IPv6 Reliable Multicast に対応したソフトウェア更新システムの開発

小鷹狩 晋　　†河野 英太郎　　†前田 香織　　††天野 橘太郎
E-mail: kodakari@nets.ce.hiroshima-cu.ac.jp

広島市立大学大学院　情報科学研究科
〒731-3194 広島市安佐南区大塚東 3-4-1
†広島市立大学　情報処理センター
††広島市立大学　情報科学部

概 要

常時接続環境において，セキュリティパッチをあてるなどインターネットサーバの安全対策はサーバ管理業務に必要とされるが，すべてのネットワーク利用者が適切な管理業務を行えるとは限らない．本稿では今後普及が想定される IPv6 ネットワーク上で，利用者個々にインターネットサーバを構築，保守管理する必要性の増加に備え，遠隔から保守支援することを目的としたシステムの開発について述べる．提案システムでは IPv6 環境で標準対応されているマルチキャストを利用し，遠隔地から多数のインターネットサーバを一括更新する．また，システムの評価についても触れる．

Development of a Software Update System using IPv6 Reliable Multicast

Susumu KODAKARI　Eitaro KOHNO　Kaori MAEDA　Kitsutaro AMANO

Graduate School of Information Sciences, Hiroshima City University
3-4-1 Ozuka-Higashi, Asa-minami, Hiroshima, 731-3194, Japan

Abstract

It is important to maintain the required software version for the network security, especially in the always connected environment to the Internet. However, all network managers cannot always do it. In the next Internet using IPv6, it is expected that more and more Internet servers increase and each user maintain them himself. In this paper, we describe our design and implementation of a management system to support to maintain Internet servers from a remote location. Our proposal use IPv6 reliable multicast to update software version. Also, we mention an evaluation of our system.

1. はじめに

現在のインターネットへの接続環境は，ダイヤルアップ回線や ISDN 回線のような狭帯域のものが主流であるが，光ファイバや DSL 技術を用いたインターネット接続サービスが低価格で提供されるようになり，比較的容易にインターネットへの広帯域常時接続環境を導入することが可能になった．それにより，多くの利用者が個人単位で独自にインターネットサーバを構築する機会も増えてくる．また，今後普及していく IPv6 インターネットではすべてのインターネット接続機器がグローバルアドレスを持ち，すべての端末が互いに双方向通信を行うことが可能となるため，これまで IPv4 プライベートアドレスしか利用できなかった組織でもインターネットサーバを構築することができる．

しかし，このような常時接続回線の導入は容易にインターネットを利用できるという利点と共に，常に外部からの攻撃にさらされる危険性を持っていると言える．そのため各組織の管理者はインターネットサーバを最新に保ち，か

つ適切なセキュリティパッチを適用するなどの管理作業を行い, 常に組織内のノードを安全に保つ必要がある. 適切な管理業務を行うには専門的な技術や知識を持った専任の管理者をおくことが望ましいが, 専門の管理部署をおくことの難しい教育現場や企業では, 専任のネットワーク管理者はなく, 通常業務と兼務して管理作業を行うことが多いため, 大きな負担を強いることになる. 本稿では, 広帯域回線で接続された多数のインターネットサーバを, 専門的な知識を持った専任の管理者が遠隔地からネットワークを介して更新作業を行うことにより, 現場の管理者の負荷を軽減させるシステムを提案し, そのプロトタイプを開発する. さらに実際の複数小学校のインターネットサーバの IPv6 対応化等の更新作業によって動作検証を行い, その性能について評価を行う.

教育現場などを対象にしたインターネットサーバの遠隔管理支援システムの例として文献[1]のようなシステムが提案されている. この管理支援システムはユニキャストで 1 対 1 通信を用いて遠隔管理を行い, 低速狭帯域回線を前提として送信データ量をいかに抑えるかについて検討されたものであり, 今後の広帯域ネットワークにおいて十分な仕様であるとはいえない. そこで筆者らが開発するシステムでは, IPv6 インターネット環境でインターネットサーバを構築する組織に対して, マルチキャストを利用して散在するインターネットサーバに更新プログラムを配送し, 管理単位毎のサーバを一括で更新作業を行い, 管理業務を効率化するシステムを構築することを目的とする.

2. システム開発の背景

2.1. 既存の Reliable Multicast 手法

すでに Reliable Multicast（高信頼マルチキャスト）手法は数多く提案されている. ファイル配信に適した高信頼マルチキャスト手法としては, MFTP[2], RMTPv3[3][4]などがあり, これらの高信頼マルチキャスト手法を利用したアプリケーションも開発されている[5].

