大規模災害時のインターネット非接続環境における情報共有システムの提案及び仮想環境下の実装

理学専攻・情報科学コース YU HUI (ウキ)

1 はじめに

インターネット及びスマートフォンの急速な普及に伴い，その関連技術及びアプリケーションが現代生活に不可欠な一部分になった．日常時であっても，災害時であっても，情報の収集手段として，電子メール，SNS 等のインターネットを介する方法が考えられている．近年，日本は自然災害が多く発生している．災害時に，被災地のインターネットインフラが断片的に切断されることにより，インターネットが使用不能になる可能性がある．その上，インターネットに強く依存しているアプリケーションも使えなくなる．しかし，避難情報や生活一般情報等の支援情報を被災者へ伝達することが必要であるとともに，被災程度を支援者に報告することも不可欠である．そのため，本研究では断片的なネットワーク及び XMPP[1] を搭載したサーバを利用する．災害時の情報支援を目指し，情報共有システム及び接続認証手法を提案する．又，仮想環境下で，システムの実装実験や接続認証手法の評価実験を行う．

2 関連技術

XMPP とは，アプリケーションに対応可能な通信用オープン XML 技術である．全てのメッセージは XMLstanza を標準とし，パッケージされて転送される．Openfire とは，XMPP に基づくインスタントメッセージ用サーバの一つである．使用方法が簡単で，基本的な通信システム機能が付いており，プラグインがサポートできるため，拡張性が高い．

3 提案手法

3.1 情報共有システムの提案手法

図 1 のように情報システムを提案する．ユーザは管理者と利用者の 2 種類を想定し，それぞれ支援者と被災者に対応している．サーバは管理サーバとサブサーバの 2 種類を想定し，それぞれ災害対策本部や避難所に分散して設置する．

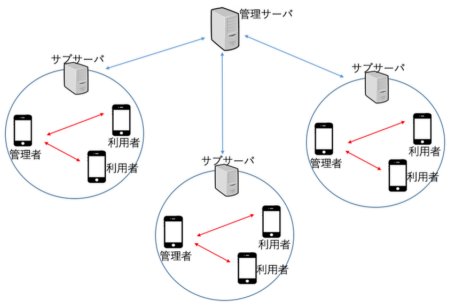

図 1 情報共有システムの提案手法

各避難所で，サブサーバはユーザにサービスを提供する．全てのユーザはアプリケーションでデータを収集する．そのため，「登録とログイン」，「情報管理」，「掲示板」や「チャット」の 4 つの仕組みを提案する．又，管理サーバはシステムの”管理者”とし，サブサーバの追加と削除や情報の共有を責任とする．

3.2 接続認証の提案手法

災害時の不安定な接続環境に対応するための接続認証方式が不可欠である．分散されたサーバ同士の接続セキュリティが守れる上，できる限り情報共有の可能範囲が拡大できるようにするため，以下のように接続認証手法を提案する．

(1) サブサーバは同期された「Server-List」のピアサーバ以外には通信しない．
(2) 管理サーバが利用可能な場合，サブサーバは管理サーバからの接続許可以外には従わない．
(3) 管理サーバが遮断された際に，サブサーバは「Server-List」によって，自動的に接続の回復を行う．

3.3 DTN を用いた情報運搬・共有の提案手法

接続認証手法はインターネットに強く依存しなくても，基礎なネットワークインフラが必要である．通信が途絶えた際に，情報共有ができなくなると考えられた．そのため，DTN を用いて，情報運搬・共有の方式を提案する．図 2 のように，ノードサーバを介し，サブサーバ 1 とサブサーバ 2 の間で，情報の運搬・共有を行う．

