社員証型センサを用いた健康増進システムへのSTAMP/STPAの適用検討

小林良輔*　伊藤信行†　梶克彦††
内藤克浩††　水野忠則††　中條直也††

*愛知工業大学大学院
†三菱電機エンジニアリング
††愛知工業大学

目次

- 研究背景
- 健康増進システム
  - 社員証型センサを用いた運動量測定
  - オフィスでの歩行軌跡推定に基づく運動量推定
  - エルゴxウェアラブル心拍計を使った運動実験
  - システムの高信頼化
- 研究課題
- 研究目的
- 健康増進システムの構成要素
- STAMP/STPA
  - Step0 準備1 Loss,Hazard,Safety Constraintsの識別
  - Step0 準備2 CSの構築
  - Step1(UCAの抽出)
  - Step2(HCFの特定)
  - 対策
- 考察
- まとめ

研究背景

- 三菱電機エンジニアリングと共同研究
- 健康増進システムの開発

対象:運動にあまり
関心がないオフィスワーカー

特徴:エルゴメータと
社員証型センサを併用して
個々人に適した運動の提供

健康増進システムの提案

オフィスでの
運動量推定

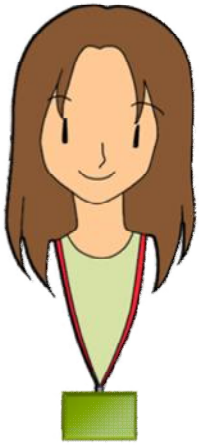
他システム

体重・血圧

運動量データ

運動量データ

時系列分析
（個人）



情報提供

スマホアプリによる
健康管理・情報提供

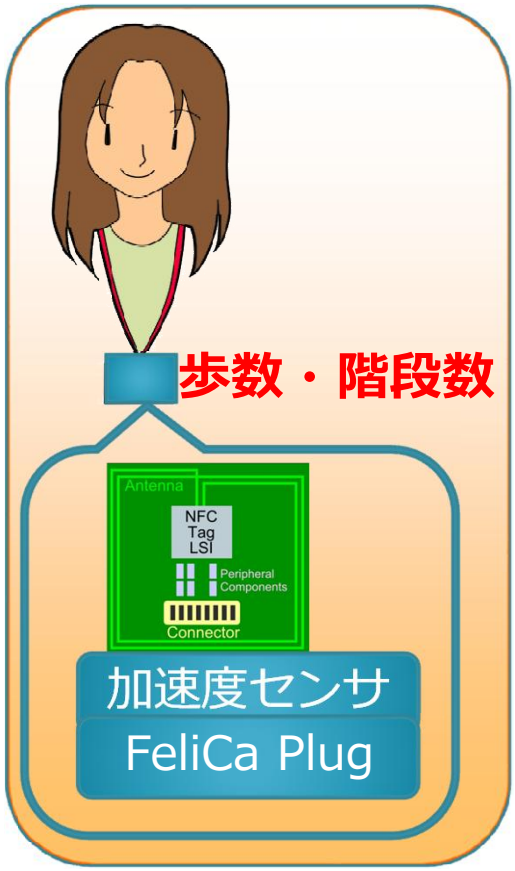
心肺能力
データ

目標心拍，運動強度の
測定（個人の特性）

社員証型センサ

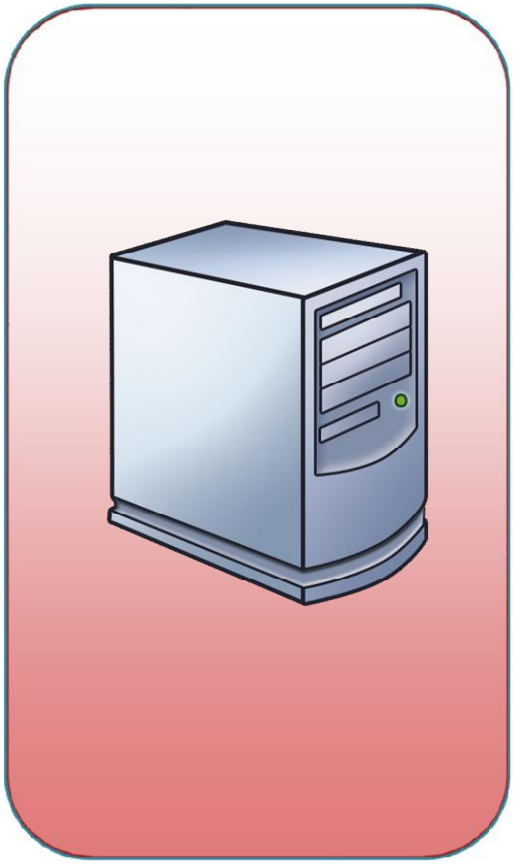
社員証型センサを用いた運動量測定ハードウェア

日常の運動量を測定したい！



社員証型センサによる運動量測定

RFIDリーダによる測定値収集

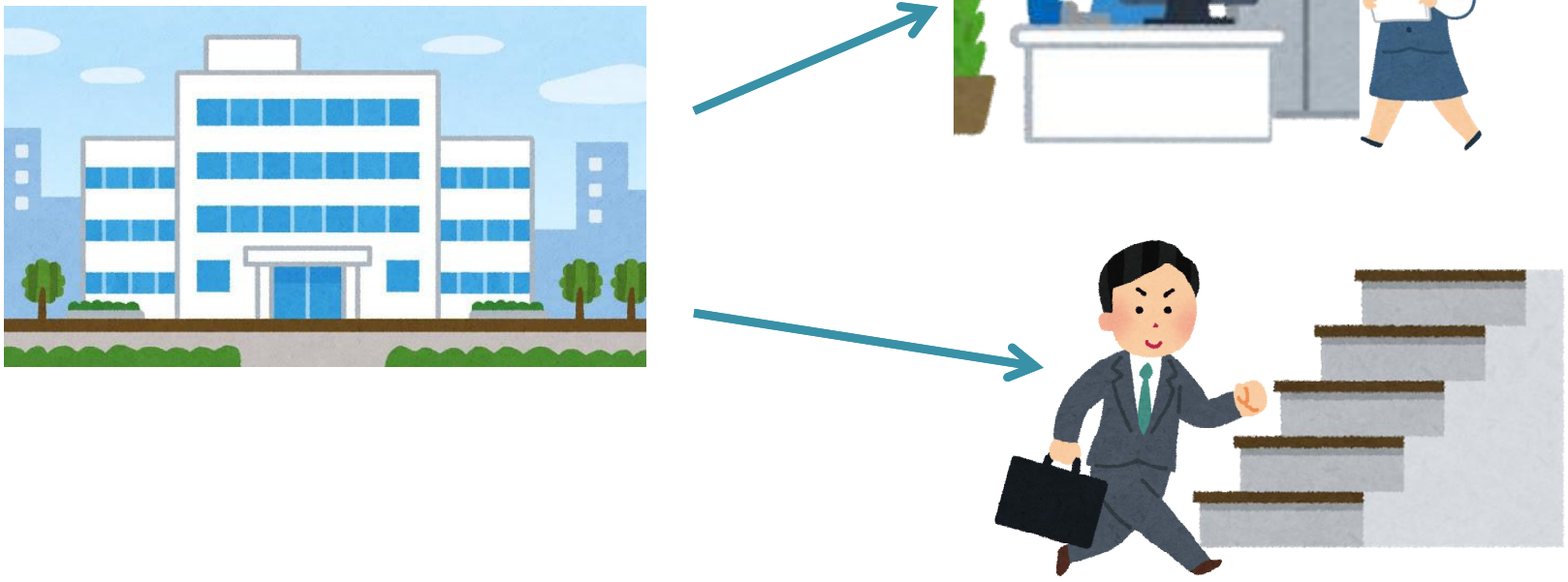


測定値管理

オフィスでの歩行軌跡推定に基づく運動量推定

