情報処理学会論文誌　コンシューマ・デバイス & システム　Vol.7　No.1　21–33 (Jan. 2017)

コンシューマ・システム論文

# 狭域エリアにおけるICT活用システム

城ヶ﨑 寛[1,a)]　原 政博[2]　森 信一郎[3]　中村 嘉隆[4]　高橋 修[4]

受付日 2016年6月30日, 採録日 2016年10月31日

**概要**：会議室や飛行場の打ち合わせスペースといったきわめて狭い範囲（狭域エリア）でのICT活用に関しては，目前に存在する情報共有対象者のIDを遠隔地のサーバで管理したり，本人を容易に識別できるにもかかわらず認証サーバを要したりと，ネットワークリソースの活用が非効率的であるという問題があった．そこで，遠隔地との通信環境に依存せずに処理を実施するエッジコンピューティングの一種であるデューコンピューティングを応用したエンドデバイス間のサーバレスの通信技術でネットワーク接続性と高いネットワーク効率性を実現し，これまで着目されていなかった人の識別する力を活用して，安全性の確保された利便性の高い認証技術を提案する．この手法を用いて，狭域エリアにおけるICT活用システムについて新しい基盤技術を提案し利便性の高さを実証するための実験を行った．これにより，人の識別能力の活用が，実用的なレベルの利便性を実現しており，狭域エリアにおけるICT活用システムに有用であることが示された．

キーワード：狭域エリア，サーバレス

# ICT System in Narrow Area Network

Hiroshi Jogasaki[1,a)]　Masahiro Hara[2]　Shinichirou Mori[3]　Yoshitaka Nakamura[4]
Osamu Takahashi[4]

Received: June 30, 2016, Accepted: October 31, 2016

***Abstract:*** ICT usage in a narrow area such as meeting room or meeting space in the airport have problems. Even when members are right in front, the system manages information in far remote servers. Even when members recognize each other, the system requires authentication servers. In this instance, the system wastes network resources ineffectively. New system is required which can construct groups easily when members gather, and can share information in the group members. We propose the ICT infrastructure, which has the following features: authentication using human cognitive ability, grouping in local area network immediately, distributed shared memory sharing data among each terminal without server. We have done the experiment with using such methodology to prove the effectiveness of such methods in terms of usability. The experiment proved effectiveness of our proposing method to show enough usability in the real world.

***Keywords:*** narrow area network, server less

[1] 株式会社ワールド・ビジネス・アソシエイツ
World Business Associates Co., Ltd., Chiyoda, Tokyo 102–0083, Japan
[2] 株式会社富士通研究所
Fujitsu Laboratories Ltd., Kawasaki, Kanagawa 211-8588, Japan
[3] 千葉工業大学
Chiba Institute of Technology, Narashino, Chiba 275–0016, Japan
[4] 公立はこだて未来大学
Future University Hakodate, Hakodate, Hokkaido 041–8655, Japan
[a)] hiroshi.jogasaki.1@gmail.com

## 1. はじめに

ICT（Information & Communication Technology）は遠隔地間の距離を技術の力で近づけることを可能にした．その技術は情報を電子化し遠方の情報を瞬時に伝えることができるようにし，通話をはじめメールやSNSを含めた多くのサービスに活用されている．また，実際には遠くに存在する通信相手の識別の必要性は，ID/パスワードなど本人しか知らない識別情報を利用して，通信相手が正しい相

手であることを認証する技術を発達させた．相手の通信環境は，利用するネットワーク環境により変化する．自宅では家庭で契約しているインターネットサービスプロバイダ経由の接続，職場では会社の構築したネットワーク経由の接続，スマートフォンでは通信会社経由の接続となる．これらを常時把握することは困難であるため，通信環境が不変である代理サーバに対してお互いが接続し，そのサーバを経由して通信するようになった [1], [2], [3], [4]．これまでの ICT はこのように多様な技術を組み合わせて実現されている．

近年システムへの短納期・低コスト要求から，オンプレミス型（サーバ設置型）のシステムから，クラウドコンピューティングに需要が大きく変化してきている．クラウドも代理サーバの一種であるが，センサからの多量のデータを発生する IoT（Internet of Things）への期待の高まりにより，通信負荷の削減と，短い（10 ms 以下）レスポンスタイムの要求から，エッジコンピューティング [5], [6], [7] やフォッグ（霧）コンピューティング [8] のコンセプトが現出している．Skala らの研究 [9] では，さらにデュー（露）コンピューティングによるエンドデバイスどうしの通信によるコンピューティングのコンセプトが提案されている．ただし具体的な実装は個別の研究に依存しており，標準化に向けた議論が開始されたばかりである [10]．

従来技術における認証とは，遠隔地にいる通信相手が本人であることを証明する本人認証と，その通信相手の持つ権限に従ってアクセス可能な情報を限定するアクセス制御を実現することを意味している．

最近，タブレット端末（タブレット型 PC）や画面サイズの大きいスマートフォンが普及するにつれ，ICT 技術は音声やデータ，簡単なテキストのみのコミュニケーションから，長い可変長のテキスト，画像や動画を使ったコミュニケーションへと変化してきている．さらに，互いに相手を識別できるような狭いエリア（以後狭域エリアという）において，タブレット端末を使った情報共有サービスの普及が始まろうとしている．

飛行機のフライト前のブリーフィングにもタブレット端末が採用され，情報共有機器として利用されている [11], [12]．プロジェクタを備えた専用の会議室ではなく，その場で空いている会議机などにフライトアテンダントが集合し，フライト時の接客サービスや想定される課題を共有するために，それぞれの人がタブレット端末を持ち寄り，互いの情報を画面に表示してブリーフィングを実施している．集合する場所に依存することなく会議を開始することができるので，会議室予約などの事前の手続きなしで，利便性の高い打ち合わせが可能である．

狭域エリアにおけるタブレット端末を代表とする ICT 機器の使われ方はこれまでの距離を技術の力で近くする使われ方とは大きく異なる．狭域エリアでは従来のようにお互いが対面しない遠隔地にいる前提でシステムを考える必要性がない．目前のネットワークリソースのみの活用で事足りるのに，わざわざ遠隔地にある認証サーバを利用する必然性はない．ここでいうネットワークリソースとは，一般にはネットワーク上の資源のことをいう．回線，HUB，ルータ，プリンタ，サーバ，共有フォルダなどである．本稿では，ネットワークで使用される HUB，回線，ルータなどの基盤の資源のことをさしている．タブレット端末が狭域で使用される環境では，ローカルデバイスどうしの通信に限定すれば，ローカルなネットワークリソースのみしか使用しないのに対して，サーバを利用した通信では，タブレット端末とサーバ間のネットワークリソースを使用することにより，本来不必要な資源利用が生じる．このことにより端末からサーバに至るネットワークに不具合が起こると，ローカルでのシステム利用ができなくなる場合が出てくる．狭域エリアの ICT 活用システムを従来システムの発想で考えることはネットワークリソースの活用が非効率であり，動的にグループを形成する際には認証のために事前に参加者の設定が必要で利便性が低いという問題がある．

