無線ネットワークにおける接続確認通信の解析

Analysis of Connectivity Testing over Wireless Links in a Redistribution System of Early Information

銭谷 英李* 松田 勝敬**

Eri ZENIYA* and Masahiro MATSUDA **

概要

As increasing the awareness of disaster prevention and mitigation, various early warning systems have been developed and operated in Japan. In most cases, a system is composed of servers and clients. A server receives warning information from ministries and other government agencies and redistributes it to clients. Clients are normally deployed in a fixed and protected area, such as a server room, in order to ensure the reliable reception of the information. We have studied mobile clients of early warning systems. In this paper, we focus on connectivity testing in early warning systems operated with mobile clients. Conventional testing methods assume only a stable environment based on wired networks. We discussed issues and requirements of the testing method in an unstable environment including wireless links.

In this paper, we conducted experiments on connection confirmation communication when we operated an emergency bulletin reporting system on a wireless network using mobile terminals. We also discussed how to manage the receiving terminal when operating the emergency bulletin reporting system in the wireless network.

1. はじめに

日本は外国と比べ地震，台風による洪水等の自然災害が多く発生している[1]．2011 年 3 月 11 日の東日本大震災以降でも，2016 年 4 月 16 日に発生した熊本地震など甚大な被害が発生した地震が発生している．台風などによる大きな被害が発生した水害については, 2011 年の台風 12 号, 2013 年の台風 26 号，2014 年の広島市土砂災害，2015 年の関東・東北豪雨，2017 年の九州北部豪雨などが発生している．それ以外にも，2014 年の平成 26 年豪雪，2014 年 9 月 27 日の御嶽山噴火など，多くの死傷者が出ている自然災害が起こっている．このような背景から，日本では災害に対する備えについての関心が高く，様々な防災システムが開発され運用されている．

また技術の進歩により，コンピュータが小型，高性能，安価になり，コンピュータネットワークは高速，広帯域になった．その結果，特に最近では無線通信技術の進歩と普及がめざましく，個人が高性能なコンピュータを携帯し，各所で高速なネットワークを利用できるようになった．そこで，自然災害による被害を防ぐ，減らす目的でコンピュータネットワークを利用した様々な災害対策システムが作られるようになった．現在，多くの災害対策システムが運用されており，無線ネットワークの普及により，スマートフォンなどの携帯端末で災害対策システムから災害情報を得ることが可能となった[2].

我々はこれらの災害対策システムのなかでも，日本が世界に先駆けて実用化し運用している，緊急地震速報システム[3]について着目をしてきた．これまでに通信のロバスト性や携帯端末を利用する，新たなシステム運用などについて研究開発を行ってきた[4][5]．その結果，緊急地震速報システムをスマートフォンやタブレット端末などの

2017 年 10 月 23 日受理

* 情報通信工学科 学生

** 情報通信工学科 准教授

無線ネットワークを利用する機器で運用する際の問題点が明らかとなってきた．従来の緊急地震速報システムは，安定した有線ネットワークで運用されている．そのため，携帯端末を用いた無線ネットワークでの運用では問題が生じる恐れがある．特に，サーバ・クライアント構成を採用しているシステムでは，サーバとクライアント間の接続状況が不安定になり，緊急速報をクライアントで受信できない場合が発生し得ることがわかった[6]．このような問題は緊急地震速報だけでなく，有線ネットワークを想定しているサーバ・クライアント構成の緊急情報を扱う防災システムなどでも発生すると考えられる．そこで今回は，サーバ・クライアント構成の緊急情報を扱う災害対策システムのなかで，実際に広く運用されており実績もある緊急地震速報システムを無線ネットワークで運用した際の再配信サーバと受信端末間の接続確認通信で発生する問題について，実験を通して考察，検討した．

2. 実用化されている災害対策システム

2.1 実用化されている緊急速報システム

日本列島は 4 つのプレートに囲まれ，日本は外国と比べ地震の多く，特にマグニチュード 6 以上の地震も多く発生する[1]．直近の 10 年間にも岩手・宮城内陸地震，東日本大震災，熊本地震と大きな地震発生し，それによる大きな災害も発生している．現在，こういった大災害の被害を防ぐ，最小限に抑えることを目的として，緊急速報システムが開発され運用されている．

