社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2005－MBL－32 (10)
2005－UBI－ 7 (10)
2005／3／17

WOWnet:地域密着型防犯ネットワーク

片岡 真里帆[†] 竹田 和弘[†] 西尾 信彦[‡]

mariho@ubi.cs.ritsumei.ac.jp tiku@ubi.cs.ritsumei.ac.jp nishio@cs.ritsumei.ac.jp

概 要

近年, 学童に対する防犯, 路上犯罪への対策等, 地域社会の安全・安心に対するニーズが日ごとに高まりを見せている. こうした現状を受け, 防犯を核としたコミュニティーの形成を視野にいれた地域密着型の防犯システムの開発を行っている. 子供の持ち歩く端末が発する危険信号を周辺住民や親へ伝えるために, アドホックネットワークとインフラネットワークの両方を用いた広域通信環境の整備, さらには本システムを構成する各要素（子供の所持する端末, 無線通信用基地局, データセンタ）の構築を行い, 近接通信と End-to-End 通信を併用する防犯サービスの提供を目指す. 本稿では, システムのプロトタイプをモデル地域で実証実験し, そのシステムの実践的な評価について述べる.

WOWnet:Community-Based Security Network

Mariho Kataoka[†] Kazuhiro Takeda[†] Nobuhiko Nishio[‡]

ABSTRACT

In recent years, the needs for countermeasures against urban crime such as crime committed towards school children, as well as enhancing the safety and security in local communities are increasing day by day. Under these circumstances, we are developing a community-based security system aiming at preventing crime through close cooperation between members of the local community. In order to transmit danger signals emitted from small devices carried by school children to their parents as well as to community members located nearby, we have built a wide area communication environment formed both by both ad-hoc and conventional infrastructure network technology. With this network we aim at providing a security service using both End-to-End communication and communication to adjacent nodes. The system includes devices carried by the children, wireless base stations detecting danger signals and a data center. In this paper, we describe our evaluation of the demonstration experiment using our prototypical system in the model area.

1. はじめに

近年, 犯罪の増加や凶悪化が進行する中で, 学童に対する防犯, 路上犯罪への対策, 高齢者のケアに対する要望等も含め, 地域社会の安全・安心に対するニーズが日ごとに高まりを見せている. こうしたことから, 犯罪から子供を守るために地域住民らが立ち上がり, 団結し, 防犯活動を行うケースが増えている [1][2]. このような現状から, 本研究では防犯を核とし, 地域内のコミュニケーションの活性化の一端を担えるようなシステムの構築を目標としている. このシステムの核心部分は, 地域住民の防犯に対する日々の活動をどれだけサポートすることができるか, 防犯に対する意識を高め, 危険が迫っている地域内の人間を自ら助けるための手助けをこのシステムでどれだけ実現できるかということである. また, 将来的には, 本システムで使用するネットワークを有効活用し, 地域内のコミュニケーションの活性化だけでなく, 産業の発展も視野に入れたシステムの開発を行いたい. IT を最大限利用し、地域で犯罪を防ぐシステムを実現, そしてユビキタス社会におけるの安心安全な街づくりのモデルになるようなシステムを構築するため, WOWnet プロジェクトを行っている. 緊急時にサービスの緊急対処員ではなく近隣住民に現場に駆けつけてもらい助けてもらうという地域コミュニティの形成も視野にいれた防犯モデルの実現を目指し, 地域密着型の防犯システムのプロトタイプを構築, 実地にて実証実験を行い地域に密着した防犯システムの構築を行う. 本稿では地域密

[†]立命館大学理工学部情報学科
[†]Department of Computer Science, Ritsumeikan University
[‡]立命館大学情報理工学部
[‡]Department of Computer Science, Ritsumeikan University

