Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

携帯電話によるソーシャルプラットフォームのための端末グループ管理方式

大畑 真生[†] 太田 賢[†] 土井 千章[†] 稲村 浩[†]
松浦 伸彦[‡] 峰野 博史[§] 水野 忠則[¶]

本稿では，対面コミュニケーションを支援するソーシャルアプリケーションのための，携帯電話端末を利用した対面グループ管理方式を提案する．本方式は，Bluetooth による端末認証とユーザ認証との組合せにより，その場所にいることの確認と本人性を検査し，その場の参加者による対面グループを形成可能とする．対面グループ管理機能を含む，OpenSocial ベースのソーシャルプラットフォームのプロトタイプと，ソーシャルアプリとしてパーティアプリを Android 端末に実装し，評価を行った．その結果，端末認証等を含むグループ形成時間は，ソーシャルアプリの Web ページダウンロード時間内に収まり，ユーザの使い勝手に影響しないことが確認された．また，電力測定の結果，多数の参加者を収容する際，管理者端末の電力消費増加が顕著となることが分かったため，対策として管理権限委譲方式も検討した．

A Method of Group Management for Mobile Social Platform

Maki OHATA[†] Ken OHTA[†] Chiaki DOI[†] Hiroshi INAMURA[†] Nobuhiko MATSUURA[‡] Hiroshi MINENO[§] and Tadanori MIZUNO[¶]

We propose a method of group management using cell phones for mobile social platform. This method can make the group for face-to-face social applications and verify the existence and the identity of participants by combination of terminal authentication using Bluetooth and user authentication. We built social platform and a party social application based on OpenSocail API. The time of the group formation including the verification of the participant is shorter than that of downloading web pages of the party social application, thus the impact of user response is negligible. Additionally, we propose a method of delegating manager's authority based on the result of power measurement, an increase in participants affects battery life of manager's cell phone.

1. はじめに

近年，Facebook や mixi 等のソーシャルネットワークサービス（SNS）において，ゲームやコミュニケーション，コラボレーションなど，多様なソーシャルアプリケーションが提供されており，SNS のアプリケーションプラットフォーム化が進展している[1]．これらのソーシャルアプリケーションは，携帯電話端末等を利用したモバイル環境から利用でき，いつでもどこでも相手の状況や関心に気づくことができたり，協調作業や共同でゲームを楽しんだりと，オンラインのコミュニケーションの支援がなされている．

一方，ソーシャルアプリケーションの利用シーンの広がりとして，携帯電話端末による対面コミュニケーション支援が考えられる．会議や懇親会において，参加者のプロフィール情報や，参加者の名簿，会議や懇親会に関する情報などを携帯電話に提示したり，その場で携帯電話同士によるファイル等の情報交換手段を提供するなどの支援が考えられる．従来，同じ興味を持った人同士に対し，ショートメッセージを交換する電子名札を利用したコミュニケーション促進の手法[2]や，参加者が保持するタグから取得される行動履歴を保存し，参加者間のコミュニケーション支援を実施する手法[3]など，様々な対面コミュニケーション支援の手法が提案されている[4][5][6]．本研究では，対面コミュニケーションを支援する様々なアプリ（対面ソーシャルアプリと呼ぶ）が共通的に必要とする機能を API として提供する，携帯ソーシャルプラットフォーム（携帯ソーシャル PF と記す）の構築を目的とする．

2. 携帯ソーシャル PF

本章では，既存のソーシャルアプリケーションプラットフォームの共通的機能を概観した後，多様な対面ソーシャルアプリを実現するために，携帯ソーシャル PF が備えるべき機能を述べる．

2.1 ソーシャルアプリケーションプラットフォームの共通機能

様々なサービスプロバイダがソーシャルアプリケーションプラットフォームを提供しており，プラットフォームが備える機能はそれぞれ異なるものの，その多くがユーザのプロフィール情報や友人関係，行動情報の更新，取得機能を持つ．OpenSocial Foundation[7] はソーシャルアプリケーションプラットフォームの共通的仕様を策定しており，その仕様では，以下のように API が規定されている（表 1）．

† 株式会社 NTT ドコモ 先進技術研究所，NTT DOCOMO, Inc. Research Laboratories.
‡ 静岡大学大学院 情報学研究科，Graduate School of Informatics, Shizuoka University
§ 静岡大学 情報学部，Department of Computer Science, Shizuoka University
¶ 静岡大学大学院 創造科学技術研究部，Graduate School of Science and Technology, Shizuoka University

Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

表 1 OpenSocail API

API 種別	説明
People API	個人や友人関係についての情報取得 API メソッド例：newFetchPersonRequest 引数：ユーザ ID，パラメータ，返り値：友人情報
Activities API	個人の行動を投稿，最新情報を参照する機能 メソッド例： newActivity 引数：パラメータ，返り値：新規行動情報
Persistence API	サーバ不要のステートフルなアプリケーションを実現する，key と value によるシンプルなデータストア API メソッド例：newUpdatePersonAppDataRequest 引数：ユーザ ID，key，value，返り値：(データ更新)