オフィスでの運動量を知りたい！

- 社員証型センサで歩行軌跡を推定
- オフィスや階段の歩行での運動量推定

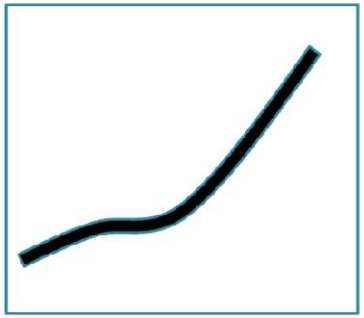


エルゴxウェアラブル心拍計を使った運動実験

日常の運動量から体力の向上を知りたい！

個人の特性を詳細に分析

心拍数

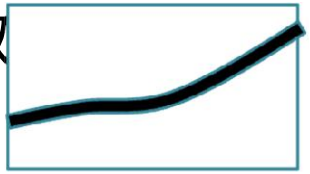


運動負荷

エルゴメータ

日常運動量測定

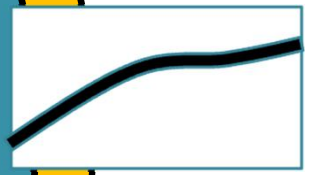
歩数



心拍数

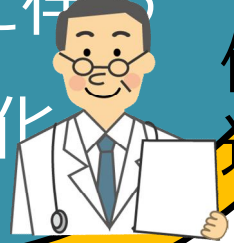
通勤・オフィスワーク

歩数



運動負荷

時間経過に伴う特性変化



健康状態の情報
運動方法の提案

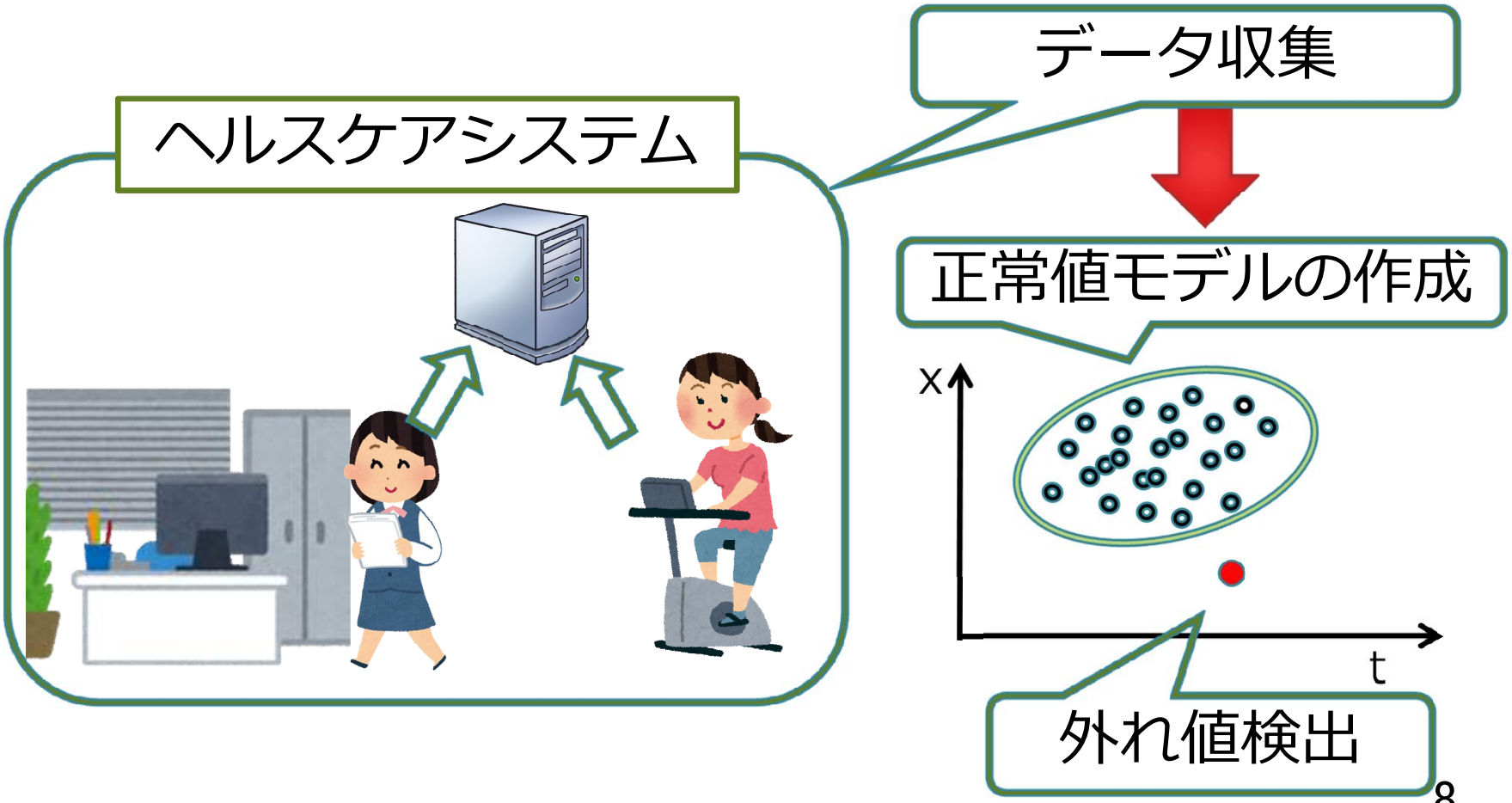
特性の変化
健康促進

システムの高信頼化

安全に利用できるか知りたい!