着型防犯システムのプロトタイプモデル"SUZUKA"の設計，実装を述べ，モデル地区でおこなった実証実験の結果と評価を報告する．

2. システムの概要

このシステムの構成要素として学童の所持する無線デバイス，既にインターネットに常時接続している近隣住民の家庭 LAN 内に設させてもらう，我々が独自に構築した無線通信用基地局，そしてすべてのデータが集約されるデータセンタ，大きく分けてこの 3 つの要素に分けられる．登下校中の学童に IEEE802.11bg の無線デバイスの内蔵された小型端末を所持してもらうことで，このシステムの実現を図る．子供が所持する小型端末には，緊急時に近隣住民に助けを求めることのできる危険信号を発信するためのスイッチがついている．そのスイッチを押すことで近隣住民へ危険信号などの情報を発信することができる．本実装では子供の所持する端末はノート PC で実装し，プログラムを実行すること＝ボタンを押すことと定義する．また，このシステムを導入する地区の住民に対しては家庭 LAN 内に我々が独自に構築した無線通信用基地局を設置してもらうことで子供からの危険信号をキャッチし，子供の危険を知らせる．さらにそのデータは基地局から，防犯ネットワークを通じて，データセンタに集約され，防犯情報や子供の位置情報として保護者や地域住民に情報を提供するようなサービスを展開する．本実装では，基地局は Linux Box で独自に構築し，無線の NIC をアドホックモードで動かすことで子端末側のネットワークを全てアドホックネットワークで構築した．マルチホップ通信を実現することで，基地局を増やすことなくこのシステムがカバーする範囲を広げた．さらに基地局を設置した地域住民のみならず，端末を所持したほかの子供たちにも注意を呼びかけることができ，危険地域から遠ざけるための警告を伝えることができる．また，基地局をルーター化することで，ネットワークを 2 つに分け，局地的に危険信号を発信することを可能にした．

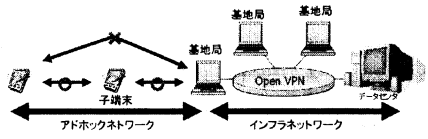

図 1: システム概要図

3. 設計と実装

3.1 システム構成

データセンタ

データセンタは立命館大学ユビキタス環境研究室内に設置し，VPN サーバーとしての役割をもつ．データセンタと各家庭に設置された基地局との間を結ぶ，独自の防犯ネットワークの構築のため OpenVPN を用いた VPN を構築した．OpenVPN はフリーの VPN 構築ソフトウエアであり，Linux をベースとした VPN を実現できる．認証にはよりセキュアな通信を目指すために TLS 認証を用いており，データセンタが認証局（CA）になって鍵，証明書を各基地局に発行することで VPN 接続時に認証を行うようにした．また，仮想の NIC として tun デバイスを用いレイヤ 3 トンネリングを実現する．基地局からの VPN を通して送られてきたデータをデータセンタが受信すると，パケットデータに到着時刻を負荷し標準出力及びログに出力する．さらに，データセンタは，危険信号以外にも常時子供からの位置情報データを受け取っており，危険信号を発信していない子供の位置もわかるようになっている．

無線通信用基地局

無線通信用基地局の無線の NIC はアドホックモードで動いており，有線の NIC は各家庭のインターネット回線とつながっている．またこの無線通信基地局は VPN クライアントとしても動作しており，VPN サーバーであるデータセンタとの間の通信を VPN によって確立している．さらにこの基地局はルーターとしても動作しており，アドホックネットワークとインフラネットワークを分離している．

子供の所持する端末

子供の所持する端末（子端末）はすべてアドホックモードで動いており，危険信号を発し始めた子端末からのパケットを受け取った他の子端末は，中継ノードとして作用し，データを基地局まで転送する．子供の端末では危険信号である Danger Packet(DP) と常時子供の位置情報をデータセンタに知らせる Location Packet(LP)2 つのパケットが送出される仕様になっている．