2.2 携帯ソーシャル PF の基本機能

携帯ソーシャル PF は, 既存のソーシャルアプリケーションプラットフォームに対して，対面コミュニケーション支援のための拡張 API を追加するものである．拡張 API の具体化のため，パーティにおける対面コミュニケーションを支援するユースケースを例に説明する．対面コミュニケーション支援システムを利用して，パーティの様々な情報の管理を行うユーザを管理者と定義する．管理者がパーティにおいて，参加状況を確認したい場合，管理者は，参加者が受付に来場した際に参加状況を随時確認する．パーティ会場では，その参加者に対してパーティの関連情報等を提供し，共有した情報を参加者端末とネットワーク間, 参加者端末間で同期するシーンが想定される．このような参加者のグループに対して，同一の場所にて対面及びオンラインでコミュニケーションを行う，端末を持った参加者によって構成された集合を“対面グループ”と定義する．

表 2 対面ソーシャルアプリ分類

分類	アプリ例
コミュニケーション	チャット[8] 名刺交換アプリ[13]
協調作業	資料やコメントの共有[5] 投票[9]
ゲーム	すれ違い通信ゲーム[10]
マッチング	興味を共有するユーザ同士のマッチング[2] 行動履歴による活動振り返り支援[3]

表 2 では例として挙げたパーティアプリを含めた対面ソーシャルアプリを分類している．分類結果から，携帯ソーシャル PF の基本機能として，以下の機能が挙げられる．

1) 対面グループを管理する機能
2) 対面グループに属する参加者に情報の共有や発信を行う機能
3) 参加者の行動履歴情報を保存する機能

上記 3 つの機能は，汎用性があり，表 2 に分類した対面ソーシャルアプリのそれぞれに対した潜在的適用可能性が見て取れる．

本稿では，対面グループを形成する際に必要となる 1)の対面グループ管理方式を提案する．既存の SNS はオンライン上でグループを形成し，参加者情報を登録することが可能であるが，本稿では，SNS によりオンライン上で形成されるグループを，対面グループ形成に拡張する方式提案を行う．

3. セキュリティ分析による要件導出

本章では，対面グループ管理機能における要件を導出する．まず要件導出のため，参加者の分類を行う．対面グループへの参加権限の有/無及び，対面グループに属す/属さない，の 2 軸で分類している．例えば，なりすましによる攻撃を考える場合，前者は本人性の虚偽に相当し，後者は場所の虚偽に対応する．

対面グループ管理機能において参加者は，以下の 4 つに分類される．

I. 参加権限有かつ対面グループに属す
II. 参加権限有かつ対面グループに属さない
III. 参加権限無かつ対面グループに属す
IV. 参加権限無かつ対面グループに属さない

各 I からIVの攻撃パターンにおいて，Microsoft の脅威分析手法[11]を用いてセキュリティ分析を実施した．まず，対面グループ管理機能は，参加者の参加状況を管理することを目的としており，参加状況が記載されたリスト（参加者リスト）及びリストから閲覧できる参加者のプロフィール情報（名前，所属，年齢等）が重要な情報となる．この重要情報を保護資産として，システムのデータフローを作成した図が図 1 となる．また，脅威分析を実施する上での前提条件は以下の通りである．

- サーバ：信頼する
- 端末：信頼する（ただし，3rd パーティ製の一般アプリは端末内に存在する.）
- 管理者：信頼する
- 参加者：信頼しない

このデータフロー図から，攻撃経路となりうる，エントリポイントを抽出する．エントリポイントとしては，信頼できない参加者が端末内の一般アプリを利用してサーバへアクセスする経路（①），対面グループ管理のアプリケーションへの経路（②），OS への経路（③）の 3 点がエントリポイントとして存在する．端末は信頼できるた

Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

め，②，③は対象外とする．したがって，①のエントリポイントに関して，Microsoft の脅威分析手法である STRIDE 分析を行う．STRIDE 分析では， 6 つに分類した脅威を用いて分析し，セキュリティ課題を検証する手法である．実際に STRIDE 分析を実施した結果を表 3 に示す．