狭域エリアの ICT 活用に関する従来の研究や事例では，狭域エリアを従来ネットワークとは異なる独自プロトコルでの実装が行われていてネットワーク効率性は高いが実装が TCP/IP でなく閉鎖的でありネットワーク接続性が確保されておらず維持コストが高かったり，悪意のある第 3 者が認証を通過する危険があり，安全性が確保されていなかったりする．ここでいうネットワーク効率性とは，ローカルなネットワークリソースのみ使用する場合に効率性が高く，外部のネットワークリソースを使用することにより，本来不必要な資源利用が生じる場合には効率性が低いと定義する．ローカルデバイスどうしの通信に限定すれば，ローカルなネットワークリソースのみ使用するのに対して，遠隔地のサーバを利用した通信では，タブレット端末とサーバ間のネットワークリソースを使用することにより，本来不必要な資源利用が生じる．またネットワーク接続性とは，インターネットをはじめとするほとんどのネットワークが使用している通信プロトコル（通信手順）である TCP/IP を利用して，他のネットワークとの接続を可能にすることと定義する．クラウドコンピューティングで利用される通信手順も TCP/IP であるため，グローバルな広がりを持つような IoT では，収集したセンサデータを蓄積するために TCP/IP を使用する必要がある．Microsoft 社は，OS に独自のネットワークプロトコルである NetBIOS，NetBEUI を使用してきたが，インターネットの一般化と TCP/IP が主流になったために，WindowsXP 以降のクライアント OS では標準プロトコルとしては実装しなくなっている．これも NetBIOS のネットワーク接続性の不適合である．接続性も確立され，安全性も確保されているが従来の距離を技術の力で近づける技術が前提の認証技術を活

用しているために利便性に問題をかかえている研究もある．いずれもネットワーク接続性，ネットワーク効率性，安全性，利便性のどこかに課題をかかえており，完全ではない．

狭域エリアにおける人と ICT システムにおいては，通信方式は，インターネットもしくは LAN/WAN にもネットワーク接続性が確保されたエッジコンピューティング方式で基盤を構成し，認証および情報共有の場面では，ネットワークリソースの活用が効率的なエンドデバイスどうしでデューコンピューティングを実現する新しい考え方が必要である．

また狭域エリアにおける本人認証に，これまで着目されてこなかったその場にいる全員の識別する能力に着目し，安全性が確保され利便性の高い認証を目指した．

本稿では上記で紹介した狭域エリアにおける ICT を使ったサービスを俯瞰的にとらえて，技術的な要素について検討する．具体的には狭域エリアでの通信方式と認証方式について述べ，その有効性について検証する．

本稿の構成を示す．2 章では狭域エリアにおける ICT 活用システムの関連研究とその課題について述べ，3 章では狭域エリアにおける通信方式と認証方式を実現する基盤技術を提案し，ネットワーク接続性と効率性および安全性に関する理論的検証を実施する．4 章では実験で認証方式の利便性に関する有効性を検証し，5 章で狭域エリアにおける通信方式と認証方式およびその上に搭載するサービスアプリケーションを実装した実証実験によって得られたこれまでにない狭域エリアでの ICT 活用を通じた実用性に関する考察を報告し，6 章でまとめを行う．

## 2. 関連研究・事例

本稿の対象とするシステムは狭域空間で実施される会議で利用される情報共有システムである（これを対象システムと呼ぶ）．

本章ではまず，対象システムに関し，狭域エリアでの通信要件を定義する．次に狭域エリアでの認証技術の前提条件とセキュリティ要件をあげ，最後に関連研究および事例において通信要件およびセキュリティ要件を満たすかどうか確認する．そのうえで関連研究における課題を明確にする．

### 2.1 通信要件とセキュリティ要件

対象システムを，従来システムの発想で考えることはネットワークリソースの活用が非効率であり，動的にグループを形成する際には認証のために事前に参加者の設定が必要で利便性が低いという問題があった．このことから狭域エリアで，通信技術においては最も普及しているプロトコル TCP/IP の実装を用い（ネットワーク接続性），認証技術においては効率的なエンドデバイス間で通信する（ネットワーク効率性）という通信要件を満たす必要がある．

対象システムにアクセス権限を持ち会議の参加者であるユーザを，本稿では「参加者」と呼ぶこととする．また対象システムにアクセス権限を持ち参加者候補となるユーザを「参加候補者」と定義する．対象システムに関し，認証技術の前提条件をまとめると以下のようになる．

(1) 会議は信頼関係の成立する参加候補者同士で実施．
(2) 参加候補者各自のタブレット端末には情報共有アプリが導入済みで最初の起動時にパスワードを設定可能（これにより本人の端末であることを担保する）．
(3) 会議の参加人数は人が識別することが可能な 10 名程度とする．

対象システムでのセキュリティ要件を以下にまとめる．従来のシステムでは遠隔地間の認証サーバを前提とするためにサーバ関連のセキュリティを考慮する必要があった．しかし狭域エリアにおける ICT 活用ではサーバ関連のセキュリティを考慮する必要はない．

セキュリティの脅威を Microsoft 社の STRIDE 分析 [13] で分析してみる．STRIDE（ストライド）分析は，マイクロソフト社の Security Engineering and Communications グループによって策定された手法で，システムにおいて攻撃者の攻撃を想定し，システム側で適切な防御策を講じるための分析手法である．なりすまし（Spoofing），改ざん（Tampering），否認（Repudiation），情報漏えい（Information Disclosure），DoS（Denial of Service）の中では，なりすましのリスクが今回の特別な要件（安全性）として対象となる．その他のリスク対策は一般的対策で十分である．

### 2.2 関連研究・事例

対象システムにおける通信要件とセキュリティ要件に関連する研究・事例としては，次のような研究および商用サービスの事例が存在する．

(1) Apple の通信方式 Bonjour [14]
(2) 「あいことば」による認証方式
(3) 物理的ソーシャルトラストに基づくコンテキストアウェア認証 [15]
(4) ソーシャルネットワークシステム LINE 方式
(5) 携帯電話によるソーシャルプラットフォームのためのタブレット端末グループ管理方式 [16]

以下これらの認証方式において，認証時のインタラクションを比較することにより，通信要件（ネットワーク接続性とネットワーク効率性）およびセキュリティ要件（安全性）を考察する．また，狭域エリアにおける ICT 活用には必要なメンバで集まりすぐに利用可能となる必要があるため，利便性が高くなければ活用が進まない．

#### 2.2.1 Apple の通信方式 Bonjour

Bonjour（ボンジュール）は Apple 社の開発したゼロコンフィグレーション技術の実装である [14]．主として LAN

環境で，何の設定も実施せず，機器を使用可能とすることができる．TCP/IP ではないためネットワーク接続性は確保されない．しかし，独自プロトコルであるため，サーバを介することなく直接プリンタなどこのプロトコルを実装した機器とのやりとりが実施可能で，ネットワーク効率性は高い．当プロトコル単独でアクセス制限は不可能であるため，安全性は担保できない．ただし事前にアクセス権限の設定は不要のため利便性は高い．

また，この方式は，それぞれの機器に Bonjour の実装を要求するが現実的にはタブレット端末のデータを同一 LAN 内にあるプリンタや PC とタブレット端末間の接続などといった限定した用途のためにしか実用化されていない．

#### 2.2.2 「あいことば」による認証方式

狭域エリアにおけるタブレット端末を活用した対象システムでは，グループ形成時にあらかじめグループで決めておいた「あいことば」を入力するという認証方式が考えられる．あいことばによる認証は，通常の TCP/IP を採用するアプリケーションに実装可能であるため，接続性は確保されている．またあいことばをサーバで管理する必要がありネットワーク効率性は低い．事前にアクセス権限の設定が不要であるため利便性は高いが，この方式では，悪意のある第 3 者が不正なルートで入手した「あいことば」を使って認証を通過するなりすましを防ぐことができないため安全性を満たしていない．

#### 2.2.3 物理的ソーシャルトラストに基づくコンテキストウエア認証方式

有村らの研究 [15] では，「人間が人間を目視する」ことによって被認証者と周囲のユーザとの間に成立する信頼度という文脈情報を用いて，なりすましを検知し，被認証者の認証可否をコントロールする新たなタイプのコンテキストウエア認証が提案されている．