ネットワーク構成

本実装では VPN クライアントには VPN サーバーから DHCP で IP アドレスを割り振り，同一の VPN に所属させた．さらにすべての子端末及び無線基地局の無線 LAN には固定の IP アドレスを割り振り，同一のアドホックネットワーク内に属すように設定した．

データセンタ	有線 NIC	133.*.*.*
	VPN NIC	172.16.0.1
無線通信基地局	有線 NIC	各家庭に依存
	VPN NIC	172.16.0.0./24
	無線 NIC	10.0.0.0/24
子供の端末	無線 NIC	10.0.0.0/24

表 1: IP アドレスの割り当て

表 1 では今回割り当てたネットワークアドレスの一覧を示し，図 2 では SUZUKA のネットワーク構成を示す．

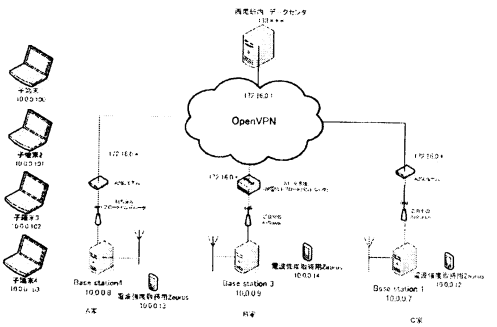

図 2: SUZUKA のネットワーク構成図

3.2 システム動作概要

- Danger Packet(DP)
  本実装では子供が危険を感じた時に DP を UDP で発信する．DP は基地局まで確実に知らせることが重要であるため，Best Effort で発信し続ける必要がある．しかし長時間 Best Effort で DP を発信し続けるのは，子端末の無線デバイス，ネットワーク全体の負荷が膨大になる恐れがあるため，適切であるとはいえない．そこで今回の実験では，子供端末が危険ボタンを押すと Danger Packet が 10 パケット Best Effort で流れ，100ms 休止する．その後，再び 10 パケット流し，100ms という流れを 300 回繰り返し，計 3000 パケットを 1 回の動作で送出した．また仮に基地局と直接通信できない場所にいても，他の子端末が DP を受信し，再度発信することで，基地局までパケットを届かせることを可能とした．

- Location Packet(LP)
  子端末は常に自分の位置情報をデータセンタに連絡するために LP を DP の場合と同様に，UDP で 1 秒間隔で発信している．今回に限り実験後のデータ解析をより円滑に行なうための機能として，パケット内に GPS で取得した緯度経度の位置情報を内包することで，パケット発信元の子端末と受信した子端末との距離を測定する機能を搭載した．また子端末に各基地局の緯度経度情報を事前に登録しておくことで子端末間の距離だけでなく基地局までのおおよその距離を表示させた．

使用機器	無線 LAN チップセット	デバイスドライバ
子供端末		
LOOX T90D (C1)	PRO/Wireless 2100B	ipw2100-1.03
Let's note W2 (C2)	PRO/Wireless 2100B	ipw2100-1.03
Thinkpad X31 (C3)	PRISM2.5	orinoco0.15rc2
Let's note R3 (C4)	PRO/Wireless 2200BG	ipw2200-0.21
無線基地局		
ベアボーン	PRO/Wireless 2100B	ipw2100-1.03
データセンタ		
デスクトップ PC	-	-

表 2: 使用機器，および無線環境

3.3 実験環境

実機の環境として，ノート PC4 台（子供端末用），ベアボーン 3 台（無線基地局用），デスクトップ PC 1 台（データセンタ用）を用意し実験を行なった．各 PC は Fedora Core 3(kernel2.6.9-1.667) をベースに構築し，子供端末，基地局では IEEE802.11bg の無線 LAN カードをアドホックモードで稼動させた．表 2 に子端末，基地局，データセンタで使用した機器，無線 LAN チップセット及びデバイスドライバの一覧 (表 2) を示す．また LP の位置予測機能のために子端末に CF カードタイプもしくは USB タイプの GPS を取り付けた．