実用化されている緊急速報システムの例を挙げると気象庁の緊急地震速報[3]，消防庁の J-ALERT[7]などがある．気象庁の緊急地震速報は 2004 年に一部地域での試験提供を開始し，2007 年から一般提供されている．緊急地震速報は地震発生直後に震源近くの地震計が P 波を観測したデータをもとに気象庁が震源やマグニチュード，震度などを予測し，各地に素早く発報するシステムである．地震波の伝わる速度よりも，観測データをもとに気象庁のコンピュータで予測した情報をネットワークで各地に伝える速度の方が速いため，震源から離れた地域であれば大きな被害が発生する主要動が到達する前に危険を知らせることができる．気象庁の予測した情報は緊急地震速報「警報」としてテレビ局やラジオ局，携帯電話各社に発信され，一般の方にテレビやラジオ携帯電話を介して提供される．また，高度な機械制御などに利用される緊急地震速報「予報」は気象庁から予報業務許可事業者などに発信され，そこから利用者の受信端末へ配信される．

消防庁の J-ALERT(全国瞬時警報システム)は 2007 年に運用を開始している．J-ALERT は災害情報を含む対処に時間的余裕のない事態に関する情報を国民に瞬時に伝達するシステムである．J-ALERT で扱われる緊急情報は気象庁が発報する津波警報や緊急地震速報などの自然災害に関する情報と，内閣官房が発報する弾道ミサイル情報や大規模テロ情報などの武力攻撃情報の 2 つがある．どちらの緊急情報も消防庁に発信され，人工衛星や地上回線を介して各地の J-ALERT 受信機へ発信され，防災行政無線やテレビなどで国民に伝達される．また，自然災害に関する情報は気象庁から直接，武力攻撃情報は消防庁を介し，携帯電話会社に発信され，エリアメールや緊急速報メールとして国民に伝達される．

2.2 緊急速報におけるサーバ端末間通信

実用化されている緊急速報システムは気象庁や消防庁などからの情報を受け取るサーバと，サーバからの電文を受信するクライアント（端末）のサーバ・クライアント構成を採用していることが多い．これらのサーバと端末間の通信は，緊急速報を確実にかつ瞬時に発信するために端末の設置場所を固定して有線の IP ネットワークが用いられることが多い．サーバ側の端末管理ソフトウェアに静的に割り当てた IP アドレスを登録し，端末を管理することが一般的である．さらに，緊急地震速報などの緊急情報の場合，何時でも瞬時かつ確実に受信端末に発信するために，一定時間ごとにサーバと受信端末間で接続確認通信を行っている．接続確認通信は数分間隔でサーバと受信端末間で行い，一定時間応答が確認できない場合はシステムの障害とし，インシデントの発生を検知する．インシデントが発生した場合は，システムの管理者などに通知を行い，障害対応を実施する．端末は物理的にもネットワーク的にも固定設置されたものとしており，接続確認通信により異常が検知された場合は，通信経路や端末自体に障害が発生したと見なすことができる．

3. 接続確認通信

接続確認通信は，情報システムの様々な箇所で用いられている技術である．コンピュータネットワークにより接続されている各機器は，他の機器がネットワークに接続されているか否かを，接続確認通信により確認する．特に高信頼性が求められるシステムにおける冗長構成の機器間や，構成機器の障害の有無などの検知のために用いられ

ることが多い．接続確認通信で障害が検知されると，冗長構成機器間で待機状態の機器を稼働状態にしたり，多くの機器から構成されるシステムの障害箇所の把握などが可能となる．

緊急速報システムの接続確認通信は，主として速報配信サーバと速報受信端末間の接続維持と速報配信サーバと受信端末もしくは通信経路の障害検知のため行われる．

3.1 接続維持

接続維持のための接続確認通信はスマートフォンなどのモバイル端末と OS のベンダが提供する通知用サーバ間でも行われている．新着の電子メールや SNS のメッセージなどは通知用サーバが受信し，通知用サーバからモバイル端末に送信されプッシュ通知が実行される．そのため，モバイル端末は通知用サーバとの TCP コネクションを常に確立しなくてはならない．例えば，通信経路中の NAT(Network Address Translator)や Firewall により TCP コネクションを切断されることを防ぐために，モバイル端末は定期的に接続確認パケットを通知用サーバへ送信する．通信経路中にある NAT (Network Address Translator) や Firewall の動作に起因するコネクション切断を避けるため，端末は定期的に Keep-alive[8]または Heartbeat と呼ばれる接続確認パケットをサーバへ送信する[9].