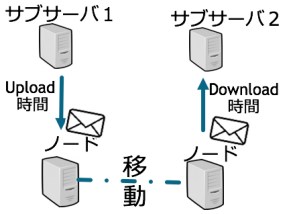

図 2 DTN を用いた情報運搬・共有の提案手法

4 実験

4.1 実験環境

図 3 のように，MacPC や PowerEdgeR430 を用い，実験環境を構築した．Virtualbox を利用し，管理者と利用者の端末機 2 台，管理サーバ 1 台とサブサーバ 9 台の仮想環境を構築した．GNS3 は仮想のネット空間と実際のネット空間が接続されている．

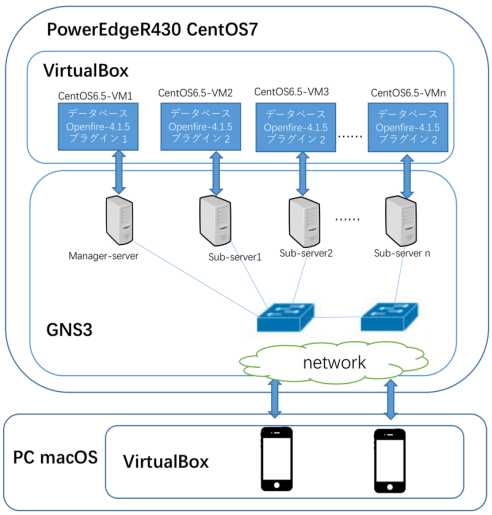

図 3 実験環境

4.2 実験結果

4.2.1 情報共有システムの細部

提案したシステムはアプリケーションでサービスを提供する．そのため，図 4 の通り，4 つの仕組みを作成

した．

図 4 の (a) は登録とログイン機能を示す．身元確認のため，登録の際に，管理者にするか，利用者にするかを確認する仕組みを作成した．管理者として登録した場合，特別な識別子を入力する必要がある．そして，図 4 の (b) のように，情報管理によってシステム情報が見えるようになる．又，被災者は自らの状況をシステムに報告する仕組みを作成した．この仕組みから，被災程度を把握することができるようになる．図 4 の (c) との (d) は掲示板とチャットの仕組みを示す．掲示板によって，管理者は避難情報，生活一般情報等の広く拡散させたい情報を被災者へ素早く転送することができるようになる．しかし，人によって必要な情報が違うため，掲示板に情報を載せるだけでは足りない可能性を考えた．その場合，問い合わせが必要となることから，チャット機能を作成した．チャットによって，一対一の通信ができるようになる．

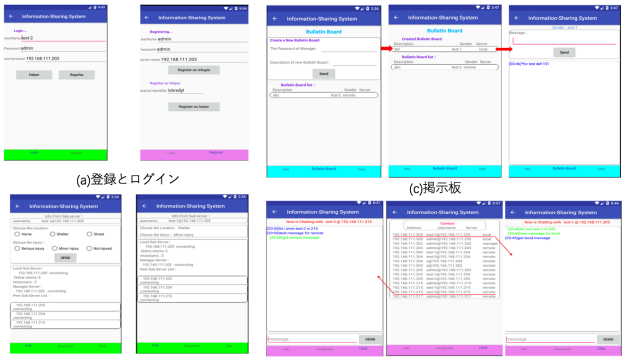

図 4　アプリケーションの仕組み

4.2.2　情報共有のウェブページ

図 5 に，情報共有のウェブページを示す．1 は「管理者リスト」であり，全ての管理者の情報と掲示板が見えるようになる．2 は「サブサーバの管理」である．この部分によって，サーバの追加や削除が管理できる．3 は「サーバリスト」であり，サーバの詳しい接続状況が見えるようになる．