次に DP，LP のパケット内のデータ構成を表 3 に示す．表 3 の予測経度，緯度とは無線基地局からの電波を使って現在の位置を測定するアルゴリズム [3] の予測結果である．本実装では DP，LP ともに同じパケットデータ構成をとり，パケットサイズを 128-byte の固定長とした．

3.4 アプリケーション層ルーティング

無線基地局においてアドホックネットワークとインフラネットワークを使用したネットワークを構築している．しかし，それら 2 つのネットワークを IP 層でルーティングするプロトコルの実装が間に合わないので，今回はアプリケーション層ルーティングを行なった．具体的には下記の 2 つを実装した．

- 中継機能の実現
  今回の実装ではアドホックネットワークの flooding 機能と同様の機能をアプリケーション層で実装した．DP，LP を発信する際には，パケットに

項目	説明
DP/LP 発信時入力データ	
Packet type	パケットタイプ
Packet ID	パケット識別子
Sequence	シーケンス番号
Send IP Address	発信元 IP アドレス
Time to Live	生存時間
Send Time Stamp	発信時間
Estimated Lat	予測緯度
Estimated Lon	予測経度
Real GPS Lat	実測緯度
Real GPS Lon	実測経度
子端末中継時更新データ	
Last Pass IP Address	中継 IP アドレス
Last Pass Time Stamp	中継時間
基地局受信時更新データ	
Base station IP Address	基地局 IP アドレス
Base station Time Stamp	基地局到着時間

表 3: パケットデータ構造

表 3 の適切な値を格納し，ローカルブロードキャストをする．子端末から送られてきたローカルブロードキャストを受信した子端末はパケットのデータを解析する．表 3 の Sequence と Packet ID から以前に同じパケットを受信したかどうかを判断し，初めて受信したパケットの場合にはパケット内の Time to Live 値を-1，Sequence 値を+1 する．さらには自端末の IP アドレス，到着時刻の情報を更新したのちに，変更したパケットを再度ローカルブロードキャストをする．もちろん Time to Live 値が 0 であればローカルブロードキャストを行なわない．

- 基地局での転送処理
  無線基地局ではアドホックネットワーク上の子端末からのローカルブロードキャストパケットを受信すると，そのパケット内のデータを解析する．もしそれがデータセンタへ転送を必要とするパケットの場合，データセンタ宛にパケットを送信する．

4. 実地実証実験

4.1 実験の概要

本研究では，滋賀県内のあるエリアに無線通信用基地局を設置し，将来，防犯システムを稼動させるために想定される環境を一時的に構築し，モデル地域での実験を行った．また，今回の実験では小学校の通学路沿いにある 3 軒の家庭を使って実際にネットワークを構築し，子供役の人間に端末をもたせこのエリアを歩かせることで，システムの運用実験を行った．

4.2 検証項目と実験方法

システムにおける様々な場合を想定し，数パターンの実験を行った．その中で本稿では特徴的な 2 パターンの実験を図 3，図 4 に示す．

実験 1:B 宅付近における 1hop の近接通信

実験 2:A 宅近辺に固定の 1 ノードを配置し,2hop と 1hop が両方起こるよう A 宅前を片方のノードが通過していったときの通信

この 2 パターンにおいて基地局から徐々に距離を置いていき各ポイントごとに静止し，DP（計 3000 パケット）を発信した．また，LP については実験中各端末の位置を認識するためにの発信し続けた．1hop の近接通信に加え 2hop でどのくらいの範囲をカバーすることができるのか，どのくらいの範囲がこのシステムにおいて適当かを検討することができる．