社員同士が，互いのタブレット端末が隣接した際に，臨席者のタブレット端末情報が自分の端末に表示される．このタブレット端末情報と目視による本人確認情報が正しいかどうかを判定する仕組みとこれを蓄積する仕組みにより，認証強度を変更することができる．このことにより，信頼度の高いユーザの認証強度を弱めることが可能となり，利便性を向上させることができると論じている．当方式は，通常の TCP/IP を採用するアプリケーションに実装可能であるため，接続性は確保されている．必ずサーバを介した通信を要求するため効率的ではない．本認証で示されている信頼度と会議に参加することのできる権利とは直接関係がない．会議に参加可能なメンバに対して事前にアクセス権限の設定が必要であるため利便性は低いが，なりすましを防止する機能を実装することが可能で安全性は高い．

#### 2.2.4 LINE のグループ形成時の通信方式および認証方式

一方，一般消費者の使用する SNS である LINE では，「ふるふる」という機能で目の前の友人をシステム上に自分の友達として登録することができる．LINE のふるふる認証は，通常の TCP/IP を採用するアプリケーションに実装可能であるため，接続性は確保されている．必ずサーバを介した通信を要求するため効率的ではない．GPS の位置情報を利用し対象者との対面関係を把握し，互いにタブレット端末を振る振動を検知することで，信頼関係を確認している．相互の認証済みのメンバしか参加できないため安全性が確保されている．しかし LINE ではグループ形成ステップとして，各人の友達リストの中で，信頼関係のある友達を個別にピックアップし，別途グループ設定をする必要がある．事前にアクセス権限の設定が必要であるため利便性は低い．

#### 2.2.5 対面コミュニケーションにおけるソーシャルプラットフォームのタブレット端末グループ管理方式

大畑らの研究 [16] では，Bluetooth ペアリングによるタブレット端末認証と SNS アプリケーション（OpenPNE）のユーザ認証を組み合わせている．この方式は必要性の高まりを見せる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において，その場所にいることの確認と本人性の検査を提案している．ところが狭域空間でのグループ形成時の認証には，事前登録されている会議参加者との突合により認証する方式がとられている．当方式は，通常の TCP/IP を採用するアプリケーションに実装可能であるため，接続性は確保されている．また必ずサーバを介した認証を要求するため効率的ではない．相互の認証済みのメンバしか参加できないため安全性が確保されている．ただし事前にアクセス権限の設定が必要であるため利便性は低い．

通信要件では，2.2.1 項は，接続性を確保できず，2.2.2 項，2.2.3 項，2.2.4 項，2.2.5 項は効率性に課題がある．セキュリティ要件では 2.2.1 項，2.2.2 項では，なりすましを防ぐことができず安全性に課題がある．2.2.3 項，2.2.4 項および 2.2.5 項は，安全性は確保しているが，会議メンバの事前登録が必要であり，利便性に欠けるという課題がある．これらをまとめると**表 1** のようになる．

**表 1**　関連研究・事例の要件の適合・不適合
**Table 1**　Suitability matrix of the related research and the case studies.

| | ネットワーク接続性 | ネットワーク効率性 | 安全性 | 利便性 |
|---|---|---|---|---|
| 2.2.1項方式 | 不適合 | 適合 | 不適合 | 適合 |
| 2.2.2項方式 | 適合 | 不適合 | 不適合 | 適合 |
| 2.2.3項方式 | 適合 | 不適合 | 適合 | 不適合 |
| 2.2.4項方式 | 適合 | 不適合 | 適合 | 不適合 |
| 2.2.5項方式 | 適合 | 不適合 | 適合 | 不適合 |

## 3. 提案手法

通信方式としては，エンドデバイスどうしのデューコンピューティングを実現する新しい考え方を提案する（**図 1**）．

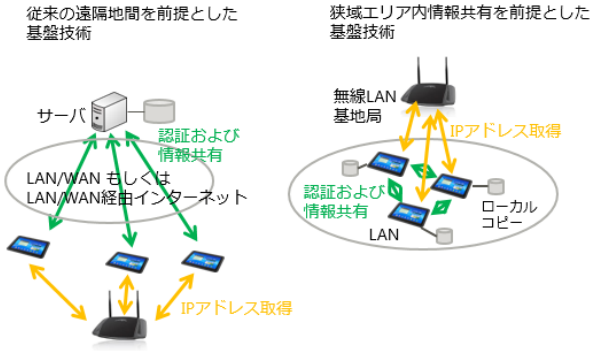



図 1　従来の遠隔地間と狭域エリアの基盤技術の違い

**Fig. 1**　Infrastructure technology comparison between current server-based in a wide area and server-less in a narrow area.

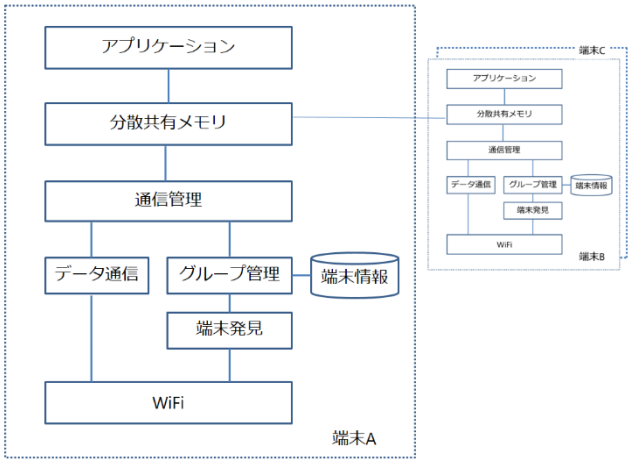



図 2　端末内機能構成図

**Fig. 2**　Functional configuration figure inside a smart device.

具体的には IP アドレスは無線 LAN アクセスポイントから取得し，認証においてはエンドデバイス間で通信する．このことにより，ネットワーク接続性を確保しながらネットワークを効率的に活用し，サーバレスでお互いのメモリを共有メモリとしてグループ形成するために利用しこれを仮想的なサーバと位置づける．無線 LAN アクセスポイントを利用する必要のない接続方式である WiFi Direct を用いると，サーバを参照したり，サーバに記録を残したりことが即時にできない．このネットワーク接続性を確保するために無線 LAN アクセスポイントを利用している．

グループ内の複数の端末は同一のサブネット内に存在するが，グループを管理したり，認証アカウントを管理したり，共有メモリを提供したりするサーバは存在しない．分散共有メモリは，それぞれの端末内にある共有メモリを同期させることで構成する．分散共有メモリと端末内機能構成図を**図 2** に示す．

認証方式は，安全性が高くかつ利便性の高い方式を提案する．安全性とは対象システムにおける 2.1 節のセキュリティ要件を満たして安全であることである．また利便性としては，動的にグループを形成する際に認証のために事前

表 2　従来と狭域エリアでのネットワーク構成の比較

**Table 2**　Network topology comparison between current server-based in a wide area and server-less in a narrow area.

| ネットワーク技術 | 従来ネットワーク | 狭域エリアネットワーク |
|---|---|---|
| 通信 | クラウド対応階層型ネットワーク | サーバレスローカルネットワーク |
| 認証 | 認証情報（ID/パスワード）による識別 | 人による識別と端末による妥当性の検証 |
| 識別対象 | 端末<br>人→（端末⇔端末）←人 | 人<br>人←——→人<br>↓　　↓<br>端末　端末 |

に参加者の設定が不要であること（利便性の要件 1）と，認証動作の人への負荷が軽く，実用的な時間内に認証が終了すること，具体的には 10 名程度の参加者の会議を前提としているため全員が集合してからのグループ形成時間は 60 秒程度（利便性の要件 2）と定義する．本章ではまず認証における安全性と利便性についてタブレット端末と人の協働関係を実現する認証方式と通信方式について述べる．

今回提案の認証方式ではブロードキャストが届く範囲である同一サブネット上に参加者全員のタブレット端末が存在することが必要条件となり，信頼関係のある参加者同士の通信のみ可能である．