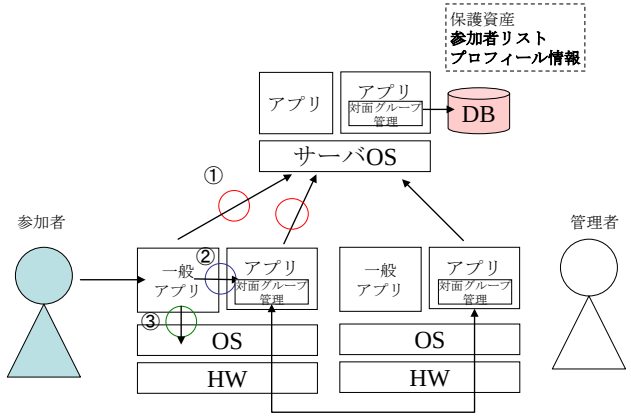

図 1 データフロー図

表 3 セキュリティ分析

分析要素	脅威	対策
なりすまし	他者へなりすまし（Ⅲ）	対面グループの場所に参加者本人が属していることの確認が必要（要件 1, 2）
改竄	履歴の改竄（Ⅱ，Ⅲ，Ⅳ）	既存 Web サービスと同様の脅威であり，不正侵入，改竄検知同様の対策を実施
否認	出欠の否認（Ⅱ）	本人認証による本人性担保が必要であり,SNS ログインによる本人性確保による対策を実施
情報漏洩	対面グループに限定した情報の漏洩， 参加 URL 等の情報漏洩（Ⅲ，Ⅳ）	会議参加中に参加者のみ情報共有できる機能が必要（要件 3）， 端末からの情報漏洩は既存端末の脅威であり，脆弱性，マルウェア対策を実施
DoS	SNS 利用妨害 偽情報によるフィッシング等（Ⅱ，Ⅲ，Ⅳ）	既存 SNS，ブラウザの脅威であり,サーバでの DoS 対策モジュールの追加, ブラウザ機能によるフィッシング防止による対策を実施
特権昇格	管理者権限の取得（Ⅱ，Ⅲ，Ⅳ）	既存サーバにおける脅威であり，ユーザの権限管理による対策を実施

表 3 の分析結果から，対面グループ管理機能における要件としては以下の 3 点が導出された．

要件 1．参加者が対面グループの場所に属することが確認できること．
要件 2．参加者が参加権限のある参加者本人であることの確認ができること．
要件 3．会議参加中に参加者のみ情報共有できる機能が存在すること．

また，使い勝手の観点から，ユーザがサービスを利用開始前に，要件 1, 2 の検証が完了している必要があるため，性能要件として以下の要件が存在する．

要件 4．ユーザがサーバへアクセスし，サーバ上のアプリケーション利用を開始するまでに，要件 1 及び 2 の確認処理が完了していること．

なお，既存 Web サービスやサーバに対する脅威関しては，対面グループ管理機能特有の脅威ではないため，信頼できるサーバを利用するなど，既存対策の範囲で対応する．

4. 関連技術

本章では，前節で抽出された要件を元に，関連技術比較を行う．

4.1 対面グループ管理における課題

対面グループ管理における課題は，対面グループに参加する参加者 A と対面グループの管理者の端末 B が同じ場所にいることをシステムに検知する手段を与えることである．また，3 章で導出した要件 1 から 4 を満たす必要がある．

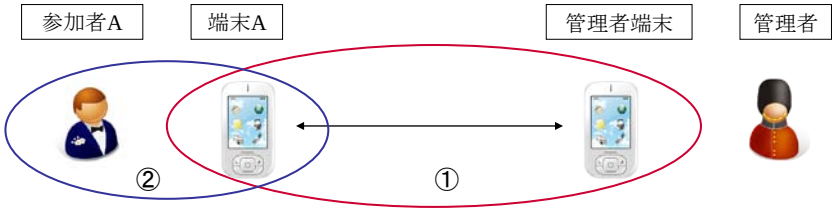

図 2 システムの検証範囲

要件 1, 2 において，参加者が管理者と同じ場に参加していることをシステムが検証する範囲としては，図 2 の①，②の部分が該当し，①の参加者端末と管理者端末が同じ場所に存在するか，②の参加者 A とその端末 A との関連付けの検証が必要となる．2 章で抽出された要件に照らし合わせると，①は要件 1 に該当し，②は要件 2 に該当する．また，3 章の前提条件から管理者は信頼することとし，管理者端末と管理者の間の関連付けは成立しているものとする．したがって，管理者端末と管理者間の認証

Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

は省略可能であり，①及び②がシステムによって検証できれば，参加者 A と管理者間の関連付けが実施できるため，同じ対面グループの場所にいるとみなすことが可能となる．

4.2 各要件における関連技術比較

次に，各要件に対して，関連技術比較を実施した結果を表 4 に示す．まず，要件 1 及び 2 を検証する既存技術に焦点を当て，比較を行った．同じ場所に端末が存在していることを確認する既存技術として，加速度センサをトリガに，GPS の位置情報と時間を利用して場所を特定し検証している名刺交換アプリの Bump アプリ[13]，耐タンパ性を持つ FeliCa を接触させることによる入退室管理技術[14]を挙げている．また，端末と本人との関連付けを実施する技術として，SMS の受信や生体認証など複数の認証技術を組み合わせて本人確認を実施する二要素認証[15]がある．

表 4 関連技術比較

	提案方式	Bump	FeliCa 入退室管理	二要素認証
要件 1（場所確認）	○	○	○	×
要件 2（本人確認）	○	×	×	○
要件 3（アクセス制限）	○	○	○	-
要件 4（性能要件）	○	-	-	-