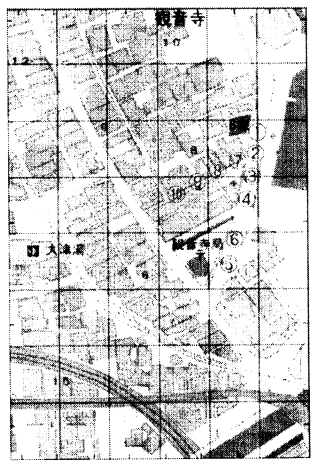

図 3: B 宅における 1hop の近接通信

さらにこれらの各実験パターンについて以下の項目を検証する．

- パケット到達時間
- パケット到達率と位置
- ネットワークトラフィック

この検証では GPS でとった子供の端末の位置情報と基地局の位置情報によってリアルタイムに算出される基地局からの距離に着目し，各ポイントごとで DP と LP の発信を行った．パケット到達時間や到達率は DP 内の経路情報から導き出すことができる．これらの実験を行うことで，このシステムにおいて重要になる地域住民への危険信号の伝達の様子を検証でき，システムの実現性を検討できる．また，各端末におけるネッ

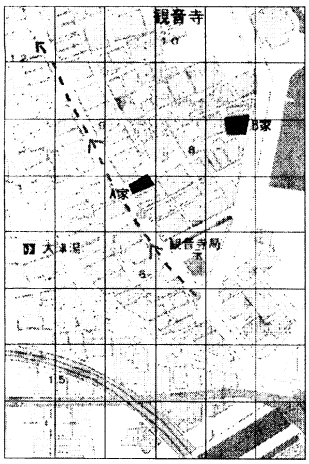

図 4: A 宅前をノードが通過していったときの通信

トワークトラフィックを計測するため，パケットアナライザを実験中常時稼動させ，アドホックネットワーク側のネットワークの状態を監視した．

4.3 実験結果

4.3.1 パケット到達時間

実験開始時に ntp サーバーに時刻をあわせ，実験を始めた．各子端末，各基地局，データセンタで受信したパケットにタイムスタンプを押し，データセンタにパケットが届くまでの経過時間の計測を行った．計測の結果 DP は 1 秒以内にデータセンタまで確実に届いていた．1hop の場合でも 2hop の場合でも同じことで，この結果はよりはやく危険な状況にある学童を助けることが可能であるといえる．

4.3.2 パケット到達率とネットワークトラフィック

各パターンにおける基地局と子端末間の距離と，それに応じたパケット到達率の図グラフを以下に示す．グラフ上に明記されている番号は地図上に書かれている番号と対応している．基地局と子端末間の距離は GPS で取得しているため多少は誤差があるものの，大体の実験位置を地図上にプロットしている．また，棒グラフの横軸は時系列にソートされた基地局から子端末までの距離 (m)，縦軸はパケット到達率 (%) となっている．次に各基地局おいてパケットアナライザをもちいトラフィックを計測したものを示す．線グラフの横軸が時間 (s)，縦軸がパケット流量 (bytes) となっている．