**表 2** は物理的に遠い距離を技術的に近くするための従来型ネットワークと狭域エリアで利用するネットワークを比較した表である．狭域エリアネットワークの場合は識別対象が端末ではなく人であることがよく分かる．

### 3.1　狭域エリアにおけるグループ認証方式

なりすまし対策としてグループ認証方式を提案する．狭域エリアでのサービスを提供するには同じサービスを享受するグループを定義する必要がある．その際，相手は識別できるが，相手が持っている端末をネットワーク上で識別することは難しい．一般的にはグループ内の代表端末を一時的なサーバとし，そのサーバに他端末がつながる方式がとられる [17]．

しかし，そのためには対象端末の管理者からその端末の ID を事前に知らされる必要がある．動的に集まるグループにおいては，会議参加者を取りまとめる人は必要であるが，その場の誰でもよいという前提である．このため，事前に取りまとめ役を定義しておく必要はない．一時的にサーバとなる端末の選定をし，その端末 ID をグループ内の他のメンバに通知することは困難である．一方，人がグループ

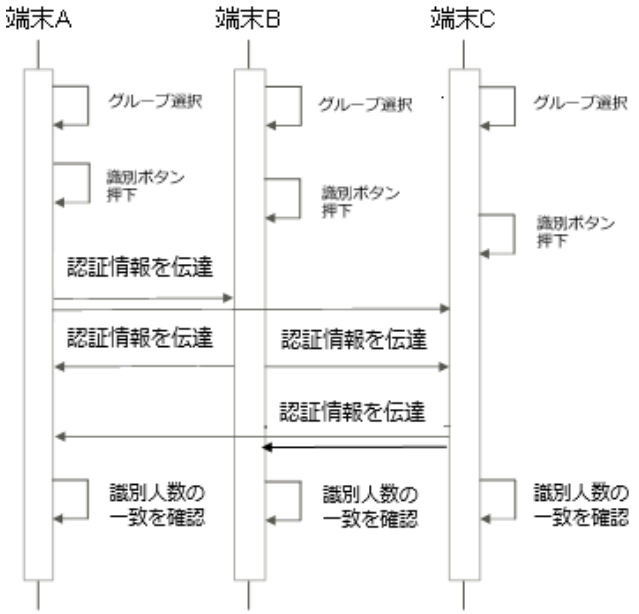



図 3　グループ認証のシーケンス
**Fig. 3**　Group authentication sequence.

内のメンバを識別することは容易である．そこで，共通のアプリケーションをそれぞれの端末に入れ，グループ形成時にそのアプリケーションを起動することとする．グループメンバの識別は人が対応し情報の妥当性の検証は端末が行うことで，ICT と人を組み合わせたグループ形成方式を採用した．**図 3** に認証ステップを示す．この認証の特徴は人と ICT の作業分担である．参加者が，アプリケーションを立ち上げると，現在同じサブネット内で使用されていないグループ名をアプリケーションが自動的に生成する．自動生成されたグループ名はアプリケーションがブロードキャストで同じサブネット内にある端末に通知する．最初にアプリケーションを立ち上げたメンバが自分のグループ名を他のメンバに口頭で通知することにより，メンバは指定されたグループ名を選択することが可能となる．人はグループの参加者を識別するたびにボタンを押す．端末は押された回数をカウントし，その情報を同一サブネット内の端末に識別情報として通知する．つまり，ほぼ同時刻（30 秒以内）に起動したアプリケーションを有する同じグループの参加人数をそれぞれの端末間で比較することでグループの形成可否を判断する．基本的には必要最小限なメンバがそろった段階で全員がアプリケーションを立ち上げるため，30 秒以内という想定をしている．

全員の入力するメンバ数が完全に一致するまで会議が開始されないため，アプリを持つ参加権限のないユーザがなりすまして狭域空間内にいても参加を拒否される．すなわちこの認証は参加者同士の信頼関係によりアクセス制御機能を提供し，安全性が確保されている．またこの認証は，参加者間での情報の共有が主たる目的であり，お互いの信頼関係によりアクセス制御が完結するため，事前の会議参


図 4　認証画面
**Fig. 4**　Authentication screen.

加者の設定も，アクセス権限の個別設定も不要である．これにより利便性の要件 1 が満たされている．グループ形成時の人数情報は，認証時にブロードキャストを用いて伝達する．各端末は，IP アドレスなどの端末情報，入力された人数情報などの認証に必要な情報などをパケットに載せてローカルエリアネットワークのサブネット内にブロードキャストする．端末情報は，(1) 端末の IP アドレス，(2) 端末の MAC アドレスであり，認証に必要な情報とは，(1) 入力された人数情報，(2) グループ名，(3) アプリの起動時刻のことである．

実際のデータ形式は，たとえば以下のような形式で送受信される．

device_ip_address:　タブレット端末の IP アドレス
device_mac_address:　タブレット端末の MAC アドレス
device_number:　入力された人数
device_group:　グループ名
startup_time:　アプリの起動時刻

他端末は，ブロードキャストで通知される情報をもとに，どの端末がサブネット内に存在するのかを検出する．これによって利用者は識別した相手の端末 ID を知ることなく利用できるようになる．

グループのメンバ数を人が数えて入力する場合，何か他の仕草にあてはめて数えることがある．たとえば指差しにあてはめたり，言葉にあてはめたりすることで数を数える．つまり数を数えることは人にとって得意な処理ではない．したがって，人は人の識別のみを行い，人数加算は指の操作を端末で行うという形で作業を分離することは，それぞれ得意とする処理を行ううえで重要と思われる．**図 4** に後述の実装アプリ例である模造紙アプリでの，各自の端末に表示されるグループ形成画面を示す．左中央に識別ボタンがあり，人は参加する人が正しい人であると判断すればボタンを押下する．他のメンバも識別するごとにボタンを押下する．端末は押された回数をネットワークに送信し，他の同グループの端末情報と比較することでグループ形成可否を判断する．上記の方式を使うことで，事前に特定のグ

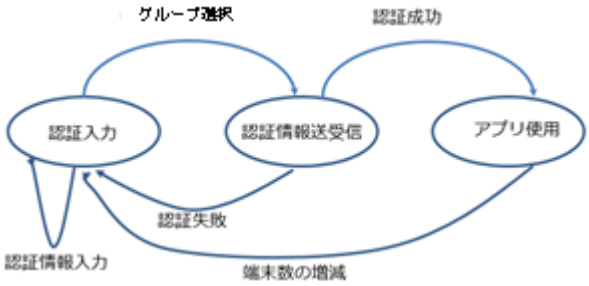



図 5　グループ形成における状態遷移
**Fig. 5**　State transition of group forming methodology.

ループに向けた設定や，ID/パスワードなどの認証情報を入力することなくグループ形成が可能となる．

グループ形成における状態遷移図を**図 5** に示す．提案システムのタブレット端末は，認証入力状態→認証情報送受信状態→アプリ使用状態に遷移する．この状態管理は共有メモリ上で実施される．通常は認証入力状態でリーダのタブレット端末が狭域空間へ立ち入り，グループ名が指定され認証が入力されると，このデバイスは認証情報送受信状態となる．メンバ全員の認証が正常終了すると，アプリ使用状態に遷移する．会議が終了すると認証入力状態に戻る．

途中退出する参加者がいる場合には，2 通り想定される．皆に退出を告げて電源 ON のまま立ち去る場合と，電源を OFF して立ち去る場合である．電源 ON のまま立ち去る場合は退出を確認する画面が他のメンバのタブレット端末に表示される．ここで OK すると共有メモリで管理されている人数が減ることとなり，正常状態が保たれる．電源 OFF して立ち去る場合には退出するメンバの状態は，会議状態から変更されないため会議の総人数は減るが，共有メモリ上で管理されている人数は減らない．このとき，権限のない人物が参加者になりすまして会議情報共有システムにアクセスする危険性が想定されるため，図 5 のように再認証が必要となる．

