L-003

次世代ネットワークにおけるセキュアなサーバレスコミュニケーションシステムの開発
Development of Secure Serverless Communication System in the Next Generation Network

近藤 靖司† 野中 雅康† 野澤 雅之†
Seishi Kondou Masayasu Nonaka Masayuki Nozawa

1. はじめに

IP ネットワークのコミュニケーションシステムでは、一般的にサーバコンピュータを用いてメンバの参加・退去などの情報を集中管理する。本報告では以後、これを「集中管理方式」と呼ぶ。集中管理方式では以下の問題がある。

(1)サーバに発生した障害がシステム全体に影響するため、サーバは信頼性や安定性の確保のために高コストとなる。

(2)グループに参加するメンバは、サーバの IP アドレスを取得して、各自のコンピュータに設定するといった煩雑な事前作業を伴う。

本報告では、次世代ネットワークプロトコルである IPv6 で標準化される IP マルチキャストを利用して、上記の問題を解決したコミュニケーションシステムを提案する。さらに、この IP マルチキャストを利用することによる、メッセージ配信に必要なトラフィックの軽減について報告する。

2. 本システムの特徴

図１に本方式の概念図を示す。本システムでは、グループを開設した端末が、そのグループに参加する他のメンバの参加・退去を管理する。本報告では以後、前者を「マスタ」、後者を「スレーブ」と呼ぶ。マスタとスレーブとは対等の立場で接続されており、マスタが停止する場合、チャットに参加しているスレーブがそれを認識して、マスタの権限がスレーブに委譲される。マスタの権限を委譲されたスレーブは新規マスタとして、他のスレーブを管理する。よって、本システムではマスタの障害がシステム全体に与える影響が小さい。本方式は IP マルチキャストを利用した以下の特徴がある。

(1)グループへの参加

スレーブがグループに参加するには、そのグループを開設しているマスタとの通信のために、マスタの存在およびその IP アドレスを自発的に確認する必要がある。そこで、スレーブはグループ検索のために本システムで規定した IP マルチキャストを、マスタおよびスレーブを問わず、全てのコンピュータに送信する。マスタのみが送信元のスレーブにこの応答を返信する。これにより、スレーブがマスタの存在およびその IP アドレスを確認することでマスタとの通信が可能となり、グループに参加することができる。

(2)トラフィック軽減

本方式では、スレーブから発信されたメッセージを、マスタを経由して他のスレーブに送信する。マスタから他のスレーブへの転送は表１に示す通信方法で行う。ここで「同リンク」「別リンク」とは、ネットワーク構成におけるマスタースレーブ間のルータの有無を区別するための定義であり、前者はルータが無いこと、後者はルータが有ることを表す。別リンクでの通信は IP マルチキャストを利用することによりトラフィックを軽減している。一方、同リンクでの通信は端末間で直接通信することによりルータの負荷を軽減している。本報告では、以後、これを「トラフィック軽減方式」と定義する。

表１　リンク種別と送信方法との相関

リンク種別	送信方法	目的
同リンク	ユニキャスト通信	ルータの負荷軽減
別リンク	マルチキャスト通信	トラフィック軽減

(3)メッセージ配信のセキュリティ

IPv6 で標準化される IPsec により、メッセージ配信にセキュリティを設定する機能を設けた。これはマルチキャスト通信も対象としている。IPsec の設定に要するセキュリティ情報をマスタが管理しており、スレーブは公開鍵暗号化方式を用いてマスタからセキュリティ情報を通信上秘匿して取得する。

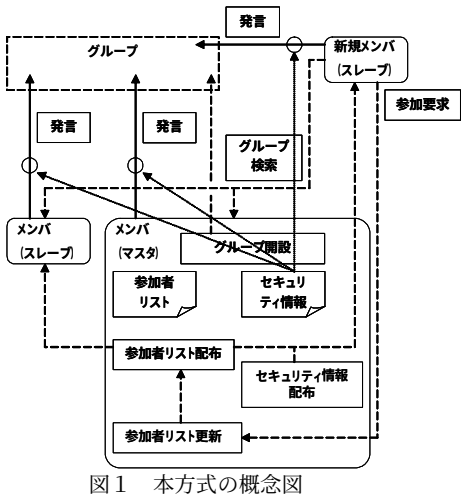

図１　本方式の概念図

3. 通信シーケンス

図２に本システムの通信シーケンスを示す。以下、これをもとにプロセスごとに処理の流れを説明する。

(1)グループ参加

① スレーブは、グループ検索の IP マルチキャストを送信し、この応答によりマスタを確認する。
② スレーブは参加したいグループのマスタへ参加要求を通知する。マスタはこれに応じて、参加者リストおよびセキュリティ情報を返信する。
③ マスタースレーブ間の IPsec を設定する。
④ マスタは参加者リストを更新して、それを他のスレーブに送信する。

