4-3　動的ファイアウォール制御を実現するグリッド通信ライブラリ

4-3 Grid Communication Library Allowing for Dynamic Firewall Control

長谷川一郎　馬場健一　下條真司
HASEGAWA Ichiro, BABA Ken-ichi, and SHIMOJO Shinji

要旨

現在のグリッド技術はファイアウォールに対する考慮が十分でなく、広域ネットワークに接続された資源に対して不必要なポートに対しても外部からの接続を許可する設定がされる傾向がある。そのため、一拠点におけるセキュリティレベルの低下が問題となっている。本研究では、各拠点のセキュリティレベルを低下させることなくファイアウォール内部の資源同士がグリッド上で自在に通信できる環境を実現することを目的として、連携した拠点間でアプリケーション要求に応じてファイアウォールの設定を動的に変更するための機能拡張をグリッド通信ライブラリに適用し、その有用性を示す。

Current Grid technologies tend not to consider firewall system properly, and as a result cause the decline in the security of Grid-sites on the wide area open network in practical use. This paper discusses the dynamic firewall control working with the Grid communication library to connect each resource on the Grid safely and flexibly. It shows a reduction of an administration load.

[キーワード]
動的ファイアウォール制御，グリッド通信ライブラリ，アクセス制御，管理コスト
Dynamic firewall control, Grid communication library, Access control, Administrative cost

1　まえがき

複数の組織によって計算資源（CPU やストレージ）が提供されて構成された環境では、すべての資源の管理を一元化して実施することは困難になる。特に、その環境にアクセスする人数が増えれば増えるほど資源の追加、削除、移動などが発生し、少数の管理者による手作業の管理は破たんする。現在の技術では資源の追加、削除などは管理者の手作業が必要であり、これが複数組織でのグリッド環境構築の大きな障害となっている。そのため、ユーザが自分の権限で資源の追加や削除が実施でき、自分で追加した資源を関係者以外に非公開にできるようなセキュリティ（アクセスコントロール）の手段の研究開発は、グリッドコンピューティングの普及に大きな意義がある。

本文では、グリッド技術におけるファイアウォールの設定に関する問題点を述べた後、**3** で動的にファイアウォールの設定変更を達成するための手段を提案する。本提案方式は、ファイアウォールの制御をトランザクション単位で行い、拠点への接続にかかわる IP アドレス及びポートを限定するため、セキュアな拠点間の連携を実現することができる。**4** で提案方式によりシステム管理者の煩雑なファイアウォール設定作業を削減できることを示す。

2　動的ファイウォール設定機構

2.1　従来技術

グリッド技術は様々な資源を組織を超えて相互に接続するために用いられる技術である。これは、

システムへの不正侵入の観点で言うならば、グリッド技術を用いて相互に接続された複数の拠点は、一度、ある拠点で外部からの不正侵入を許すと、連鎖的に不正侵入が達成されやすいということであり、サイバーテロのための踏み台や不正なファイル交換のための場に利用されるといった被害が拡大しやすいということを意味する。各拠点における外部からの不正侵入を防ぐためには、ファイアウォールの適切な運用・管理が重要である。しかし、各拠点のファイアウォールにおいて常に適切なルールが設定された状態を維持することは、次の三つのグリッド技術の特徴のために困難である。

(1) アプリケーションによっては外部拠点との通信に用いるポートがジョブの実行時に動的に決定される場合がある。
(2) 仮想組織は多数の拠点が相互に接続されたネットワーク形態になっており、その構成が常に同じであるということが保障されていない。
(3) ジョブの実行期間のどの時点で拠点間の通信が発生するかを予測することが不可能である。

すなわち、現在のグリッド技術はファイアウォールに対する考慮が十分でなく、広域ネットワークに接続された資源に対して不必要なポートに対しても外部からの接続を恒久的に許可するといった設定がされる傾向がある。そのため、各拠点において外部ネットワークからの不正侵入のきっかけを与えるようなセキュリティ状況となることが問題となっている。

セキュアに拠点間を接続するための既存技術の一例として、VPN を構築した上で資源共有を行う方法がある。しかし、VPN の構築はネットワーク層での設定を必要とするために、高度な技術を要する。また、多拠点間を連携する際の柔軟性に欠ける。本研究では、ユーザやシステムの運用者に対して高度なネットワーク技術を要求することなく、柔軟に多拠点間で資源を共有するための環境を構築できるようにするため、アプリケーション層による問題の解決を試みる。