後から参加する参加者がいる場合総人数が増加し，新たなメンバの信頼関係を確認する必要があるため，アプリ使用状態から再度認証入力状態に戻り，グループ認証が開始される．なお共有メモリ上の会議のログ情報には位置情報（無線 LAN の MAC アドレスとグループ名）および参加者のタブレット端末の IP アドレス，MAC アドレスが記述されており，参加者としての記録は保持される．

### 3.2　狭域エリアにおける通信方式

サーバレスの認証を実現するために前節で説明したグループ情報を利用する．グループを形成している端末にはグループ内の他端末の IP アドレスが記録されている．この情報を使って各端末がお互いに情報を交換し合うことで分散された共有メモリ（分散共有メモリ）を作ることができ，グループ内で仮想的なサーバとして利用することができる（**図 6**）．分散共有メモリは以下の方式で実装されている．

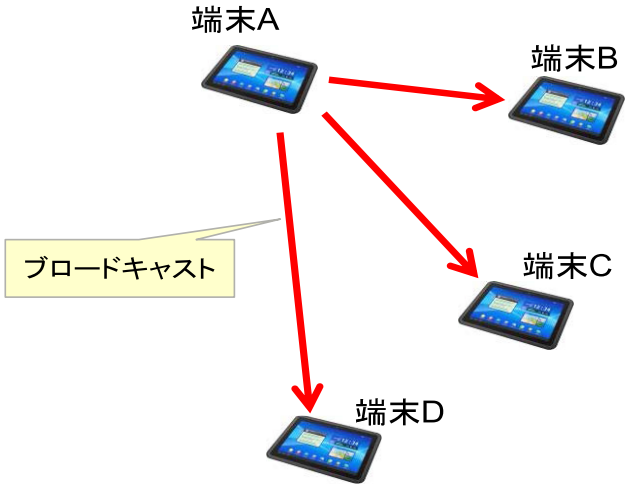



図 6　ブロードキャストによる端末・認証情報通知
**Fig. 6**　Terminal authentication notification by broadcast.

【方式】ローカル・ブロードキャストおよびブロードキャストレシーバ

【アルゴリズム】ローカル・ブロードキャスト（大きく分けるとダイレクト・ブロードキャストとローカル・ブロードキャストに分けられ，ローカル・ブロードキャストは同じサブネット内にブロードキャストパケットを配信する）によって同じサブネット内にある端末に情報を送信する方式である．

【実装方法】ブロードキャストレシーバでデータを取得し，格納するための配列のデータ構造は下記のような形式である．

wlan_mac_address:　無線 LAN ルータの MAC アドレス
auth_status:　グループ形成時の状態
device_ip_address:　タブレット端末の IP アドレス
device_mac_address:　タブレット端末の MAC アドレス
device_number:　入力された人数
device_group:　グループ名
startup_time:　アプリの起動時刻

## 4.　実証実験

ネットワーク接続性を確保しながらネットワークを効率的に活用し，安全性が確保されている提案手法である今回の認証方式が利便性の要件 2 の観点で実用的なレベルで認証されることを確認するために実験を行った．

### 4.1　実験内容

今回の認証では，人の識別する能力によってグループ認証できることを説明した．この過程を分析すると，

(1) 人物を特定する，
(2) 人数を数える，

という 2 つの行動に分けることができる．

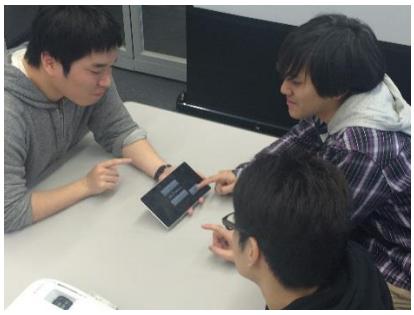


図 7　人物識別実験実施状況（実験 1）
**Fig. 7**　Experiment scene of human recognition (experiment 1).

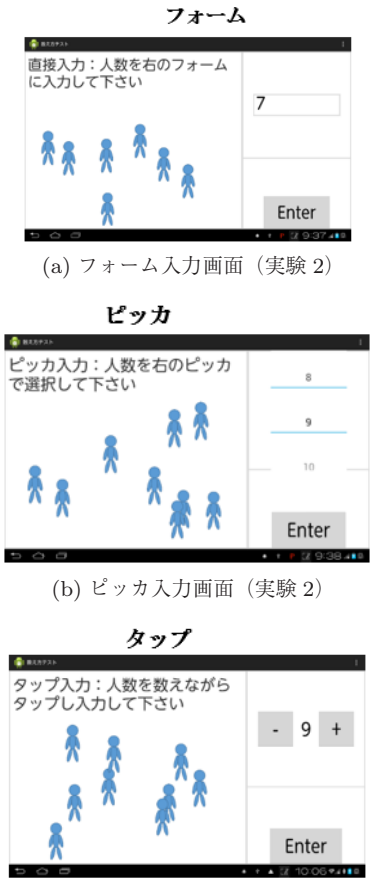
(1) では，目の前にいる人物が信頼関係のある参加候補者かどうかを判断する．(2) では，(1) で信頼関係ありと判断された参加候補者の数を数える．認証のタイミングで人数の自動認識ができるのであれば誰かが数字を声に出してしまうと，(2) だけの実行となり有効なグループ認証とはならない．このため，(1) を人間が実行し，(2) をタブレット端末上で人が操作する設計にする必要がある．信頼関係のある人を識別するには各種の簡便なインタフェースとの組合せの中で最も利便性の高い認証方式を考える必要がある．今回の実験は人物を特定する時間を評価する実験 1 と人物を数える時間を評価する実験 2 を実施した．

それぞれの実験詳細は次の 4.2 節のとおりである．実際に作成した業務アプリの全体の流れとしては，「グループ形成→情報共有→終了」であるが，実験 1 と実験 2 では，実用的な時間内でグループ形成されることを検証するため，実証評価対象プロセスは「集合→グループ認証によるグループ形成」に限定している．

### 4.2　実験詳細

実験 1 では，同じ研究室の学生被験者 9 名に自分以外の 8 名の写真をランダムに表示し，人物を特定するのにどの程度時間を要するかを測定した（**図 7**）．測定時間は表示ボタンを押してから名前を言い終わって次の写真の表示を実施するボタンを押すまでの時間である．また，9 名にそれぞれ 8 枚の写真を表示したため，合計 72 回の実験を実施した．実験に使用したタブレット端末は Android タブレット 3 台である．3 台で 3 人 1 組 3 回の実験で 1 巡するため，実験効率を高める狙いで 3 台での実験を実施した．

実験 2 では，プログラムで 5 名から 9 名までのランダムな人数の人間を画面に表示し，その人数を 3 種類の画面インタフェースで入力する実験を実施した．被験者 12 名が 3 つのインタフェースでそれぞれ 10 回ずつ試験を実施し合計 360 回の実験を実施した．インタフェースは簡便なインタフェース 3 種類である，フォーム入力，ピッカ入力，タップ入力による入力時間を計測する実験を実施した（**図 8** (a)，(b)，(c)）．自作評価ツールを導入した Android タブレット端末を 3 台使用した．3 台は 1 台ごとに 3 種類




(a) フォーム入力画面（実験 2）
(b) ピッカ入力画面（実験 2）
(c) タップ入力画面（実験 2）

図 8　実験 2 の入力画面
**Fig. 8**　Input screen of experiment 2.