情報共有のウェブページにより，被災対策本部の係員は詳しい接続状況と管理者の情報を把握することができるようになる．

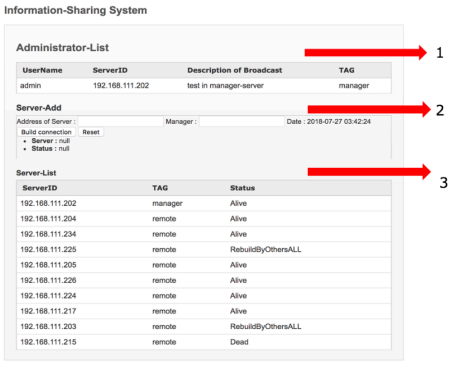

図 5　情報共有のウェブページ

4.2.3　接続認証の評価実験

非常時の不安定なネット環境に応じ，可能な状況を考えなければならない．表 1 のように，主な 4 つの可能性を考え，表を作成した．結果は接続環境が安定した後にシステム内に通信可能なサーバの台数として示す．

この表によって，管理サーバであっても，サブサーバであっても，インフラ等の原因により，実際に遮断された時だけ，通信の回復ができなくなる．他の場合には，システム内の通信が自動的に回復することができる．又，新たなサーバをシステムに追加する際に，管理サーバが必要である．

表 1　接続認証の評価実験

サーバの台数	管理サーバの遮断された場合				管理サーバの稼働している場合			
	全てのサブサーバが稼働している	サブサーバが制御されない	サブサーバが遮断された(n S)	新サーバがシステムに追加された	全てのサブサーバがが稼働している	サブサーバが制御されない	サブサーバが遮断された(n S)	新サーバがシステムに追加された(n S)
1M+6S	6S	-	(6-n)S	6S	1M+6S	1M+6S	1M+(6-n)S	1M+(6+n)S
1M+7S	7S	-	(7-n)S	7S	1M+7S	1M+7S	1M+(7-n)S	1M+(7+n)S
1M+8S	8S	-	(8-n)S	8S	1M+8S	1M+8S	1M+(8-n)S	1M+(8+n)S
1M+9S	9S	-	(9-n)S	9S	1M+9S	1M+9S	1M+(9-n)S	1M+(9+n)S

M：管理者サーバ
S：サブサーバ
n：問題が発生したサーバ

本接続認証手法によって，接続セキュリティが守られる上，状況が許す限り情報の共有範囲を限定せず，管理サーバが利用可能な場合には，拡大する可能性がある．

4.2.4　DTN を用いた情報運搬・共有の実装実験

仮想環境下の仮想マシンを利用し，DTN を用いた情報運搬・共有手法を検討する．ノードサーバが受信を準備してから，ファイルがノードに格納されるまでの時間はアップロード時間と想定する．目的地のサブサーバが受信を準備してから，ファイルが格納されるまでの時間はダウンロード時間と想定する．アップロード時間とダウンロード時間を合算したものは伝送時間と想定する．情報集のサイズを変化させ，実験結果は図 6 を示す．このグラフから，DTN 技術を用い，情報の運

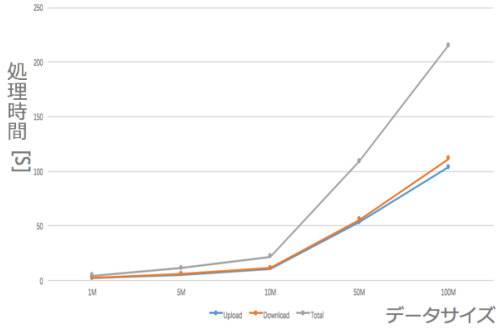

図 6　DTN を用いた情報運搬・共有の実験結果

搬・共有できることがわかる．そこで，災害によって，通信が途絶えた場合でも，本提案手法は有効に働くことが期待できるだろう．

5　まとめと今後の課題

災害時の大規模な配信需要に対応するため，被災者と支援者が繋がる情報共有システムを提案した．そして，各避難所同士で情報を交換するためや接続セキュリティと情報の共有範囲のバランスを取るため，接続認証方式を提案した．最後に，仮想環境で，システムを実装し，接続認証方式の評価実験を行った．今後は実物を利用し，システムの評価実験を行いたい．

参考文献

[1] Extensible Messaging and Presence Protocol (XMPP): Core, MARCH 2011, P. Saint-Andre,http://www.rfc-editor.org/info/rfc6120