- Step 1 自作Androidアプリを使って、歩行・走行・階段昇降時の3軸加速度データを取得
- Step 2 加速度データから43個の特徴を抽出
- Step 3 分類アルゴリズム(決定木とニューラルネットワーク)を用いて認証・識別 → 90%以上の識別精度を達成

[Kwapisz 10] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Cell Phone-Based Biometric Identification," Proc. of the 4th IEEE International Conference on Biometrics: Theory Applications and Systems, pp.1-7, 2010.

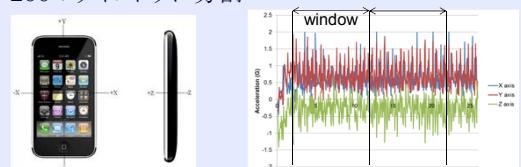
2013/10/31

人工知能とロボット3

65

## 加速度取得アプリ

- 3軸加速度センサ値を毎秒20データで記録するiOS用アプリを開発
- 時系列データに対してオーバーラップを許さないサイズ200のウインドウに分割



- 各ウインドウに含まれるデータから43個の特徴を抽出

2013/10/31

人工知能とロボット3

66

## 43個の特徴

- ◆ 平均値(3軸)  $\bar{x} = \sum_{i=1}^{200} x_i / 200$
- ◆ 標準偏差(3軸)  $\sqrt{\sum_{i=1}^{200} (x_i - \bar{x})^2 / 200}$
- ◆ 平均絶対偏差(3軸)  $\sum_{i=1}^{200} |x_i - \bar{x}| / 200$
- ◆ 平均合成加速度  $\sum_{i=1}^{200} \sqrt{x_i^2 + y_i^2 + z_i^2} / 200$
- ◆ ピーク間の時間(3軸)
- ◆ ビン分布(3軸×10個)

2013/10/31

人工知能とロボット3

67

## 実験

- ◆ 端末:iPod touch
- ◆ 被験者:8人
- ◆ 行動:歩行
- ◆ 方法:  
被験者はポケットにiPod touchを入れ、約50m  
距離の廊下に沿って5回往復(約7-8分)  
歩行が終了したら、iTunes経由で記録された  
各加速度データを取得

2013/10/31

人工知能とロボット3

68

## 歩行時の認証結果

被験者	決定木(J48)		ニューラルネットワーク(NN)	
	FAR (%)	FRR (%)	FAR (%)	FRR (%)
A	<b>0.4</b>	<b>0</b>	<b>0</b>	<b>0</b>
B	0.4	13.9	0.8	8.3
C	1.2	11.1	0.4	0
D	0.8	5.6	0.8	8.3
E	0.8	5.6	0.4	8.3
F	<b>0</b>	<b>2.8</b>	<b>0</b>	<b>0</b>
G	0.4	16.7	0	2.8
H	0.8	13.9	0	2.8
平均	0.6	8.7	<b>0.3</b>	<b>3.8</b>

2013/10/31

人工知能とロボット3

69

## 一部の特徴の結果

特徴	決定木		ニューラルネットワーク	
	平均 FAR (%)	平均 FRR (%)	平均 FAR (%)	平均 FRR (%)
全部	0.6	8.7	0.3	3.8
平均値	<b>0.3</b>	<b>4.9</b>	1.0	<b>2.1</b>
標準偏差	2.1	18.4	3.1	18.4
平均絶対偏差	2.6	15.6	1.0	24.3
平均合成加速度	1.3	84.0	0.4	85.8
ピーク間時間	1.5	91.7	1.3	93.8
ビン分布	2.3	19.5	1.1	8.0
平均値除き	2.1	14.9	<b>0.7</b>	4.9

2013/10/31

人工知能とロボット3

70

## 別のアルゴリズムの結果(43特徴)

分類アルゴリズム	平均 FAR (%)	平均 FRR (%)	識別(%)
RBF Network	0.1	3.5	99.2
IB1	0.3	1.4	98.4
Decorate	0.2	4.5	98.0
...	...	...	...
Neural Network (NN)	0.3	3.8	97.7
...	...	...	...
Decision Tree (J48)	0.6	8.7	94.4
...	...	...	...
Grading	0	100	7.6
Stacking	0	100	7.6
Zero R	0	100	7.6

2013/10/31

人工知能とロボット3

71

## 最後に… 再び

- ◆ スマートフォン情報セキュリティ3か条
  - ◆ OSを更新
  - ◆ ウイルス対策ソフトの利用を確認
  - ◆ アプリケーションの入手に注意
- ◆ スマートフォンプライバシーガイド
  - ◆ スマートフォンのサービス構造を知る
  - ◆ アプリの信頼性に関する情報を自ら入手し理解するように努める
  - ◆ 利用者情報の許諾画面等を確認する

2013/10/31

人工知能とロボット3

72

## 最後に… 配布資料の間の解答

- ◆ A : Android
- ◆ B : iOS
- ◆ C : URL
- ◆ D : Webサーバ
- ◆ E : インストール
- ◆ F : 遠隔操作
- ◆ G : インストール
- ◆ H : 水平展開型のサー  
ビス
- ◆ I : プライバシー
- ◆ J : サンドボック
- ◆ K : パスワード認証
- ◆ L : 身体的特徴
- ◆ M : 行動的特徴
- ◆ N : バイオメトリクス  
認証
- ◆ O : データマイニング
- ◆ P : 決定木学習
- ◆ Q : ニューラルネット  
ワーク

2013/10/31

人工知能とロボット3

73

## 参考サイト

- ◆ 平成24年7月27日掲載の政府広報オンライン、  
<http://www.gov-online.go.jp/useful/article/2012072.html>
- ◆ 総務省「スマートフォンを安心して利用するために実施されるべき方策」、[http://www.soumu.go.jp/menu\\_news/news/01ryutsu03\\_02000020.html](http://www.soumu.go.jp/menu_news/news/01ryutsu03_02000020.html)
- ◆ 総務省「国民のための情報セキュリティサイト」、[http://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security/index.htm](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm)
- ◆ Google Play、<https://play.google.com/store>
- ◆ コンピュータセキュリティシンポジウム2012、2013  
<http://www.iwsec.org/css/2012/>  
<http://www.iwsec.org/css/2013/>

2013/10/31

人工知能とロボット3

74