(2)メッセージ配信

トラフィック軽減方式に従ってメッセージを配信す

†エヌ・ティ・ティ・コムウェア株式会社
NTT COMWARE CORPORATION

る。

(3)マスタ退去

①マスタは、次期マスタとなるスレーブにマスタの権限を委譲することを通知して、他のスレーブにマスタが変更になることを通知する。

②マスター全スレーブ間の IPsec を解除する。

③マスタ変更後、メッセージ配信を継続する。

(4)スレーブ退去

①退去するスレーブはマスタに退去要求を通知する。

②マスタは参加者リストを更新して、それを他のスレーブに送信する。

③マスター退去スレーブ間の IPsec を解除する。

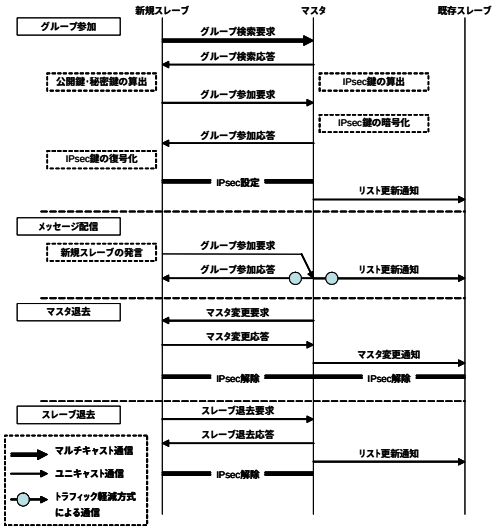

図２　本方式のシーケンス図

4. 実装

本システムを、FreeBSD4.7 上で実装した。なお、IPv6 の機能は、KAME プロジェクト[1]が発行している KAME kit を OS に反映させることにより性能を向上した。実装を通して、本方式が正しく動作することを確認した。

5. 考察

メッセージ配信プロセスのネットワーク負荷の論理式を表２に示す。ただし、集中管理方式ではメッセージがサーバを経由しないで直接メンバ間で通信すると仮定した。表２の本方式で、①はスレーブからマスタへのメッセージ送信、②はトラフィック軽減方式によるマスタからスレーブへのメッセージ転送を表す。

表２をもとにシステム全体での本方式と集中管理方式とのネットワーク負荷の差分の論理式を式(1)に示す。

式(1)

$$Diff = \underbrace{M + U * Cm}_{①} + \underbrace{\{U * P + (M + U * Cs) - U * (C-1)\} * S}_{②}$$

Diff　(本方式での負荷) － (集中管理方式での負荷)

Cm　本方式でのマスタ数

ただし、マスタ退去プロセスは本方式に特化しているので対象外として、スレーブ退去プロセスは両方式で負荷は同じであるので、式(1)に影響を与えない。式(1)の①はグループ参加プロセスにおいて、本方式でのグループ検索およびその応答による負荷の増大を示す。しかし、この負荷増大により、(a)ネットワーク上の全てのコンピュータの IP アドレスの検知、(b)ユーザがマスタの IP アドレスをシステムに投入するといった煩雑な設定、が不要となる効果が得られる。式(1)の②は表２に示したメッセージ配信プロセスでの差分である。式(1)をもとに、複数リンクに跨る企業内のネットワークでの意見交換に使用することを想定した場合の、スレーブの発言確率(P)と差分(Diff)との相関の一例を図３に示す。図３から集中管理方式と比較した本方式の負荷が、(a)発言回数が増加するに伴い低減すること、(b)スレーブの発言確率が低いほど急速に負荷が低減していること、がわかる。

表２　メッセージ配信プロセスのネットワーク負荷

方式	ネットワーク負荷
本方式	$\underbrace{U * P * S}_{①} + \underbrace{(M + U * Cs) * S}_{②}$
集中管理方式	U * (C－1) * S

U　ユニキャスト１パケット分の負荷

M　マルチキャスト１パケット分の負荷

Cs　本方式でマスタと同リンクのスレーブ数

C　集中管理方式でのメンバ数

P　スレーブの発言確率

S　システム全体の総発言回数

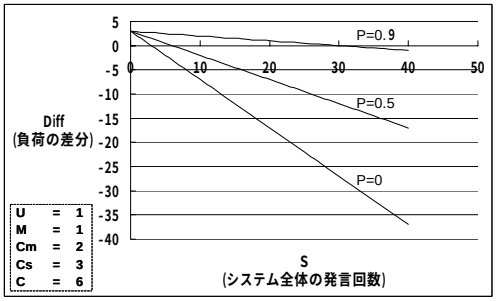

図３　スレーブの発言確率と差分との相関の一例

6. まとめ

本報告では、IPv6 で標準化される IP マルチキャストを利用して、サーバを必要としないコミュニケーションシステムを提案した。本方式と集中管理方式とのネットワーク負荷の相違を実測して、これを理論値と比較することにより、本方式の特性をさらに探究することが今後の課題である。

参考文献

[1] Webpage of Kame Project ：　http://www.kame.net/

[2] Marcus Goncalves, Kitty Niles 著：「IPv6 プロトコル徹底解説」日経 BP 社

[3] RFC2460 Internet Protocol, Version 6 (IPv6) Specification：http://www.ietf.org/rfc/rfc2460.txt

[4] RFC2401 Security Architecture for the Internet Protocol：http://www.ietf.org/rfc/rfc2401.txt