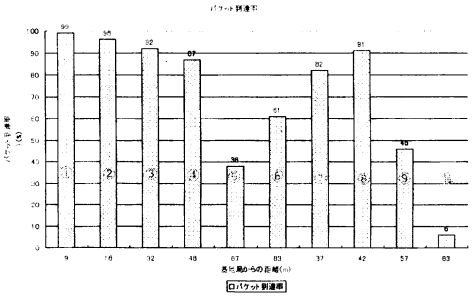

図 5: 子端末 1 から B 宅までの距離とパケット到達率

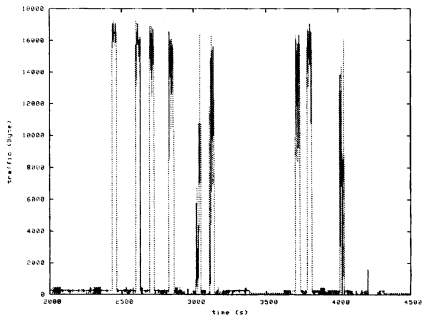

図 6: B 家の基地局のパケット流量の変化

実験 1:B 宅付近における 1hop の近接通信

図 3 の場所で実験をおこなった．この実験で使用した子端末は C1(表 2 参照) である．地図でもわかるように B 宅付近は見通しのよい直線道路となっている．図 5 上の①～⑥はその直線道路を南下し，各ポイントごとに Danger Packet を発信しパケット到達率を示している．⑦～⑩に関しては細い路地に入り計測したため同じ 83m 地点でもパケット到達率に大きな差がでた．また見通しのよい直線道路であれば 50m 付近を境に到達率が大きく変化した．つまり子供が基地局のある家庭の 50m 以内であれば 80%以上の確率でパケットが到達するという結果が得られた．図 6 ではこの実験で DP が 10 回発信されたことを意味している．また，パケット到達率に応じてパケット流量が変化しており，グラフの線が細くなっている部分でパケットロスが，頻繁に起こったと考えられる．

実験 2:A 宅近辺に固定の 1 ノードを配置し,2hop と 1hop が両方起こるよう A 宅前を片方のノードが通過していったときの通信

A 宅付近の路地の前に子端末 C4 が静止しており，その横を C3 が各ポイントごとに DP を発信しつつ通

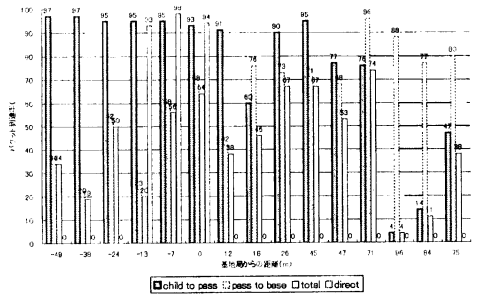

図 7: A 宅前をノードが通過していったときの距離とパケット到達率

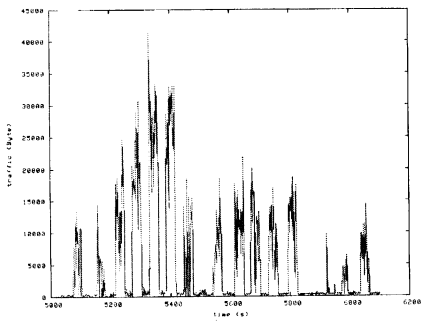

図 8: A 家の基地局のパケット流量の変化

り過ぎていく図 4 のような形態で実験を行った．図 7 の横軸は基地局の場所を 0 とした時の C3 から A 宅までの直線距離を表しており，基地局から南側をマイナスとしてプロットした．つまりこのグラフは A 宅から南に 49m の地点から，A 宅の目の前を通り 75m ほど北上したということを表している．そして，中継端末として動作する子端末 C4 はこのグラフでは-16m のところに位置しており，図 4 では細い路地の前に位置している．縦軸はパケット到達率 (%) となっている．グラフ中に 4 つの指標があるが一番左は DP を発している発信端末 C3 から中継端末 C4 までのパケット到達率，左から 2 番目は中継端末 C4 から A 宅基地局までのパケット到達率，左から 3 番目はそれら二つを合わせた 2hop で届いた合計のパケット到達率，左から 4 番目は C3 から基地局に 1hop で届いたパケット到達率をあらわしている．また図 7 からわかることとして，2hop で C3 → C4 → A 宅の経路を通る際に，C3 → C4 間のパケット到達率が高ければ，C4 → A 宅間のパケット到達率が急激に減ることがわかる．つまり，端末がパケットを多く受け取れば，送出できるパケットが減るということがわかった．この理由として考えられるのが，無線基地局の電波をつかって現在の位置を測定する位置推定プログラムの中でつかわれている iwlist というコマンドの使用状況であると考えられる．iwlist とは Linux の wireless tools の中のコマンドであり，周囲の基地局情報を取得するものである．位置推定プログラムでは DP 発信中はこのコマンドをたたかないように設定してあるのだが，中継端末では DP を中継していてもこのコマンドをたたき続けていた．そのためパケットの送受信にこのような影響が出たと考えられる．次に，C3 → A 宅への 1hop の通信が 3 点でしか行われなかったことについてだが，これは A 宅の基地局のアンテナが屋内にあり (図 9)，なおかつ両サイドに自動販売機があったため限られた範囲にしか電波が届かなかったものだと考えられる．