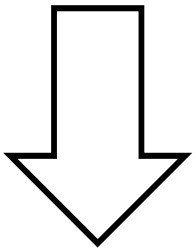
STAMP/
STPA

- データ学習による異常の検出
- 疲労や怪我を防止する安全性解析



健康増進システムの課題

オフィスワーカーが安全に利用できる
システムであることが求められる



- オフィスワーカーはシステムに
  関する専門知識がない一般の利用者
  - 社員証型センサが新しい機器

課題がないか分析が必要

課題の事例

運動中の心拍数を82と低く取得

不審に思ったトレーナーが
別の機器で心拍数を測定
160を計測

利用者による集団訴訟

重大な事故に
つながる恐れ

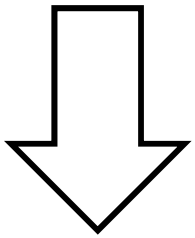
ウェアラブル心拍計

精度問題かセンサの故障かは定かではないが
デバイス周りの安全性分析は必要

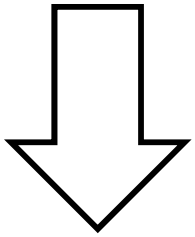
出典:http://www.gizmodo.jp/2016/01/_fitbit_classaction.html

研究目的

健康増進システムにSTAMP/STPAを適用



社員証や利用者に関するリスク分析



開発中の健康増進システムの安全性確保

健康増進システムの構成要素

社員証型センサ

利用者

エルゴメータ

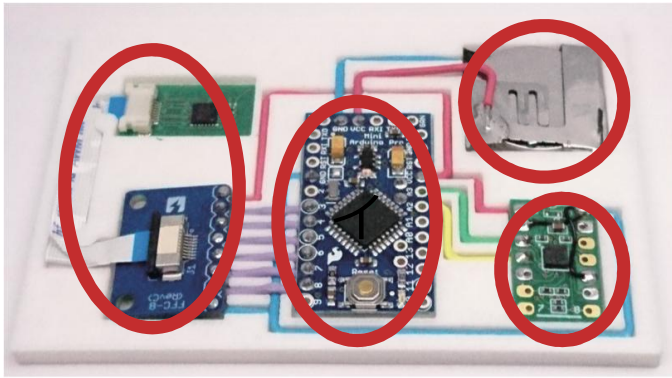
スマートフォン

サーバ

ゲート

社員証型センサ

プロトタイプ評価中
加速度センサの動作確認
無線通信も動作確認



前提

- Arduinoマイコン，加速度センサ FeliCa Plug，ボタン電池，気圧センサを搭載
- FeliCa Plugを用いて出退勤管理
- 社員証は首に下げている