一般的にマルチキャストを利用したファイル配送アプリケーションでは以下のような点が要求される.

- マルチキャストによる効率的な配送
- スケーラビリティ
- 配送ファイルの完全性の保証
- 送信者によるすべての受信者の受信確認

前述した既に提案されている高信頼マルチキャストプロトコルはこれらの要件を満たしており, 汎用的に利用できるが, その分実装が複雑になる. そこで, 本システムではこれらの高信頼マルチキャスト手法を参考に, 用途をソフトウェア更新に絞ってプロトコルを設計する. また, 本システムでは, マルチキャストファイル配送における信頼性を以下の点に限定して保証するものとする.

- 配送ファイルの完全性の保証は FEC[6]および再送の組み合わせで実現する
- 更新を要求するすべての受信者に更新プログラムを確実に配送するため, 送信者によってすべての受信者の受信確認を管理する

また本システムは以下を対象範囲とする.

- スケーラビリティとして 1000 台程度のマシンが接続されたネットワークを対象とする
- 確実にファイルが配送されることを目的とするためリアルタイム性は必要としない

2.2. IPv6 の普及

本システムは, IPv6 ネットワーク環境での利用を想定している. IPv6 は現在利用されている IPv4 を置き換える新しいインターネットプロトコルとして規定された. IPv6 には, 将来的なインターネットを想定した仕様が新しく提案されているが, 本システムでは以下の点について着目した.

- 広大なアドレス空間
- マルチキャストの標準利用
- 比較的強固なセキュリティ機能

今後, ブロードバンドインターネットの普及と共に, すべてのインターネット機器にグローバルアドレスが割り当てられる IPv6 が急速に普及していくと思われる.

現在の IPv4 インターネットでのマルチキャスト通信の位置付けはオプションであり, ネットワーク機器をマルチキャストに対応させるための特別な処理が必要である. IPv6 インターネットではマルチキャスト対応が標準であるため, 特殊な作業は必要なくマルチキャスト環境の構築およびマルチキャストアプリケーションの利用を容易に行うことができる.

また, IPv6 では配送データの暗号化などの

セキュリティ機能をもつ IPsec への対応も定められており, これを利用して配送データの秘匿性を確保することが可能である.

本稿で提案するシステムは，IPv6 マルチキャストを利用したファイル配送を行う．IPv6 マルチキャストも IPv4 と同様にトランスポートプロトコルに UDP を用いており, パケットロスなどが発生した場合に正常なファイルが配送できないと言う問題があるため, 信頼性の確保の手法として高信頼マルチキャスト手法を組み込み, 確実にファイル配送を行える機能を取り入れた.

3. ソフトウェア更新システムの概要

3.1. 基本構想

本システムは, 単一の管理方針に基づいて管理される範囲内の組織に設置されたインターネットサーバをソフトウェア更新の対象とする．例として，図 1 のような県や市の教育センターから管理下の小中学校に設置されているインターネットサーバのソフトウェアを一括更新する場合などが挙げられる.

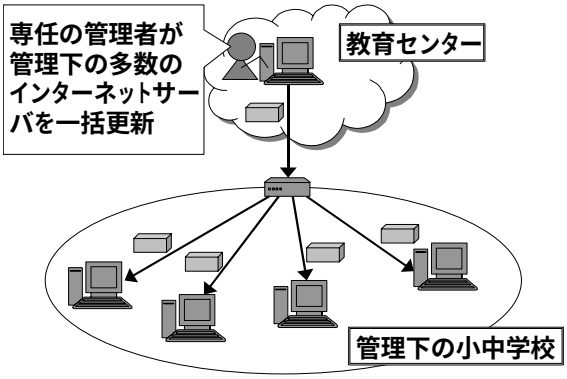

図 1. ソフトウェアの多地点一括更新の例

本システムの利用に際して, ソフトウェアの更新サービスを受ける多数のクライアントでは，以下の前提条件を満たすものと仮定する.