比較した結果を表 4 に示す. Bump では, 位置情報を元に場所の検証はしているが，本人が端末を利用する前提であり，交換される名刺情報やプロフィール情報は，端末に設定されている情報が元となる．したがって，交換する情報を容易に変更可能であり，本人の情報であることを確認する手段が存在しない．FeliCa による入退室管理においても，FeliCa による接触動作によるその場所に存在することを確認することが目的であり，本人との関連付けを行うための認証方法が別途必要である．したがって，いずれも図 2 における①（すなわち要件 1）の端末がその場に存在していることは確認できるが，図 2 における②（すなわち要件 2）の端末と本人との関連付けを検証する手段が提供されていない．また，参加者と端末を関連付ける手段として二要素認証が存在するが，図 2 における②（要件 2）の参加者と端末の関連付けは実施できているが，図 2 における①（要件 1）のその場に端末が存在することを検証する手段は提供されていない．本稿では，要件 1, 2 に加え，要件 3, 4 を満たす端末グループ管理方式を提案する．

5. 提案方式

本章では， 2 章で抽出された要件 1 から 4 を全て満たす対面グループ管理方式を提案する．提案方式は，図 2 における参加者 A と管理者間の認証を，端末の Bluetooth 通信による端末認証とユーザ認証を利用して実現している．

5.1 提案方式における入退室時処理シーケンス

提案方式における入室時のシーケンスを図 3，退室時のシーケンスを図 4 に示す．入室時の管理者端末と参加者端末との間の認証手段として，QR コードを利用した場合（図 3 左）と，FeliCa を利用した場合（図 3 右）を示す．なお，以降，スマートフォンを含む多くの端末で利用可能である QR コードによる方式を元に説明を行う．

退室時は，参加者が自らサーバに退室を申告する場合（図 4 左）と，管理者端末と参加者端末の間で，Bluetooth 通信による定期的な在席判定を行う場合（図 4 右）を挙げている．