2.2 グリッド技術におけるファイアウォールの設定に関する要求

拠点のセキュリティを維持しつつ、多拠点間で資源共有のための環境を構築する場合、資源提供者のファイアウォールの設定に対する要求は次のようなものである。

① オープンなネットワークに対してはできるだけ資源をさらさない。
② 拠点間の資源の共有に必要な接続は許可する。

特に、センサ系デバイスのようなアドホックな外部からのネットワーク接続を伴う資源を共有する場合、その接続・切断のたびに各拠点において常に適切なファイアウォールの設定を行うことは、管理コスト面の問題から困難である。オンデマンドで拠点の外部からのアクセスに対して資源共有のために必要な最小の許可だけをファイアウォールの設定に与え、仮想組織の中であればファイアウォールの存在を意識することなく資源を共有できるようにする技術が求められている。

3 提案方式

拠点間で発生する通信に応じてファイアウォールの設定を変更するため、ファイアウォールのルール変更の機会をサインオン単位やジョブ単位のような長期にわたる期間ではなく、トランザクション単位とする。

これを実現するため、資源共有の際に発生するトランザクションを正確に検出するための機能拡張を、グリッドミドルウェアの通信ライブラリに適用する方式を提案する。本提案方式は、拠点間の各々の通信の契機だけでなく、接続先の IP アドレス及びポートを検出することができる。なお、ファイアウォールの設定を変更するリモートサイトへのトランザクション情報の伝達は HTTP プロトコルを用いて実現する。

この提案方式を図 3 に示す。ここで、一つのトランザクションに対してグリッドミドルウェアが行う一連の処理は以下のとおりである。

(1) トランザクション発生の直前に接続元の IP アドレス及びポート番号といったトランザクション情報を収集、保存し、接続先のファイアウォールの設定を変更するためのリクエス