- IPv4 インターネット環境でルータ及び必要なインターネットサーバが正常に設定され動作していること
- 更新対象となる単一のマルチキャストグループに参加するクライアントホストの OS などが統一されていること

本システムのシステム構成を図 2 に示す. 本システムは 1 台の管理サーバと，複数台のクライアントホストから構成される．ここで

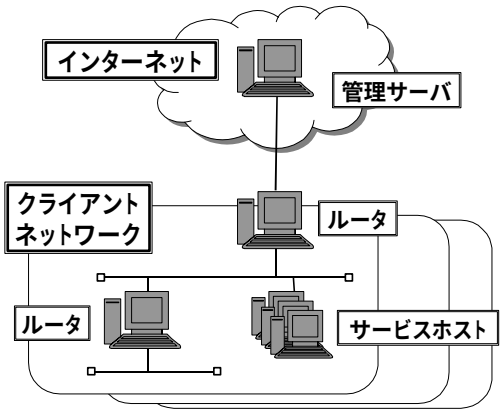

図 2. システム構成図

クライアントホストとは, クライアントネットワークにおけるルータやサービスホストの総称であり, サービスホストにはネームサーバや, メールサーバ，WWW サーバなどのインターネットサーバが動作するホストが含まれる. 管理サーバの専任の管理者は, 本システムを利用することで, 必要に応じてマルチキャストを用いてクライアントホストにソフトウェアの更新プログラムを配送し, ソフトウェアの更新処理を行う.

3.2. 本システムで提供する機能

本システムで提供する機能を以下に示す.

- OS の更新
- ソフトウェアの更新
- セキュリティパッチの適用
- システムの設定変更
  ソフトウェアのバージョンに対応した各種設定ファイルの更新
- ネットワークの環境設定
  ルータ機能の設定や IPv6 ドメイン名の自動登録
- 設定ファイルのバックアップ，リストア

さらに，本システムは IPv6 に対応していないネットワークに対しては, 簡易に IPv6 のネットワーク設定が行える機能を付加している. IPv6 に対応したネットワークでは，プラグアンドプレイ機能により, 機器をネットワークに接続した時点で自動的にアドレスが生成されるため, ネットワーク機器の追加が容易に行えるなどの利点がある.

開発対象の OS は IPv6 の対応状況から FreeBSD を想定しており，ルータ機能の設定などの機能は FreeBSD で動作する PC ルータを想

定している．また，一括更新に対応するソフトウェアには，KAME[7], Bind[8], Sendmail[9], Apache[10], Squid[11]を対象とする．

3.3. ソフトウェア更新処理

3.3.1. 更新処理の概要

本システムは図 3 で示す処理の流れでソフトウェア更新サービスを提供する．更新処理は 4 つの部分からなり，各部の機能は次のとおりである．

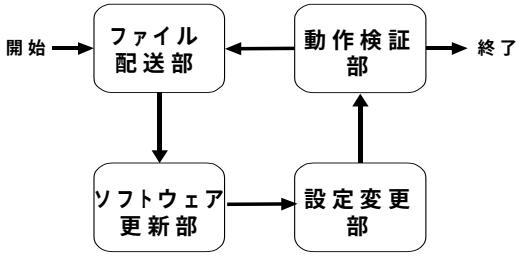

図 3. ソフトウェア更新モデル

(1) ファイル配送部
- 更新プログラムのマルチキャスト配送
- 高信頼マルチキャストプロトコルを利用した信頼性保証（FEC＋再送）

(2) ソフトウェア更新部
- OS の更新
  遠隔地から起動 OS を保守用の OS に切り替え，通常利用されるサーバ稼動用の OS を更新する
- ソフトウェアの更新

(3) 設定変更部
- ソフトウェア更新に際して，既存の設定ファイルを元に新しい設定ファイルに変換する

(4) 動作検証部
- 更新されたソフトウェアが要求を満たす動作をしていることを各クライアント毎，あるいは管理サーバからネットワークを介して検証する

これらの各機能部分の内，ファイル配送部および動作検証部は管理サーバとクライアントホスト間でネットワークを介して行われるが，ソフトウェア更新部および設定変更部の処理はクライアントホスト内で処理される．

3.3.2. ファイル配送部の詳細

本システムでは，ctrl セッションで制御コマンド（ASCII 文字列）が配送され，data セッションではコマンドに対応するバイナリデータが配送される．管理サーバ（Sender）からクライアントホスト（Receiver）への制御メッセージ，およびデータパケットは基本的にマルチキャストで配送され，Receiver からの応答はユニキャストで配送される．