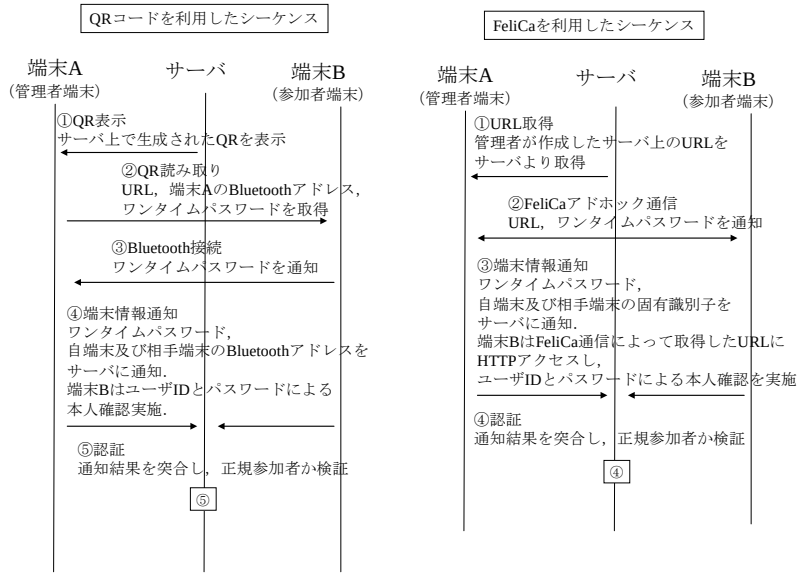

図 3 提案方式における入室時シーケンス

Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

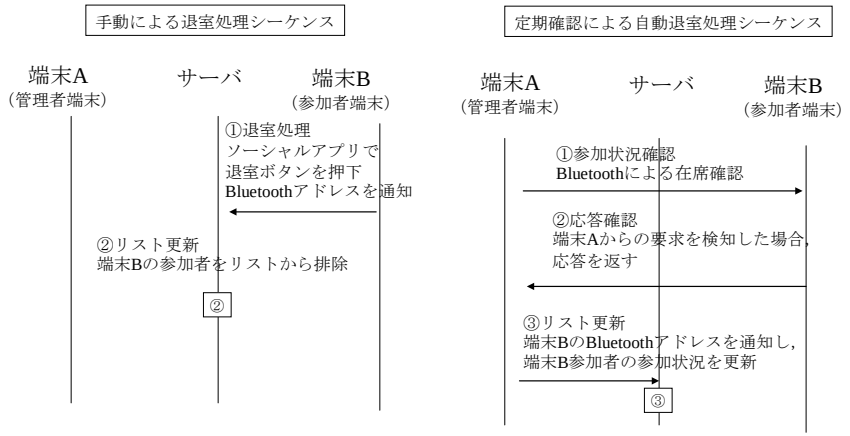

図 4 退室処理シーケンス

5.2 要件から見た提案方式の妥当性

本節では，各要件に対する QR コードを利用した提案方式の具体的な処理内容を示す．まず，要件 1 の対策を示す．図 3 左に示した処理シーケンスの中で，要件 1 の参加者が管理者と同じ場所にいることの確認手段として，Bluetooth による端末認証を実施している．手順②と並行して行う手順③の中で，ペアリング済みの管理者端末 A と参加者端末 B の間で Bluetooth 接続を行い，管理者端末に表示されている QR コードに記載されている一時的な乱数情報を Bluetooth 通信にて参加者端末 B から管理者端末 A に送信している．(ペアリングが未実施な場合は，管理者端末と参加者端末の間でペアリングを行う必要があるが，Bluetooth ver.2.1 よりペアリングの簡略化が可能となったため，Bluetooth ver2.1 以降に対応した端末であれば，利便性に影響を与えるものではない.) この乱数情報はワンタイムパスワードとしての役割を担っており，管理者端末 A は，参加者端末 B から受信したワンタイムパスワードが QR コードにて表示していた情報と同一か比較を行い，同じ場所に端末が存在していることを確認している．したがって，要件 1 を満たしている．なお，提案方式では，Bluetooth アドレスの漏洩防止のため，QR コードに埋め込まれた管理者端末の Bluetooth アドレスを直接指定して接続を行う．すなわち，管理者端末の Bluetooth アドレスを外部からスキャン可能としておく必要はない．

要件 2 に該当する，参加者と端末との関連付けに関しては，手順④において，Bluetooth のアドレス情報を送信すると共に，ユーザ ID とパスワードによる本人認証を行っており，要件 2 を満たしている．また，本人確認手段としては，生年月日やパスワード等による本人確認を実施する手段も利用可能である．

ここで，要件 1, 2 が独立して満たされてもシステムとしては意味をなさない．つまり，要件 1 及び要件 2 が同時に満たされて初めて検証が可能となるため，提案方式では，手順④の中でワンタイムパスワードをサーバ側にも送信し，管理者端末と参加者端末間，参加者端末と参加者間との関連付けを行っている．したがって，サーバ，参加者端末，管理者端末の 3 者間認証を利用することで，参加者から管理者端末までの関連付けを実施し，要件 1 及び 2 を同時に満たしている．また一時的な乱数情報であるワンタイムパスワードは，参加者端末 B と Bluetooth 接続を行った際に，QR コードを更新した際に，ワンタイムパスワードも変更することで，攻撃者の攻撃可能時間を制限している．

要件 3 に関して，既存のデータ保護技術として，データ暗号化による保護法[12]が存在するが，信頼できないサーバを前提とした技術である．本稿では信頼できるサーバを利用するため，サーバ上で各データに対してユーザ権限を設定し，ユーザ個別にアクセス制御を実施することで，サーバ上のデータを適切に制御する．

性能要件である要件 4 に関しては，プロトタイプ実装により評価を実施する．

また，退室処理に関しては，前述の通り，参加者が手動で退室を行う場合と，入室時と同じく，管理者端末と参加者端末間で Bluetooth 接続を行い，Bluetooth 接続可否によって，在席判定を実施している．

5.3 提案方式におけるシステム構成

図 5 に提案方式のシステム構成図を示す，対面グループ管理方式における端末側の機能としては，既存のブラウザ機能に加えて，対面グループ管理ミドルウェアが存在する．このミドルウェアの機能は，端末の位置情報等の端末状態をブラウザに通知する端末情報取得機能，端末の Bluetooth 情報を通知する状態通知機能，管理者端末と参加者端末の関連付けを管理するメンバ管理機能，管理者端末と参加者端末間の認証を実施する認証機能と，管理者端末に表示されている QR コードを読み取る QR 読取機能で構成されている．

対面グループ管理方式においてサーバは，既存 SNS の機能に加えて，携帯ソーシャル PF の独自機能として，参加者リスト及びそのリストや情報へのアクセス制御を実施する対面グループ管理機能，管理者端末と参加者端末間の認証機能，端末の Bluetooth アドレスの情報の管理機能や管理者端末に表示させる QR コードの生成機能等を備える端末連携機能を備えている．

携帯ソーシャル PF が提供している API は，OpenSocial で規定されている外部サーバと通信を行う API に準拠した呼び出し方法をとるように設計しており， OpenSocial 対応の SNS におけるソーシャルアプリで利用可能である．携帯ソーシャル PF の API を表 5 に示す．

Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

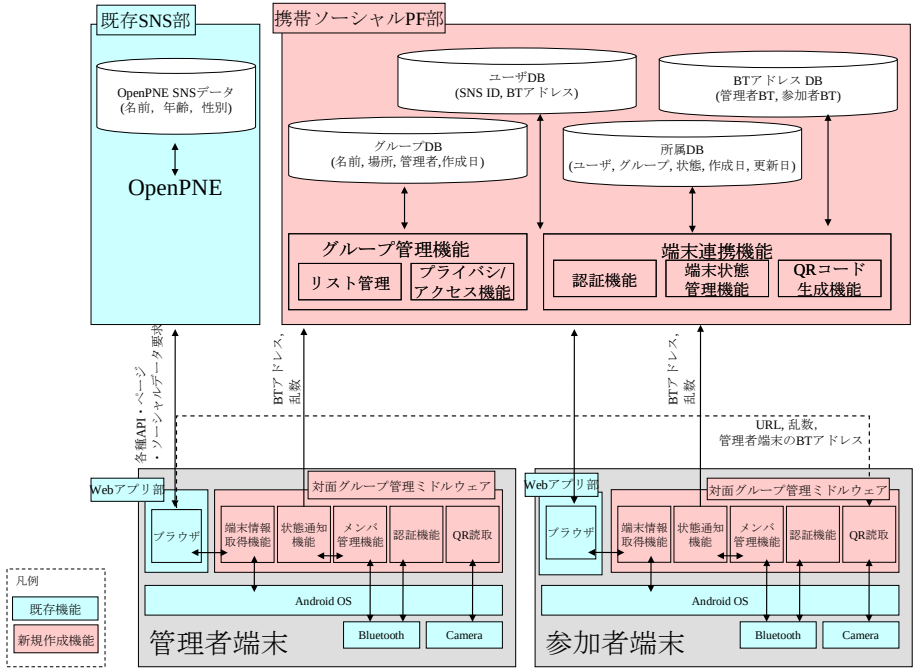

図 5 提案方式のシステム構成図

表 5 携帯ソーシャル PF 提供 API

API 種別	説明
対面グループ API	形成されている対面グループ名取得 API メソッド：getGroup 引数：無し，返り値：対面グループ名
所属対面グループ API	現在所属している対面グループ名取得 API メソッド getJoinGroup 引数：ユーザ ID，返り値：対面グループ名
所属メンバリスト API	対面グループに所属しているメンバ取得 API メソッド getJoinMember 引数：対面グループ名，返り値：ユーザ ID
ユーザ情報 API （管理者用 API）	SNS のユーザ ID 情報取得 API メソッド getUserInfo 引数：ユーザ ID，返り値：Bluetooth アドレス情報

6. 実装及び評価

提案した対面グループ管理方式を含むソーシャルサービスプロトタイプシステムを実装した．端末には OS に Android を利用した Xperia を用いた．Xperia を管理者端末及び参加者端末とし，オープンソースの SNS である OpenPNE[16]を Windows XP のサーバ上に構築した. システム構成は, 図 5 の通りである. 図 6 にプロトタイプの Android アプリケーション起動時の画面，実装したパーティアプリの利用画面を示す．実装したパーティアプリは管理者及び参加者それぞれ同一のアプリケーションとし，起動時に管理者または参加者の役割を選択する．このパーティアプリでは，管理者が作成した QR コードを参加者が読み取ると，自動的に認証処理を行い，クラウド上に生成される参加者リストに追加され，現在の参加者の参加状況（入退室時間）や，プロフィール情報が許可された参加メンバから閲覧可能となる．作成したアプリのメモリの消費量は，起動時は 3.8MB，アプリ利用中は 10 から 15MB であった．本ソーシャルアプリはブラウザ機能にて実現しており，既存ブラウザのメモリ消費と同等となっている．

表 6 実装詳細

	スペック
端末 （Xperia SO-01B）	OS：Android 1.6 RAM：384MB，ROM：1GB，プロセッサ：QSD8250 1GHz WLAN：IEEE802, 11b/g 準拠 Bluetooth：Bluetooth ver.2.0＋EDR
サーバ	OS：Windows XP 64bit RAM：11.9GB プロセッサ：Intel®Xeon®CPU E5530 2.40GHz SNS：OpenPNE ver3.4.6.2

図 6 プロトタイプにおける Android アプリケーション利用画面

Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

6.1 認証処理時間に関する評価

性能要件である要件 4 を満たすには，参加者のソーシャルアプリ利用に先立つ管理者端末と参加者端末の認証に要する時間の評価が必要である．端末認証等を含む対面グループ形成時間とソーシャルアプリの Web ページダウンロード時間を評価し，ユーザの使い勝手への影響を議論する．

管理者端末と参加者端末の認証とソーシャルアプリの Web ページダウンロードの時間的な関係を図 7 のシーケンスにて示す．参加者がページをダウンロードするのにかかる時間 A と，参加者端末の管理者端末への接続開始から管理者端末の Bluetooth アドレスをアップロードし，完了するまでの時間 B を比較する．なお，時間 B において参加者端末がページロード時に取得するサイズは 370.8 KB である．時間 B が時間 A より早く終了した場合，提案手法が要求する認証処理のオーバヘッド時間は隠蔽される．

実測したそれぞれの所要時間を図 8 に示す．参加者・管理者ともにサーバまでの接続性には WiFi または 3G のいずれかを用いるものとして，それぞれの組み合わせにて図に示した．その結果，もっとも認証時間が長い組み合わせである，参加者が WiFi を利用し，管理者が 3G 網（HSDPA）を利用している場合においても，参加者がソーシャルアプリのページをダウンロードするまでにかかる時間より認証処理時間は 2 秒程度早く終了することが確認され，要件 4 を満たしていることが確認された．すなわち，端末認証等を含むグループ形成時間はソーシャルアプリの Web ページダウンロード時間内に収まり，ユーザの使い勝手に影響しない．