の異なる入力方式に対応したプログラムを操作できるようにしてある．担当者の人数確認および人数入力でかかる時間を，画面が表示されてから入力終了するまでの時間の計測によって数値化した．

（1）フォーム入力方式

図 8 (a) のようなフォームに数字を直接入力する方式である．本検証実験においてフォーム入力は人数を数えることが人の処理が負荷となっているのかどうかを調査するために実施した．この際数える際のやりやすさから数を口に出して人数を数えてもよいとしている．

（2）ピッカ入力方式

次はピッカ（Picker）で選択する図 8 (b) のような方式である．ピッカ方式は人数をイメージとしてとらえる方式であり，指の動作と人数を数える行為が無意識化で連動しやすくフォーム入力よりは人の処理負荷が小さくなると想定される．フォーム入力のように数を口に出して数える必要がないため，より安全性の高い方式だと思われる．

（3）タップ入力方式

最後はタップして入力する図 8 (c) の方式である．タップ方式は人数を数える際に＋を押す行為で実施する．数を覚える必要性がなく，かつ人を識別するだけなので数字を口に出す必要性がない安全性の高い方式である．人の処理

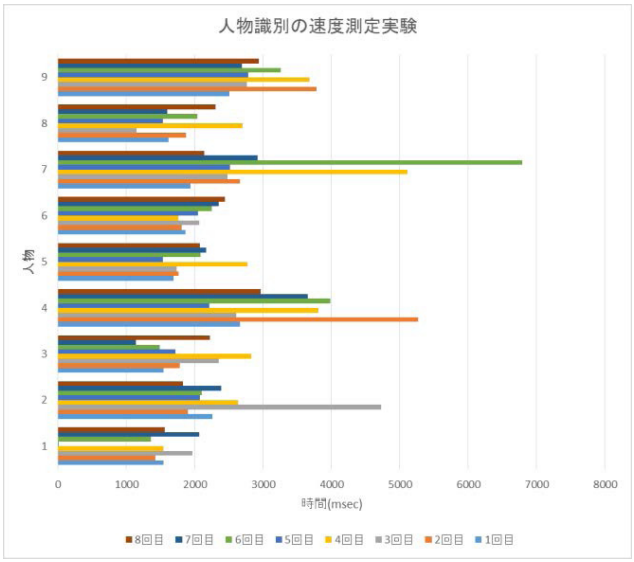



図 9　被験者が人物を特定するのに要した時間（実験 1）
**Fig. 9**　Human recognition time of testers (experiment 1).

負荷もフォーム入力よりは小さくなると考えられる．

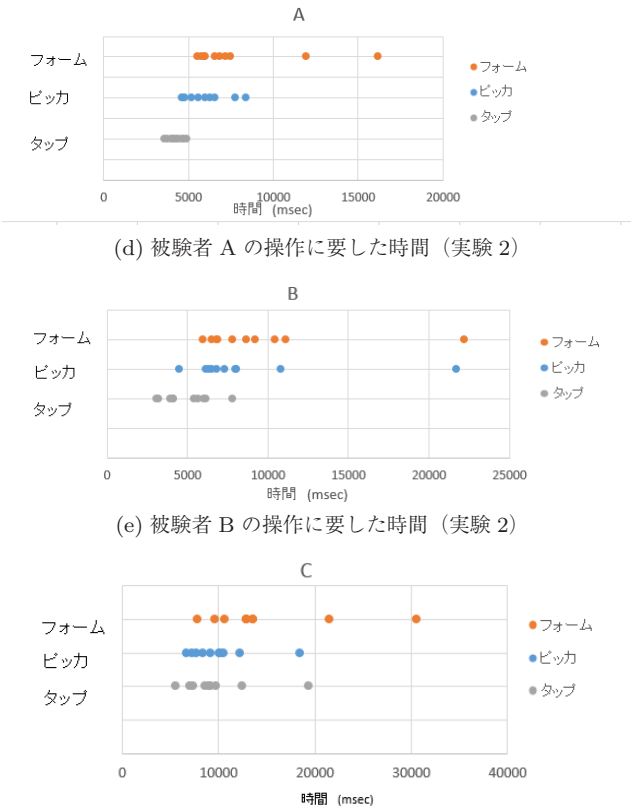
### 4.3　評価結果

評価は，入力時間計測を自作の評価ツールで実施した．実験 1 では，信頼関係を証明する方式として，画面上に表示される人を識別することにした．具体的には，画面上の人物の名前を口に出すことができる場合に信頼関係のある人という区別をつけた．被験者 9 名の実験結果が**図 9** である．全体の 86%にあたる 62 回の識別速度が 1 人あたり 3,000 ms 以下で 10 名でも 30 秒以内となっている．

実験 2 の人数に関する質問に対して簡便な入力インタフェース 3 種類（フォーム入力，ピッカ入力，タップ入力）で回答をもとめ，入力画面表示時点から，人数回答までの時間を計測した．評価実験の被験者 12 名の実験結果のうちで無作為に抽出した 3 名の 3 インタフェース 10 回の実験結果が**図 10** (d)，(e)，(f) である．この結果を見ると，被験者 A ではフォーム方式では 5,556 ms から 16,177 ms，ピッカ方式では 4,599 ms から 8,386 ms，タップ方式では 3,614 ms から 4,738 ms の範囲で入力している．多少の個人差は現れているが，ほぼ同等の傾向が見て取れる．最も短時間で処理が済む方式がタップ方式であり，2 番目がピッカ方式，3 番目がフォーム入力方式である．

タップ入力は今回実験した 3 種類の入力方法の中で最も入力時間が短いことが分かった．人の処理負荷も最も小さいと考えられる．したがって，本提案方式においてタップ入力方式が適していると考えられる．また操作時間はタップ入力ではすべてが 20 秒以内となっている．

実験 1 と実験 2 は，人物を特定する行動と人数を数える行動を別々に実験している．しかし実際のアプリケーションではこれを同時に実行可能である．また，実験 1 で信頼関係を証明する方法として，名前を口に出すという行動を




(d) 被験者 A の操作に要した時間（実験 2）
(e) 被験者 B の操作に要した時間（実験 2）
(f) 被験者 C の操作に要した時間（実験 2）

図 10　実験 2 の操作に要した時間
**Fig. 10**　Operation time of experiment 2.

採用した．実際のアプリケーションでは，名前を想起する必要はなく，顔を参加者として識別できればそれでよい．このため，実質的には実験 1 ほど識別に時間はかからず，実験 2 の測定値とほぼ同等の 20 秒以内の時間で認証が終了することとなり十分実用的である．

## 5.　考察

実証実験により，提案認証入力方式の有効性を検証した．実験結果により，人物を識別し，人数を数える認証方式は適切な入力方式を選択することにより，十分に実用的な時間での認証が可能であることが示された．このことから，従来方式では不可能であったネットワーク接続性，ネットワーク効率性，安全性および利便性をすべて満たす認証方式を実装した会議アプリケーションを利用して実際の会議を行うことにより共有メモリ方式を採用した通信方式を含む基盤技術の実用性を考察する．

### 5.1　狭域エリアにおけるアプリケーション

すでに 1 章で紹介した狭域エリアにおける各種サービスは情報の可視化によるグループ内メンバ間の意思疎通の補助を目的としていた．これは同じ能力を持ったメンバ間では大変有効なサービスであると思われる．しかしながら，メンバ内で得意とする能力に差異がある場合には，その能力差による課題を助長する恐れもある．たとえば，内向的

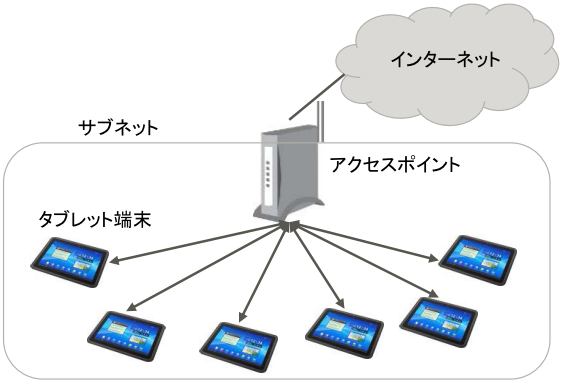



図 11　実験 3 のシステム構成概要図
**Fig. 11**　System configuration overview of experiment 3.