役割

- 加速度センサ，気圧センサを用いて日常の運動量を測定，蓄積
- FeliCa Plugによりゲートのカードリーダと通信を行い，出退勤と同時に運動量を送信

利用者

前提

- 普段運動をしないオフィスワーカー
- 測定機器などシステムに関する
  専門知識はない
- 会社内で運動するタイミングがある

役割

- 体力測定の結果やスマートフォンの
  アプリケーションに従い運動

エルゴメータ

前提
- 一定周期で体力測定
- 会社で利用できる

役割
- 心肺運動負荷試験を行うことで利用者の体力がわかる
- 利用者に目標心拍，運動強度の表示をする

スマートフォン

役割

- サーバから運動量を受信
- アプリケーションにより
  受信した運動量から
  目標心拍，運動強度を設定

ゲート

前提

- RFIDリーダの搭載
- FeliCaによる近距離無線通信
- 社員証で出退勤の確認

役割

- 出退勤と同時に社員証から
  運動量データを回収
- 運動量データをサーバに送信

サーバ

役割

- ゲートから運動量データを受信
- 運動量データを管理
- 利用者のスマートフォンに運動量データを送信

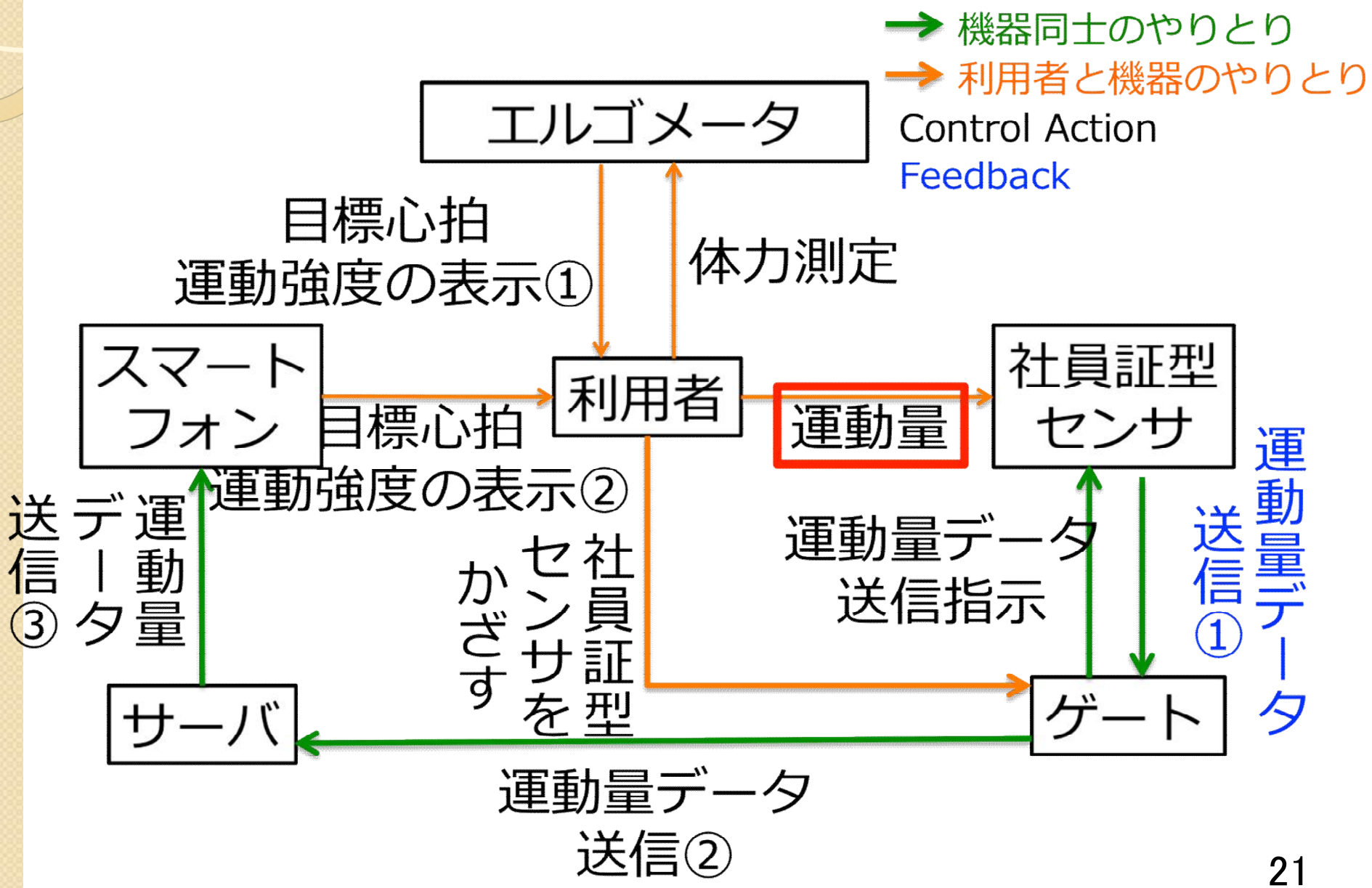
目次

- 研究背景
- 健康増進システム
  - 社員証型センサを用いた運動量測定
  - オフィスでの歩行軌跡推定に基づく運動量推定
  - エルゴxウェアラブル心拍計を使った運動実験
  - システムの高信頼化
- 研究課題
- 研究目的
- 健康増進システムの構成要素
- STAMP/STPA
  - Step0 準備1 Loss,Hazard,Safety Constraintsの識別
  - Step0 準備2 CSの構築
  - Step1(UCAの抽出)
  - Step2(HCFの特定)
  - 対策
- 考察
- まとめ