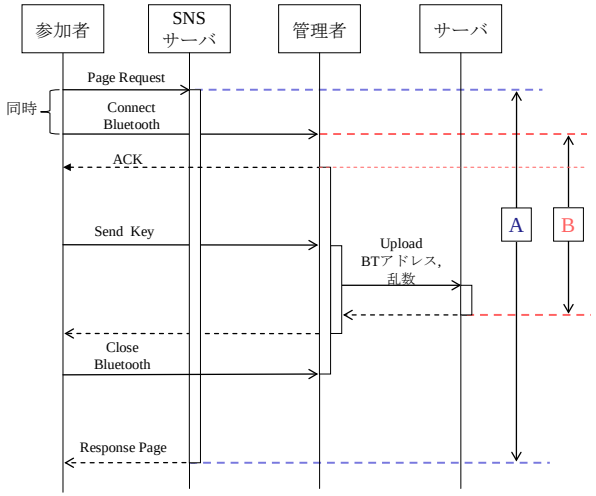

図 7 認証処理シーケンス

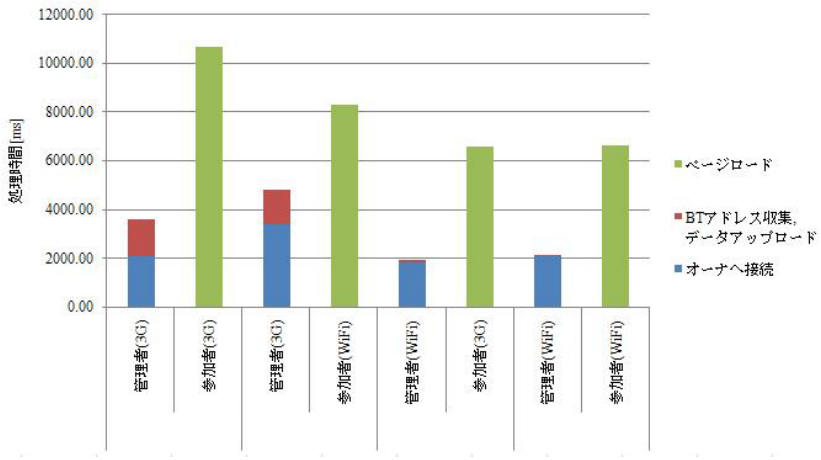

図 8 認証処理時間測定

6.2 消費電力の考察と追加要件

本節では，提案方式の実装における消費電力について考察を行う．参加者が増加すると，認証処理や在席判定に起因する Bluetooth，ネットワーク通信，処理負荷の増加によるための管理者端末の電力消費の増大が見られた．この管理者端末の電力消費増大を解決するためにこれらの処理の負荷軽減策を議論する．

提案方式では，退室時の在席判定として，Bluetooth 接続の接続可否のみによって判定している．したがって，障害物の有無等により，在席判定の誤差は大きくなる．より詳細な在席判定を行う場合には，Bluetooth の RSSI 値を利用し，距離制限による在席判定[17]や，周囲の Bluetooth デバイス状態に応じて，ユーザの行動を推定する手法[18]のような機能強化が考えられる．ここで， Bluetooth 接続試行頻度を高くして，参加者端末の状況把握を高頻度で行うことにより，より信頼性の高い参加者リストが作成できる．しかし，これら精度向上策において Bluetooth 接続回数増加による更なる消費電力増大の問題が懸念される．

この問題の検証のため，本提案方式における Bluetooth 接続の一回あたりの消費電力を測定したところ，図 9 に示す通り，400mA を 100ms の間消費する程度であり，端末のバッテリ容量（Xperia では 1500mAh）と比較すれば非常に小さい．すなわち，一回の接続あたりに消費する 0.164mAh は，理想的な環境下であればバッテリ容量全体の 0.011%に相当する．ただし実際には，環境やバッテリの劣化状態によってバッテリ容量比は変化する．管理者端末における接続試行回数は参加者数と共に増加する．条件として参加者 20 人，会議時間 2 時間，Bluetooth の定期的参加状況の確認間隔 3 分 の場合， 管理者 1 人に対して参加者 20 人を割り当てると，管理者端末におけるバッテ

Vol.2010-MBL-56 No.17
Vol.2010-ITS-43 No.17
2010/11/12

リ容量に対して 8.36%程度の負担となり，対策が必要である．これを受けて以下の追加要件を定義する．

要件 5．参加者増加に伴う管理者端末の電力負荷軽減

本稿では，要件 5 のための方式案として，管理権限委任による管理負荷分散の仕組みを提案する．信頼できるサーバにて管理者権限の委任条件を設定し，管理者権限を委任された参加者も管理者と同等の権限，すなわち参加者の入室及び退室処理を実行可能とする．

管理権限の委任による効果を上記条件と同じ条件にて机上検討する．管理者を 2 人割り当てると管理者端末への影響は 3.96%となり，管理者を 5 人割り当てると，管理者端末への影響は 1.32%であり，電力負荷は小さい．したがって，管理者端末の負荷の低減の効果が期待できる．しかし，管理者端末が増加した場合，管理者 1 人の場合には存在しなかったサーバへの同時接続が起こる可能性があるため，サーバ側の対策も必要と考えられる．