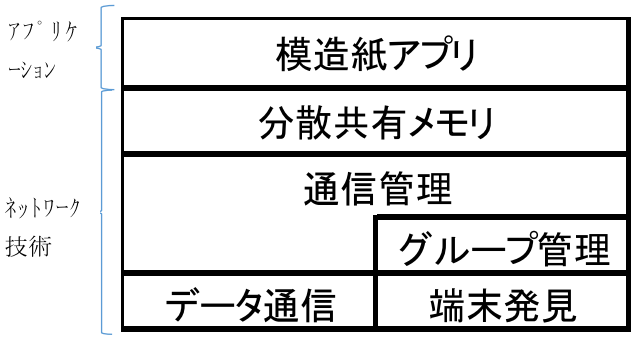



図 12　端末ソフトウェアモジュール構成図
**Fig. 12**　Software module configuration map inside a smart device.

な人がメンバ内にいる場合，上記サービスは人前での発言が得意なメンバの能力をより高めることになり，内向的なメンバの意見が見えなくなる恐れもある．そこで今回は ICT の特徴である「秘匿性」や「評価」を活用したアプリケーションを検討した．

「秘匿性」とはネットワーク上に投稿されるコンテンツの提供元が分からないという性質である．「評価」とは一般的に「いいね」ボタンと呼ばれているコンテンツに対する他人の評価機能である．発信元を秘匿することで意見が出しやすくなり，他人の評価もしやすくなると考えられる．狭域エリアにおけるサービスでもこの特徴を利用することで互いの意見を出しやすくできるのではないかと考えた．この機能を利用することで，発言力の弱い人からの意見は秘匿性を活用して引き出しやすくすることが可能になると思われる．自信を持って意見を出せるようになるに従って，レベル別に秘匿性を徐々に下げることによりプロフィールを公開していくことも可能である．秘匿性に加えて，他者からの評価に対する欲求を活用し，多様な意見を引き出す．他者が出した意見に対し，評価する手段を導入する．この評価についても，匿名性をレベル別に設定することを可能とし，様々なメンバの性格に合わせて対応することができる．

### 5.2　実験

3 番目の実験（実験 3）として狭域エリアにおける ICT 活用において，サーバレスでグループ形成を可能にするシステムを用いた実証実験を実施した．実験の目的は，これまでにない人の識別する能力を活用したグループ認証の認証方式および通信方式が実用的であることの検証である．

#### 5.2.1　実験システム構成

認証方式および通信方式の実用性を検証する実証実験のシステム構成概要図を**図 11** に示す．無線 LAN のアクセスポイントには富士通 SR-M シリーズ，タブレット端末には Android4.4 搭載の Arrows を 9 台使用した．

グループ内の複数のタブレット端末は同一のサブネット内に存在するが，グループを管理したり，認証アカウントを管理したり，共有メモリを提供したりするサーバは存在しない．また，同サブネット内に複数のグループが形成される場合もある．分散共有メモリは，それぞれの端末内にある共有メモリを同期することで構成する．

#### 5.2.2　模造紙アプリの実装

ICT の秘匿性と評価の特徴を利用することで互いの意見を出しやすくすることを目的とした模造紙アプリを作成した．模造紙アプリは，模造紙と付箋紙をメタファとしたテキスト・画像共有アプリケーションである．

端末ソフトウエアをモジュール構造で説明する．具体的には，端末発見モジュール，グループ管理モジュール，データ通信モジュール，通信管理モジュール，分散共有メモリモジュールの 5 つのモジュールが模造紙アプリを支え，アプリケーションと分散共有メモリ間の API は，共有化することで，ほかの用途のアプリケーションでも活用可能である（**図 12**）．参加時の認証インタフェースに関しては，アプリの認証画面の図 4 に示されるように，タップ入力方式を実装している．端末発見モジュールは，マルチキャストによるサブネット内の模造紙アプリ利用端末の発見や離脱の検知を行いグループ管理モジュールに通知する．グループ管理モジュールでは，端末発見モジュールで発見した他端末の端末情報（IP アドレス MAC アドレス）や認証情報（入力された人数，クループ名，アプリの起動時刻）の管理を行い，そのときのネットワーク接続状態を管理する．データ通信モジュールでは，同一グループ内に存在する他端末と通信路を確立する．通信管理モジュールは，グループ管理モジュールとデータ通信モジュールの統合管理を行い，端末発見モジュールで発見した他端末との通信路の対応付けの管理を行う．分散共有メモリモジュールでは，同期するデータの選別と，他端末へのデータ送受信によるデータ同期を実現している．アプリケーションは分散共有メモリにデータを書き込むことで同じグループに所属する端末に自動的に配信され同期が保たれる．

模造紙アプリでは，1 つのグループで 1 つの模造紙を共


図 13　模造紙画面（みんなのメモ）
**Fig. 13**　Information-sharing application's sharing memo screen.

有し，模造紙の画面上に，付箋紙を貼り付けていく形となる．共有の最小単位は，個々の付箋紙である．共有された付箋紙は，他端末と同期され，他端末の模造紙上にも表示される．秘匿レベルが低い場合には，付箋紙を作成した人の名前が付箋紙上部に表示される．他端末との同期は，前記分散共有メモリを介して行われる．本模造紙アプリでは，自分の模造紙にしか表示されない「あなたのメモ」と，グループ内の他者にも見える「みんなのメモ」（**図 13**）がある．「あなたのメモ」は，「シェアボタン」により，共有されグループ内の他者にも見えるようになる．また，他者のメモに対して評価を与える「いいねボタン」がある．「いいねボタン」が押下されると，そのことがグループ内の他者にも見える．

#### 5.2.3　実証実験の詳細

この実験では，ワールドカフェ方式を活用して，9 名の参加者が 3 つのグループに分かれて模造紙アプリを使用した．ワールドカフェとは Juanita Brown（アニータ・ブラウン）氏と David Isaacs（デイビッド・アイザックス）氏によって，1995 年に開発・提唱された討論のやり方の一形式で，与えられたテーマについて各テーブルで数人が議論する．

テーブルには移動しないテーブルホストと移動するゲストが存在する．テーブルホスト以外のゲストは他のテーブルへ移動し，そこのホストから前の議論のサマリを聞いてからさらに議論を行い，これを数回繰り返した後に，各テーブルホストが議論のまとめを行う方式である [18]．本実験ではクループ形成方式と分散共有メモリおよびアプリケーションを含むグループ認証方式が同一サブネット内で実用的に利用可能であるかを検証する．総人数は 9 名，1 つのグループは 3 名で構成され，討論は 3 回実施した．

ワールドカフェが開始されると，アプリを全員が起動する．テーブルマスタは，自分のグループ名をメンバに周知しておく．メンバは各テーブルのテーブルマスタのグループ名を選択し，そのうえでゲストとしてふさわしいメンバの数を各々がタップ入力し，認証を実行する．それから，発言をアプリ上のメモに記入していき，討論を実施する．既定の時間が経過するとメンバ全員がアプリを終了する．このときの議論内容や経過時間などは端末にログとして残される

この実験は無線 LAN ルータ 1 台に 9 名のメンバがアクセスする 10 名程度規模の実験である．複数グループが動的に形成される場面では従来方式は安全性と利便性を共存させることが難しかった．ワールドカフェ方式の会議は今回 3 名 1 組の会議であるが，メンバが交代していくことにより，あたかも参加者 9 名全員が話し合っているような効果が得られる新しい会議形式であり，提案方式の有効性を示しやすい実験であるため，この会議形式を実験対象として採用した．