図 9: A 家のアンテナ

5. 評価

5.1 システムのカバーする範囲

地域密着型防犯システム SUZUKA を使い，行った実験を総合的に評価した結果，このシステムがカバーする範囲は 1 つの基地局に対し 1hop では約 30〜50m，2hop では約 50m〜70m という結果が得られた．3hop の実験も行ったが，3hop になると危険信号が届く範囲が広すぎるので，近隣住民も危険信号が届いても助けに行くまでに時間がかかってしまう．また，子端末の 2hop 以内に基地局がない場合，近隣住民へのパケットの転送が行われず，周りの子供だけに危険信号だけが届き大人には伝えられないという場合が考えられる．これを解決するために，ある一定時間基地局からの応答がなければ，DP の TTL を自動的に増加させていき，基地局に届くまでのホップ数を増やすことで，基地局へ DP が到達する可能性を高めるような実装も行っていきたい．

5.2 危険信号の伝達時間

危険信号を発信して 1 秒以内に近隣住民や近くの子供の端末に危険信号が届くため，すばやい行動をサポートできるだろう．しかし，今回の実験では 1 秒単位でしか時間の計測，記録を行っていなかったので，もっと細かい単位での時間の計測が求められる．

5.3 スケーラビリティ

今回，クラスAのアドレス空間を用いアドホックネットワークを構築した．今後このシステムを実際に運用するためには，学童の人数分のIPアドレスが必要になってくる．しかしひとりひとりにIPアドレス1つを割り当てるにはIPv4では限界がある．そのためIPv6化も視野に入れたネットワークの構築も行っていきたい．

5.4 防犯効果

このように防犯システムを実際に運用したいと考えている自治体と共同でシステムの実現に取り組むことは，その自治体が防犯に力をいれているということのアピールにもなり，防犯効果もあると考える．また，実地にて実証実験をすることで地域住民しか得られない情報なども得ることができ，システムの実現の際の重要な材料とすることができる．今後はこのシステムを使う子供や地域住民の方々に実際に端末を持ってもらい，実証実験していければと考えている．

6. まとめと今後の課題

今回の実験では，子供→基地局→データセンタへの一方的な通信にとどまったが，今後は危険信号を発信した子供の逃げ道の誘導やデータセンタから保護者，地域住民へ情報提供，危険信号を受信した際の基地局での子供の位置表示等のサービスの実現を図っていきたい．また実装に関しては今現在行っているアプリケーション層の処理をIP層まで落とし実装を行いたい．さらにノートPCによって実現されている子端末をより小型化するために，PDAでの実装，実験を行っていきたいと考えている．さらに今後の一番の課題はこのシステムのスケーラビリティである．ネットワークの信頼性やセキュリティ管理，スケーラビリティを考慮した上で発展性のあるネットワークの構築を図っていきたい．

謝辞

本研究を進める上で貴重なご助言を頂きましたオプテックス株式会社の勝部氏，林氏ならびに実地実証実験にご協力いただきました西大津地区の地域住民の皆様に謝意を表します．

参考文献

[1] 品川区:近隣セキュリティシステム．
http://www.city.shinagawa.tokyo.jp/.

[2] 立教小学校:児童一人ひとりの登下校を確認するRFIDシステム
http://www.rikkyo.ne.jp/grp/prim/.

[3] 石原 孝通，西尾 信彦: "GPSと無線基地局検出ツールを排他利用する位置情報システム"，情報処理学会ユビキタスコンピューティングシステム研究会報告，Vol.2004, No.112, pp.91-96, 2004年12月．