3.2 障害検知

例として，障害検知のための接続確認通信は隣接したルータ同士の生存確認が行われている．例えば，OSPF (Open Shortest Path Fast) [10] では，隣接ルータ同士の生存確認のために定期的に接続確認パケット (Hello パケット) をルータ間で交換する．そして，あるルータからの Hello パケットが一定期間確認できなければ，周囲の隣接ルータは当該ルータに障害が発生したと見なす．

さらに, IETF (Internet Engineering Task Force) では下位層の通信媒体やルーティングプロトコルに依存せず，低コストかつ高速な障害検出の仕組みとして，BFD (Bidirectional Forwarding Detection) [11] を標準化している．

4. 無線ネットワーク上での接続確認通信の検証

4.1 緊急地震速報による接続確認通信

緊急地震速報システムの再配信サーバと受信端末間における接続確認通信について，テストベッドを用いて測定をおこなった．

気象庁「緊急地震速報システム」における速報には，一般に向けてテレビやスマートフォンなどで発信される「警報」と工場などの機器制御に利用される「予報」がある．「予報」では，受信端末の設置場所の震度，主要動が到達するまでの時刻が利用者に伝達される．気象庁からの「予報」は認可を受けた事業者などの再配信サーバから契約者の受信端末に再配信される．この再配信は通常は有線の IP ネットワークが用いられる．「警報」はテレビやスマートフォンなどを所有していれば，申し込みなどは必要なく受信できる．一方「予報」は，専用の緊急地震速報受信端末が必要であり，業者などと契約をしないと受信することができない．また，「予報」では「警報」より詳細な情報を入手することができ，その詳細な情報を利活用することも可能である．この「予報」を受信する速報受信端末は，速報配信サーバと端末間で接続確認通信を行い，通信経路や端末に障害が発生していないか常に確認をすることができる．

4.2 接続確認通信の測定

これまで，有線ネットワークでの再配信サーバと受信端末間の接続確認通信の通信間隔に着目して 2 つの異なる受信端末で測定を行った[4]. 緊急地震速報システムの再配信サーバと，緊急地震速報受信端末を有線ネットワークで構成し，サーバと端末間の接続確認通信を測定した（図 1）. 緊急地震速報受信端末は，メーカーと形式が異なる 2 機種を対象とした．

その結果，接続確認通信の通信間隔は受信端末ごとに異なり，60[s]から 183[s]の数分間隔で行われていた．この結果から，有線ネットワークで物理的にもネットワーク的にも固定されたサーバと端末間で，障害検知を目的とした接続確認通信は，数分程度の間隔で行われていれば，実システムとして運用可能であることが分かった．

この結果を元に，無線ネットワークでの緊急速報システムの運用とその場合の接続確認通信に

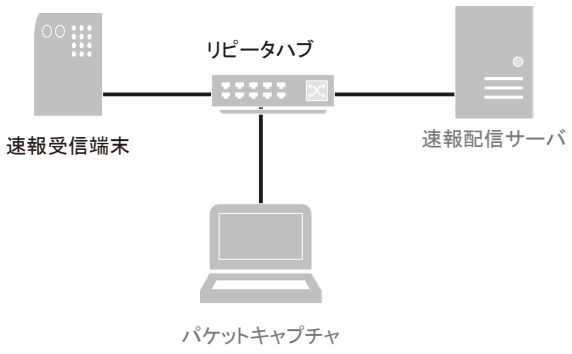

図 1　接続確認通信の測定環境

ついても検討と考察を行っている[4]．そこでは，緊急地震速報システムを無線ネットワークで安定して運用するには，接続確認通信の時間間隔の短縮，IP アドレスによらない端末の識別と管理，サーバおよび端末のどちらからも接続確認通信を開始する，などの対応が必要であると考えられた．

そこで以上の測定およびその結果と検討，考察から，今回は実際に無線の IP ネットワークで緊急速報システムを構成し，再配信サーバと受信端末間の接続確認通信を正常に行えるかについて調べた．