ファイル配送部の前処理を図 4 に示す．

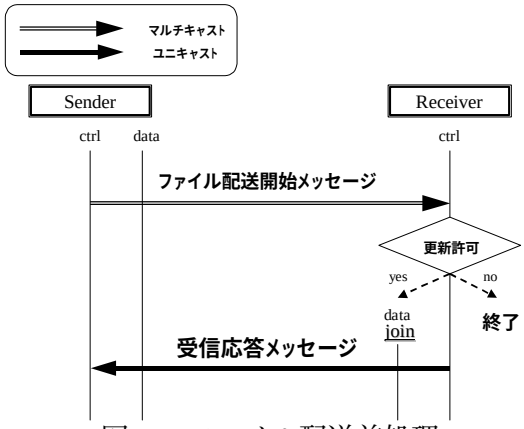

図 4. ファイル配送前処理

更新時にはファイル配送前に，Receiver 側でそのソフトウェア更新許可が設定されているか検査を行う．更新許可が出ていない場合には，Receiver は data セッションに join せず，処理を終える．許可が出ている場合には，Sender に受信応答メッセージを配送し，あらかじめ設定された data セッションに join する．Sender は Receiver からの受信応答メッセージを元に受信者リストを構成し，以後，そのリストを元に Receiver の管理を行う．

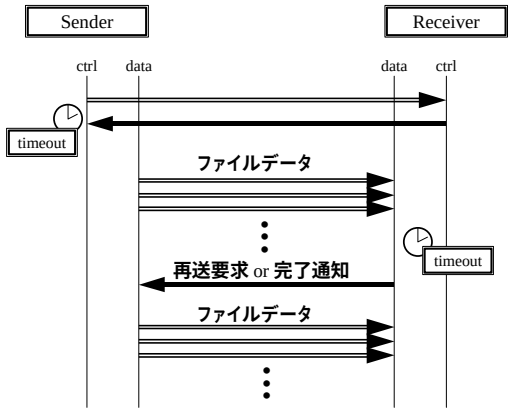

図 5. ファイルデータ配送

受信者リスト構成後，ファイルデータの配送段階に移行する．Sender はパケットロスに対

応するため, ファイルデータと共に冗長コードを含むパケットを配送し，Receiver 側で失われたパケットの復元処理を行う（図 5）．FEC による復元処理では対応できないパケットロスが発生した場合には，Receiver から Sender に再送要求通知が送られ，Sender はこの再送要求通知により次のファイル配送時に欠落パケットから再送を開始し, 再送要求がなくなるまで繰り返される．

一方，すべてのデータパケットを受信した Receiver は受信完了通知を行った後，個別にソフトウェア更新処理を開始する（図 6）．

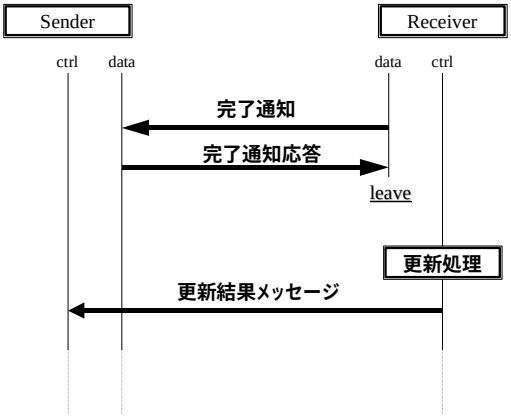

図 6.　ファイル配送後処理

Sender はすべての Receiver が受信完了したことを確認するとファイル配送を終了し, 更新処理の結果通知を収集する．

3.3.3.　データフォーマット

送受信される各データのフォーマットを以下に示す. 本システムでは以下に示すようなフォーマットに基づいたコマンド文字列およびバイナリデータが配送される．

1)　制御コマンド文字列
ファイル配送開始メッセージ：
コマンド名△ファイル名△ファイルサイズ△
ファイル ID△開始番号△終了番号△
ファイル誤り検出文字列
（例）UDATE△update.tar.gz△1234560△
3△1△2412△F5SA7EG2$#AWQ543A42