#### 5.2.4　実証実験の結果

テーブルホスト以外の被験者は本実証実験システムを初めて利用する初心者とした．ログより各セッションが計画通りの約 20 分で終了していることが分かった．メンバを 2 回入れ替え，合計 3 回のディスカッションを実施したが，3 つのテーブルの 3 回のディスカッションすべてで，全員が集合して 60 秒以内に最初の新規メモが作成されており，ディスカッションに十分な時間をとることが可能なレベルで認証が終了している．このことから，通信方式および認証方式は十分に実用的であると評価できる．動的なグループ形成も通常タブレット端末なしで実施される通常の時間内で終了しており，端末を認識せずに人を識別してグループ形成する方法は狭域エリアの討論でも有効であることが分かる．また，その後もみんなのメモボタンの押下で情報共有が行われており，その意味でも分散共有メモリが有効に機能していることが分かる．これらより，本提案の認証方式や通信方式は実用的であると判断できる．

## 6.　まとめ

本稿は ICT を活用する新しい領域として「狭域エリア」を提案した．狭域エリアとは人同士がお互いに識別できるくらい近距離で存在するようなエリアを示し，その中での ICT 利用を「狭域エリアにおける ICT 活用」として新たな利用領域における技術を通信技術と認証技術に分けて検討を行った．狭域エリアではネットワーク接続性，ネットワーク効率性，安全性，利便性をすべて満たす基盤技術の方式提案が求められている．

通信技術に関しては，サーバレスを実現するために各端末にメモリを分散させて同期する方式を提案した．ただし今回の提案システムはブロードキャストが届く範囲での狭域エリアを対象としており，同じ場所に複数のサブネットの異なる無線 LAN アクセスポイントが存在する場合には対応していない．認証技術に関しては，狭域エリア特有の技術として，参加者の識別は人が対応し情報の妥当性の検証は端末が行うグループ認証方式を提案した．理論上で

ネットワーク接続性，ネットワーク効率性，安全性に関しては当方式が条件を満たしていることが示された．そこで基盤技術である通信方式と認証方式に関して実証実験を実施し利便性を確認した．この実証実験により，「狭域エリアにおける ICT 活用」の実用性に関する展望が開けた．すでに実現性の高いシステムが企業の要望を受けて導入に向けた構築準備中である．

今後は，具体的なアプリケーションにおいて，よりその付加価値提供によるメリットを評価できる検証を進める予定である．

**謝辞**　本稿の作成にあたりにご協力いただいた公立はこだて未来大学の学生の皆様および株式会社富士通研究所の皆様に，謹んで感謝の意を表する．

## 参考文献

[1] P2P ファイル共有から Web サービスへ シフト傾向にあるトラフィック IIJ，入手先 ⟨http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol08_report.pdf⟩.
[2] 増大する一般ユーザのトラフィック IIJ，入手先 ⟨http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol04_traffic.pdf⟩.
[3] Maier, G., Feldmann, A., Paxson, V. and Allman, M.: On Dominant Characteristics of Residential Broadband Internet Traffic, *IMC2009*, Chicago, IL (Nov. 2009), available from ⟨http://www.icir.org/gregor/papers/imc09-residential-traffic.pdf⟩.
[4] Labovitz, C., McPherson, D. and Iekel-Johnson, S.: 2009 Internet Observatory Report, NANOG47, Dearborn, MI (Oct. 2009), available from ⟨https://www.nanog.org/meetings/nanog47/presentations/Monday/Labovitz_ObserveReport_N47_Mon.pdf⟩.
[5] Satyanarayanan, M., Bahl, P., Caceres, R. and Davies, N.: The case for VM-based Cloudlets in Mobile Computing, *IEEE Pervasive Computing*, Vol.8, No.4, pp.14–23 (2009).
[6] 高レスポンスやビッグデータ処理が要求される新たなアプリケーションの開拓を推進する「エッジコンピューティング構想」を策定，入手先 ⟨http://www.ntt.co.jp/news2014/1401/140123a.html⟩.
[7] IoT 時代を拓くエッジコンピューティングの研究開発，入手先 ⟨http://www.ntt.co.jp/journal/1508/files/jn201508059.pdf⟩.
[8] Abedelshkour, M.: IoT, from Cloud to Fog Computing, available from ⟨http://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing⟩ (accessed 2016-06-08).
[9] Skala, K., Davidovic, D., Afgan, E., Sovic, I. and Sojat, Z.: Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing, RonPub, *Open Journal of Cloud Conputing* (*OJCC*), Vol.2, Issue 1 (2015), available from ⟨https://www.ronpub.com/publications/OJCC_2015v2i1n03_Skala.pdf⟩.
[10] Moble-Edge Computing, ESTI Portal, available from ⟨https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1 2018-09-14.pdf⟩.
[11] iPad は ANA 客室乗務員の業務をどう変えたか 世界初の大規模導入から半年—雲上の iPad 活用術，入手先 ⟨http://www.aviationwire.jp/archives/9626⟩.
[12] ANA アニュアルレポート 2013，p.65, available from ⟨http://www.anahd.co.jp/investors/data/annual/pdf/13/13_15.pdf⟩.
[13] マイクロソフト Technet，IT 脅威の分類，入手先 ⟨https://technet.microsoft.com/ja-jp/library/dd362836.aspx⟩（参照 2005-05-30）.
[14] Bonjour Overview, available from ⟨https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/NetServices/Introduction.html⟩.
[15] 有村汐里，小林真也，可児潤也，司波　章，西垣正勝：i/k-Contact：物理的ソーシャルトラストに基づくコンテキストアウェア認証，*Computer Security Symposium 2013*, pp.224–231 (2013).
[16] 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：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，情報処理学会研究会報告，Vol.2010-MBL-56, No.17, Vol.2010-ITS-43, No.17 (2010/11/12).
[17] ネットワーク管理者のための Skype 入門，入手先 ⟨http://www.atmarkit.co.jp/fwin2k/experiments/skype02/skype02_01.html⟩.
[18] ワールドカフェとは，文部科学省，入手先 ⟨http://www.mext.go.jp/a_menu/ikusei/kyoudou/detail/1367502.htm⟩.

**城ヶ﨑 寛**　（正会員）

1987 年早稲田大学理工学部電気工学科卒業．1987 年日本アイ・ビー・エム株式会社入社 2016 年公立はこだて未来大学システム情報科学研究科博士後期課程研究指導満了退学．現在株式会社ワールド・ビジネス・アソシエイツ所属コンサルタントとして国際コンサルティングと参加型センシングの調査・研究に従事．

**原 政博**　（正会員）

1996 年東京大学大学院理学系研究科修了．1997 年富士通株式会社入社．株式会社富士通研究所所属．ネットワーク技術の研究・開発，ヘルスケア分析技術研究・開発を経て，現在，フロントデバイス向けソリューション技術の研究・開発に従事．

**森 信一郎**　（正会員）

1987 年関西大学工学部卒業．同年富士通株式会社入社．2003 年から株式会社富士通研究所．2016 年から千葉工業大学先進工学部知能メディア工学科教授．博士（情報学）．ユビキタスコンピューティング，携帯端末による測位技術に関する研究に従事．

**中村 嘉隆**　（正会員）

2002 年大阪大学基礎工学部情報科学科卒業．2007 年同大学大学院情報科学研究科博士後期課程修了．同年奈良先端科学技術大学院大学情報科学研究科助教．2010 年大阪大学大学院情報科学研究科特任助教．2011 年公立はこだて未来大学システム情報科学部助教．2016 年より公立はこだて未来大学システム情報科学部准教授．博士（情報科学）．ユビキタスネットワークに関する研究に従事．電子情報通信学会，IEEE 各会員．

**高橋 修**　（正会員）

1975 年北海道大学大学院修士課程修了．同年電電公社（現，NTT（株））横須賀研究所に入所．コンピュータネットワークの研究開発/標準化に従事．2009 年 NTT ドコモに異動．モバイルインターネットの研究開発/標準化に従事．2004 年公立はこだて未来大学システム情報科学部教授．モバイルコンピューティングとユビキタスネットワーキングに関する研究に従事．本会元理事，本会標準化貢献賞，業績賞，功績賞を各受賞．電子情報通信学会，IEEE 各会員．本会フェロー．