4.3 無線ネットワーク上での接続確認通信

今回の検証には Android 用に開発した緊急地震速報を受信するアプリケーションを[4][5]，タブレット端末(Android)にインストールして受信端末として用いた．受信端末が無線 LAN の電波が届く範囲外に移動することや，端末の電源を切断すること等よりネットワークから離脱し，リース期限が切れた後にネットワークに復帰した場合の接続確認通信の検証を行った．なお，無線 LAN の規格は IEEE 802.11n である．

実験環境を図 2 に示す．DHCP の接続台数は図 2 の状態で飽和になるよう設定した．PC は受信端末の IP アドレスのリース期限を確認するために使用し，ルータの DHCP 管理画面を表示させた．また，この PC でネットワーク内に流れるパケットのキャプチャを行い，各通信の詳細を確認，記録した．

実験 1 では，図 3 に示す手順で受信端末の IP アドレスが変化しないときの接続確認通信の実験を行った．実験 2 では図 4 に示す手順で受信端末の IP アドレスが DHCP で取得できないときの実験を行った．また，実験 2 では図 2 の環境に IP アドレスを専有するためのタブレット端末を 1 台

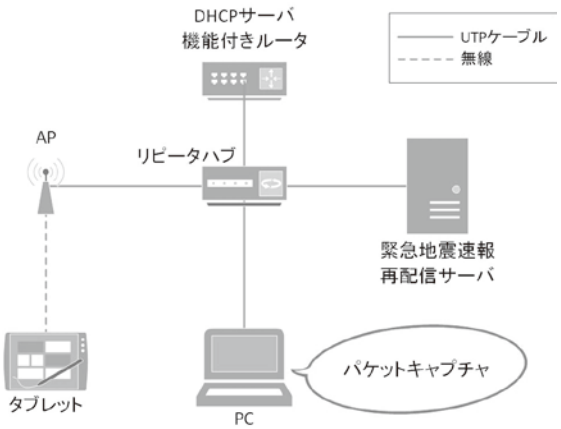

図 2　実験時のネットワーク構成図

図 3　IP アドレスが変化しない際の実験手順

追加している．実験では初めに，受信端末より接続確認通信を発生させ，再配信サーバとの接続状況確認を行う．このときの接続状況確認を①とする．次に，受信端末の電源を切断することでネットワークより離脱させる．受信端末の IP アドレスのリース期限が切れたら，受信端末を起動し，接続確認通信を発生させ，再配信サーバとの接続状況確認を行う．このときの接続状況確認を②とする．

接続状況確認は以下の 2 点について確認した．まず再配信サーバから受信端末が実験開始時に専有していた IP アドレスへの ping による疎通確認を行った．さらに受信端末の接続確認電文を再配信サーバが受信したと認識したかを確認した．