受信応答メッセージ：
コマンド名△ファイル名△受信ホスト名
（例）RECV△update.tar.gz△host.hogenet.jp

更新結果メッセージ：
コマンド名△ファイル名△状態メッセージ
（例）FIN△update.tar.gz△Message

2) バイナリデータ
図 7 は data セッションで配送されるバイナリデータのパケットフォーマットである．
それぞれのフィールドは以下のようになる．

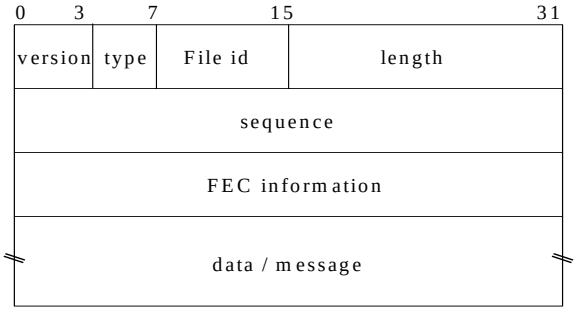

図 7.　送信データと応答パケットのフォーマット

フィールド名	ビット長	意味
version	4	プロトコルバージョン
type	4	データタイプ
length	8	データ長 (byte)
File ID	16	ファイル ID
sequence	32	パケットのシーケンス番号
FEC info.	32	FEC 情報
data		ファイルデータ

data セッションで配送される通知パケットは type フィールドに含まれる値によって識別される. 現時点で定義されているデータタイプの詳細は以下の通りである．

type	sequence	意味
0	0	未使用
1	0	完了通知
2	連続して到達したパケットの最大番号	再送要求
3	0	完了応答

4.　プロトタイプシステムの実装と評価

本システムの開発は，FreeBSD+KAME 上で行った. ファイル配送部および動作検証部の実装は C 言語を用いて行い，ソフトウェア更新部, 及び設定変更部でクライアントホスト内で処理されるプログラムに関してはシェルス

クリプト，Perl スクリプトなどを用いて実装した．本システムではセキュリティの確保に IPsec を用いることを前提としているためアプリケーションレベルでのセキュリティの実装については考慮しない．

本システムの評価は，実際のネットワークを利用して実験を行い，以下の項目について考察を行う．

- システムの動作検証
- ユニキャストとマルチキャストのソフトウェア更新におけるネットワーク資源の利用に関する負荷軽減や管理負荷軽減
- 本システム導入によるクライアントネットワークの IPv6 対応化における作業量の変化
- IPv6 高信頼マルチキャスト手法を用いたファイル配送プログラムでのエラー回復処理の性能
- IPsec の処理負荷が本システムに与える影響

動作検証実験は，「マメ de がんす」プロジェクト[12]のネットワーク回線を利用して，プロジェクト参加校に IPv6 ネットワークを構築して行う．

5. おわりに

本稿では管理者の管理負荷軽減を目的として IPv6 Reliable Multicast を利用した多地点一括ソフトウェア更新システムの設計とプロトタイプシステムの実装について述べた．現在，提案した仕様に基づいて IPv6 Reliable Multicast に対応したファイル配送部の実装を行なっている．今後はファイル配送部の実装が終わり次第，実ネットワーク上での動作検証実験を行なう予定である．

謝辞

本研究の一部は，広島市立大学特定研究(1803)の支援を受けて実施されている．ここに記して謝意を表す．

参考文献

[1] 相原玲二，石川真由美，西村浩二，``初等中等教育現場を対象としたインターネットサーバ”，情報処理学会研究報告，99-DSM-13，pp.25-30，May 1999.
[2] K. Miller, K. Robertson, A. Tweedly, and M. White, ``StarBurst Multicast File Transfer Protocol (MFTP) Specification”, Internet Draft, IETF, 1998. (work in progress)
[3] 山内長承，城下輝治，佐野哲央，高橋修，``高信頼同報バルク転送機構”，情報処理学会論文誌，Vol.39, No.6, pp.2009-2019, June 1998.
[4] T. Shiroshita, T. Sano, O.Takahashi, and N. Yamanouchi, ``Reliable Multicast Transport Protocol version 2”, Internet Draft, IETF, 1997. (work in progress)
[5] 木下真吾，長田孝彦，村主俊彦，城下輝治，``実システムへの適用性に優れたリライアブルマルチキャスト大規模情報配信システム”，マルチメディア，分散，協調とモバイル（DiCoMo 2001）シンポジウム論文集，pp. 423-428, 2001.
[6] R.E. Blahut, ``Theory and Practice of Error Control Codes”, Addison-Wesley Publishing Company, 1984.
[7] KAME Project, http://www.kame.net/
[8] Internet Software Consortium, http://www.isc.org/products/BIND/
[9] Sendmail Home Page, http://www.sendmail.org/
[10] The Apache Software Foundation, http://www.apache.org/
[11] Squid Web Proxy Cache, http://www.squid-cache.org/
[12]「マメ de がんす」プロジェクト，http://www.csi.ad.jp/activity/MAMEdeGansu/