Step0 準備1 Accident,Hazard,Safety Constraintsの識別

System	Accident	Hazard	Safety Constraints
健康増進システム	怪我をする	過度な運動	運動量の上下限
	体力が衰える	負荷の少ない運動	ルール遵守の徹底
	健康増進しない	ルールを遵守しない体力測定	機器の自己診断
		機器の故障	目標心拍の上下限
		高い目標心拍	
		低い目標心拍	

Step0 準備2 CSの構築



Step1(UCAの抽出)

機器同士のUCA

機器と機器	Control Action	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	運動量データ送信②	運動量データが送信されない	不適切な運動量データが送信される	次の目標心拍を設定するまでに運動量データが送信されない	運動データが送信され続ける
2	運動量データ送信③	運動量データが送信されない	不適切な運動量データが送信される	次の目標心拍を設定するまでに運動量データが送信されない	運動データが送信され続ける
3	運動量データ送信指示	運動量データ送信指示がされない	不適切な運動量データ送信指示がされる	社員証型センサを離すまでに指示がされない	運動量データ送信指示がされ続ける

Step1(UCAの抽出)

利用者と機器のUCA

利用者と機器	Control Action	Not Providing	Providing causes hazard	Too early / too late , wrong order causes hazard	Stopping too soon / applying too long causes hazard
1	目標心拍，運動強度の表示①	目標心拍，運動強度が表示されない	不適切な目標心拍，運動強度が表示される	早い遅いタイミングで目標心拍，運動強度が表示される	目標心拍，運動強度が残り続ける
2	目標心拍，運動強度の表示②	目標心拍，運動強度が表示されない	不適切な目標心拍，運動強度が表示される	早い遅いタイミングで目標心拍，運動強度が表示される	目標心拍，運動強度が残り続ける
3	運動量	運動量がない	不適切な運動量が与えられる	運動量が遅く与えられる	運動量が途中で止まる
4	体力測定	体力測定がされない	不適切な体力測定が与えられる	別の日に体力測定を行う	途中で体力測定を終了する
5	社員証型センサをかざす	社員証型センサがかざされない	不適切に社員証型センサがかざされる	素早く社員証型センサがかざされる	社員証型センサをかざし続ける

Step1(UCAの抽出)

社員証型センサのUCA

利用者と機器	Control Action	Not Providing	Providing causes hazard	Too early / too late , wrong order causes hazard	Stopping too soon / applying too long causes hazard
1	運動量	運動量がない	不適切な運動量が与えられる	運動量が遅く与えられる	運動量が途中で止まる

Step2(HCFの特定)

Control Action	Not Providing	Providing causes hazard	Too early / too late , wrong order causes hazard	Stopping too soon / applying too long causes hazard
運動量	• 社員証型センサの充電が切れていたため運動量が取得できない • 加速度センサの故障により運動量が取得できない	• 落とした社員証型センサを届けてもらったときに別の利用者の運動量データを計測している • 加速度センサの故障により実際の運動量と違う運動量を計測する	• 実際の運動量と保存されている運動量の時間にズレが生じている	• 社員証型センサの充電が装着途中に切れるため運動量が途切れる

対策

UCA	対策	対象
• 加速度センサの故障により実際の運動量と違う運動量を計測する	• マイコンによるセンサの状態監視 • サーバに蓄積された統計データからの外れ値検出	• 社員証型センサ • サーバ

考察

- 利用者と機器のコントロールアクションを分けることで着目したい部分を明確化

- 社員証型センサのハザードとしては
  - 社員証型センサの充電がないため運動量が計測できない
  - 加速度センサが故障し運動量を計測できない
  - 加速度センサの故障による不適切な運動量の計測
  - 他人の運動量データを計測
  - 社員証型センサの充電が装着中に切れ運動量が途切れる

- 社外で運動をするオフィスワーカーもフォローする必要がある

社外で運動をする
オフィスワーカーのフォロー

- 本研究では普段運動をしない8割の
  オフィスワーカーのための健康増進システムの分析

- 残り2割の社外で運動をするオフィスワーカーも
  健康増進システムに組み込むことが必要
- 他のシステムとの連携

- 新たなリスク分析が必要

まとめ

- オフィスワーカーの健康増進システムを対象としてSTAMP/STPAの適用

- 利用者と機器のコントロールアクションを分けることで社員証型センサに関するシナリオを明確にできた

- 社員証型センサのシナリオについて対策を講じた

ご清聴ありがとうございました