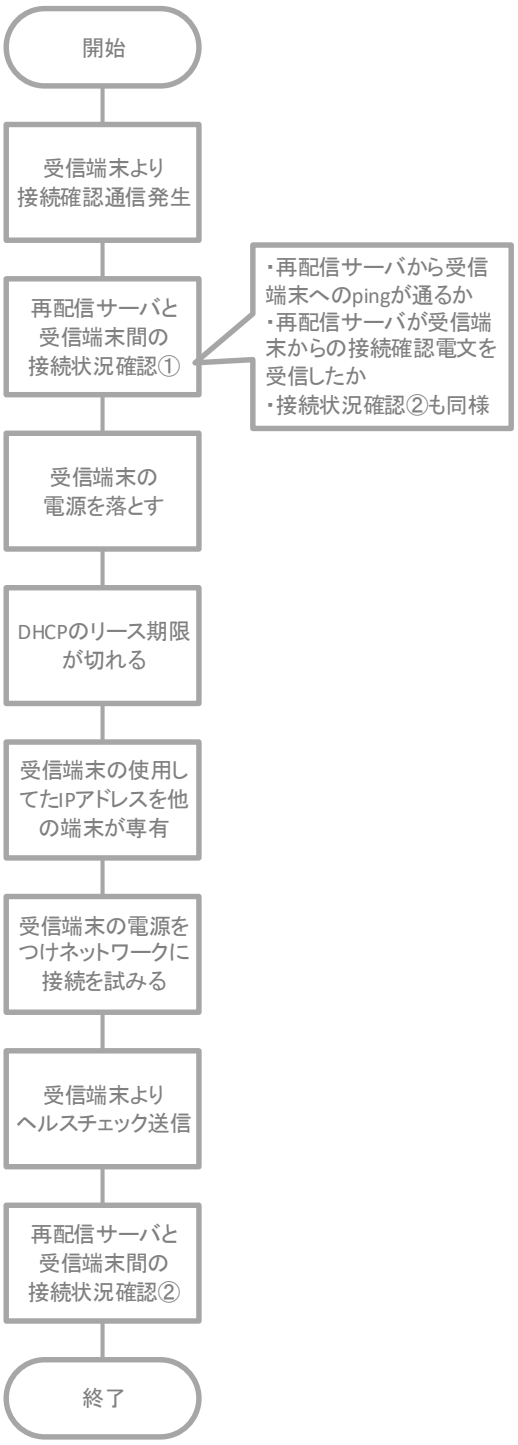

図 4　IP アドレスが DHCP で取得できない際の実験手順

4.4 実験結果

結果を表 1 に示す. ただし, 表の実験 1-①とは, 実験 1 の接続状況確認①を指す. 表の ping の項において, 実験開始時に受信端末が専有していた IP アドレスに再配信サーバから ping による疎通確認を行い，応答が返ってきた場合を○とし，返ってこなかった場合を×とする．表の接続確認通信電文受信の項において，再配信サーバが受信端末からの接続確認通信を受信したと認識した場合を○，認識しなかった場合を×とする．

表 1　実験 1,2 の接続状況確認①,②の結果

	ping	接続確認電文受信
実験1−①	○	○
実験1−②	○	○
実験2−①	○	○
実験2−②	○	×

どの接続状況確認においても ping による疎通確認への応答が得られた．ただし，実験 2-②では実験開始時に受信端末が専有していた IP アドレスは他の端末によって専有されているため，その他の端末からの応答である．接続確認電文の受信は実験 2-②のみ再配信サーバが受信端末からの接続確認電文の受信を認識できなかった．受信端末が使用していた IP アドレスが他の端末で専有されるとネットワークの端末数が DHCP の配布 IP アドレス数を上回ったため受信端末は IP アドレスを取得できない．そのため受信端末はネットワークに接続できず，受信端末から接続確認電文を送信しても再配信サーバは受信できなかった．

4.5 無線ネットワーク上での接続確認通信の考察

今回の実験のように，無線ネットワークでは受信端末がネットワークから離脱することが起こり得る．例えば，実験の様に，受信端末がネットワークの端末数が DHCP の配布 IP アドレス数を上回った端末数が接続された時などの場合，安定した接続である有線ネットワークの前提とした従来の緊急地震速報システムでは接続確認通信が行われないことが分かった．

再配信サーバは受信端末からの接続確認電文を一定時間受信できないことで受信端末が接続されていないことを認識する．接続確認通信は受信端末が電文を発信することで開始されるため，再配信サーバは受信端末がネットワークから離脱しても一定時間経過するまでは離脱したことを検知できない．安定した有線ネットワークでの運用であれば，端末の離脱の発生は，ネットワークまたはネットワークを構成する機器の障害となる．しかし，無線ネットワークでは端末の離脱，参加は通常の運用でも発生するため，再配信サーバから受信端末の接続確認通信も必要である．再配信サーバからも接続確認通信を行い相互の接続確認通信を実現することで，受信端末のネットワークの離脱と再接続などの変化にも有効であ

る.

また, 今回は受信端末の IP アドレスが変化しないときと受信端末の IP アドレスが DHCP で取得できないときの実験を行ったが，受信端末の IP アドレスが変化したときの実験も今後行う必要がある.

5. 携帯端末を利用した緊急速報システムの端末管理

5.1 携帯端末の IP アドレスの変化

無線ネットワークは有線ネットワークと異なってケーブルの配線などが不要のため，ネットワークへの参加・離脱が多い携帯端末等が接続される．特に，スマートフォンは広く普及しており，多くの人が利用する場所の無線ネットワークは接続している端末の参加・離脱が頻繁に行われることがある. そのような環境では DHCP の配布する IP アドレスが枯渇しないようリース期間を短く設定することが多い．そのような無線ネットワークの接続している端末と端末数は短時間に動的に変化する．携帯端末側から考えると，移動することで異なるネットワークに接続したときや一時的にネットワークを離脱して再接続したときに, 同じ携帯端末に異なる IP アドレスが付与されることがある. 受信端末の IP アドレスが変化した際に再配信サーバと受信端末間の接続確認通信が行われないと考えられる．そこで，無線ネットワークを利用した緊急速報システムの接続確認通信は, 受信端末の IP アドレスが変わることを考慮する必要がある.