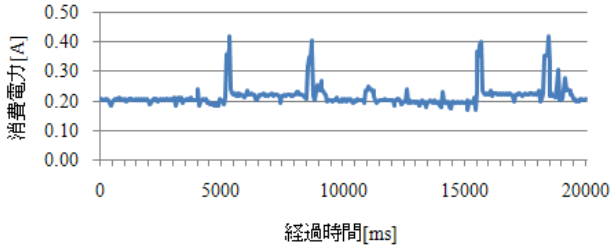

図 9 消費電力測定結果

7. おわりに

本稿では，携帯ソーシャルプラットフォームの基本機能である，対面グループ管理機能に着目し，セキュリティ分析から導出された要件を満たす対面グループ管理方式を提案した．本方式は，Bluetooth による端末認証とユーザ認証との組合せにより，その場所にいることの確認と本人性を検査し，その場の参加者による対面グループを形成可能とする．OpenSocial ベースのソーシャルプラットフォームのプロトタイプと，ソーシャルアプリとしてパーティ支援アプリを Android 端末に実装し，評価を行った．性能評価の結果，認証に要する時間は参加者がアプリケーションを利用するまでに要する時間より短く，ユーザの使い勝手を損なわない方式であることも示された．しかし，参加者が増加した場合，管理者へのバッテリ消費増大の問題が存在するため，追加要件を満たす方式が必要となった．本稿で提案した権限委任による負荷軽減方式を元に，詳細検討及び評価を継続していきたい．また，FeliCa を利用した対面グループ方式の実装や，端末が圏外状態であってもグループ形成を可能とする対面グループ管理方式についても今後の課題である．

参考文献

[1] “日米中ソーシャルアプリビジネス調査報告書 2010,” 2010 年 6 月 22 日．
[2] R. Borovoy, F. Martin, S. Vemuri, M. Resnick, B. Silverman, and C. Hancock, “Meme tags and community mirrors: Moving from conferences to collaboration,” *In Proceedings of the ACM 1998 Conference on Computer Supported Cooperative Work*, p. 159, 1998.
[3] 沼晃介，平田敏之，濱崎雅弘，大向一輝，市瀬龍太郎，武田英明, “学術会議における体験共有のための行動履歴に基づく Weblog システム,” 情報処理学会論文誌, Vol.48, No.1, 2007 年.
[4] A. K. Dey, D. Salber, G. D. Abowd, M. Futakawa, "The Conference Assistant: Combining Context-Awareness with Wearable Computing," Third International Symposium on Wearable Computers (ISWC'99), pp. 21, 1999
[5] 角康之，保呂毅，三木可奈子，西田豊明, “体験共有コミュニケーションを促すガイドシステム,” 人工知能学会全国大会（第 19 回）論文集, 2A3-06, 2005 年.
[6] 角康之，間瀬健二, “エージェントサロン : パーソナルエージェント同士のおしゃべりを利用した出会いと対話の促進,” 電子情報通信学会論文誌, Vol. J84-D-I, No. 8, pp. 1231-1243, 2001 年 8 月.
[7] OpenSocail, http://code.google.com/intl/ja/apis/opensocial/
[8] 吉野孝，松原繁夫，喜多千草，石田亨，“多言語コミュニケーションツールの異文化間対面協調作業への適用,” 人工知能学会全国大会（第 20 回），2006 年 6 月.
[9] R. Want, B. N. Schilit, N. I. Adams, R. Gold, K. Petersen, D. Goldberg, J. R. Ellis, and M. Weiser, “The ParcTab Ubiquitous Computing Experiment,” Xerox Parc, Palo Alto, 1995.
[10] TRAVATAR, http://itunes.apple.com/jp/app/travatar/id337488904?mt=8
[11] F. Swiderski, “Window Snyder: Threat Modeling,” Microsoft Press, Redmond, USA, June 2004.
[12] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, D. Starin, “Persona: An Online Social Network with User Defined Privacy,” ACM SIGCOMM 2009.
[13] Bump, http://jp.androlib.com/android.application.com-bumptech-bumpga-zDFt.aspx
[14] カイスマート，http://www.docomo.biz/html/service/kaismart/
[15] F. Aloul, S. Zahidi and W. El-Hajj, “Two Factor Authentication Using Mobile Phones,” IEEE International Conference on Computer Systems and Applications (AICCSA), Rabat, Morocco, May 2009.
[16] OpenPNE, http://www.openpne.jp/
[17] 木川真孝， 吉川貴，大久保信三，竹下敦，高橋修，“Bluetooth の RSSI を利用した離席判定方式の提案と評価,” 情報処理学会研究報告. MBL，モバイルコンピューティングとユビキタス通信研究会研究報告，pp. 95-102，2009 年.
[18] 牛越達也，出射健一郎，西出亮，河野恭之, “Bluetooth デバイスの検出履歴を用いたユーザ行動の分類,” 情報処理学会第 22 回ユビキタスコンピューティングシステム研究会, 2009-UBI-22, 2009 年 5 月.