5.2 端末管理

インターネットを利用しない安定した有線ネットワークでの緊急速報システムの端末管理では，その固定のネットワークに接続されている端末を受信端末とみなすことができる．よって端末管理は IP アドレスやそれに対応したホスト名で行われていることが多い.

携帯端末を利用した緊急速報システムの無線ネットワークでは，インターネットを利用し受信端末の IP アドレスが変わる恐れがあるため，IP アドレスやそれに対応したホスト名では受信端末を管理できない．そこで，携帯端末を利用した緊急速報システムでは，MAC アドレスで携帯端末自体を識別する必要がある.

6. まとめ

現在利用されている有線ネットワークでの利用を想定した緊急速報システムにおいて携帯端末を用いて利用する際の問題点について実験を通して確認し, 対策について検討・考察を行った.

緊急速報システムの接続確認通信について，ネットワークから受信端末が離脱して再接続し，受信端末が同じ IP アドレスを取得できた場合と IP アドレスが取得できなかった場合の 2 つの実験を行った．結果，IP が取得できなかった場合，接続確認通信は正常に行われなかった.

無線ネットワークで現在の有線ネットワークを想定した緊急速報システムを利用した場合に受信端末の管理に発生しうる問題について考察した．受信端末がネットワークから離脱・再接続を頻繁に繰り返し, 受信端末の IP アドレスが短時間で動的に変化する恐れがあり，そのような問題についての対策が必要であると考えられた.

以上より，無線ネットワークで緊急速報システムを運用する際には，再配信サーバからも受信端末の接続確認通信を行い，携帯端末自体を識別できる MAC アドレスなどを利用して受信端末を登録する必要があると考えられる.

今後は，緊急速報システムで受信端末が無線ネットワークから離脱, 再接続したときに IP アドレスが変化した場合の実験を行う予定である.

参　考　文　献

[1] 財団法人国土技術研究センター ：意外と知らない日本の国土, 入手先 http://www.jice.or.jp/knowledge/japan/commentary09/ (参照 2017-10-19).

[2] 総務省 ：情報通信白書, 平成 29 年版, (2017).

[3] 気象庁 ：気象庁｜緊急地震速報｜緊急地震速報について, 入手先 http://www.data.jma.go.jp/svd/eew/data/nc/ (参照 2017-10-19).

[4] 小林孝輔, 松田勝敬 ：緊急地震速報受信端末のソフトウェアテストベッドの研究・開発, 平成 25 年東北地区若手研究者研究発表会講演資料, pp.227-228（2013）.

[5] 阿部峻弥, 松田勝敬 ：タブレット端末による緊急地震速報受信端末の機能拡張, 平成 27 年東北地区若手研究者研究発表会講演資料, pp.285-286（2015）.

[6] 松田勝敬, 銭谷英李, 角田裕 ：無線ネットワークにおける接続確認通信に関する検討, 信学技報, CS2017-42（2017）.

[7] 総務省消防庁 ：J アラートの概要, 消防庁, 入手先 https://www.fdma.go.jp/html/intro/form/pdf/kokuminhogo_unyou/kokuminhogo_unyou_main/J-ALERT_gaiyou_h28.pdf（参照 2017-8-10）.

[8] R. Braden : Requirements for Internet Hosts - Communication Layers, RFC1122, (1989).

[9] M. S. Rahman, Y. S. Uddin, M. S. Rahman and M. Kaykobad, : Using adaptive heartbeat rate on long-lived TCP connections, 2016 International Conference on Network-

ing Systems and Security (NSysS), pp. 1-9 (2016).

[10] J. Moy, : OSPF Version 2, RFC2328, (1998).

[11] D. Katz and D. Ward, : Bidirectional Forwarding Detection (BFD), RFC5880, (2010).