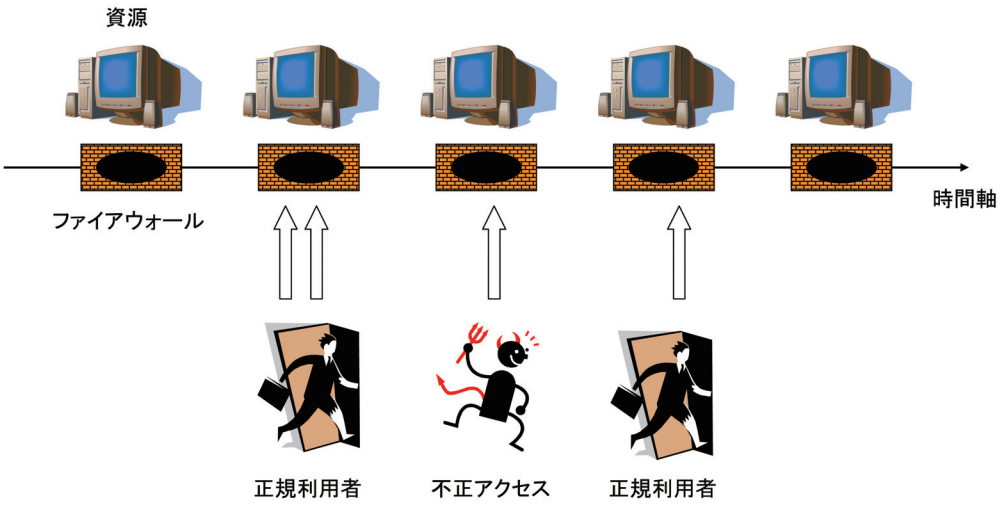


図1 既存のグリッド技術を利用する場合のファイアウォール設定状況

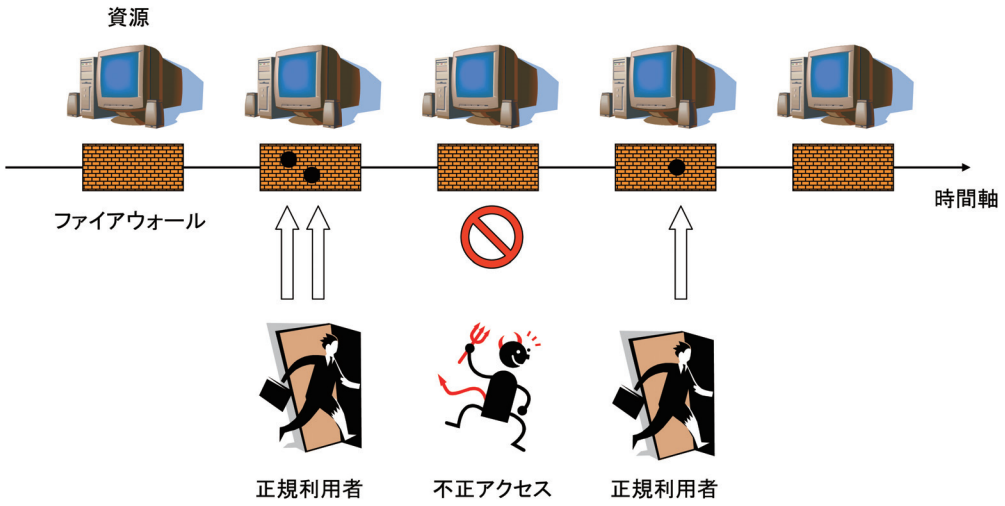


図2 トランザクション単位で行うファイアウォール制御

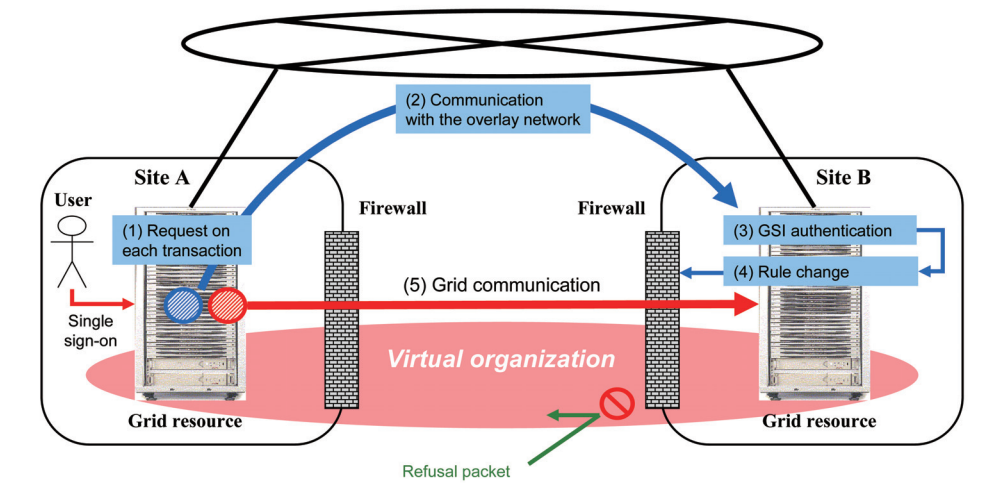


図3 グリッドミドルウェアによるファイアウォール制御

トメッセージとしてリモートサイトへ送信する。

(2) トランザクション情報を含むリクエストメッセージは、HTTP プロトコルを用いて接続先に伝達される。

(3) リモートサイト側でユーザ認証を行う。

(4) リモートサイト側で受信したリクエストメッセージに含まれるトランザクション情報を基にファイアウォールの設定を変更する。

(5) 接続元から接続先に対して接続を行い、本来の目的の I/O 処理を行う。

トランザクションの終了直後には、上の (1) で保存された情報を取り出し、上記 (2) ～ (4) を行い、リモートサイトのファイアウォールの設定を元に戻す。

本提案方式に基づくプロトタイプシステムの構成を図 4 に示す。ファイアウォール制御通信機構は、グリッド用 API・ファイアウォール制御通信発信機能・ファイアウォール制御通信着信機能を有する。グリッド用 API は、本システムをグリッドシステム (Globus Toolkit) に連動させるための API であり、グリッドシステムにより呼び出される。ファイアウォール制御通信発信機能は、グリッドシステムが他サイトに接続する場合に呼び出され、他サイトに設置された本開発ソフトウェアに接続し、他サイトのファイアウォールの制御を指示する。ファイアウォール制御通信着信機能は、他サイトに設置された本開発ソフトウェアから呼び出され、他サイトのグリッドシステムが自サイトのグリッドシステムへ接続できるよう、自サイトのファイアウォールを制御するためにファイアウォール制御機構を呼び出す。ファイアウォール制御機構は、ファイアウォール制御通信機構より呼び出され、自サイトのファイアウォールを制御する。また、これらの機構の状態表示のための GUI と、設定を行うための GUI を有する評価システムを構築した。

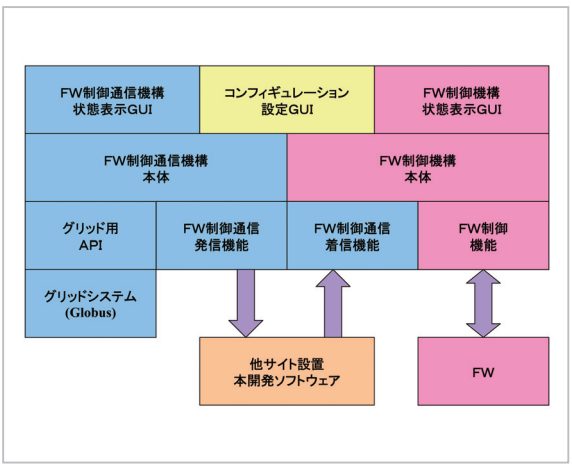


図4 ファイアウォール制御システム構成図

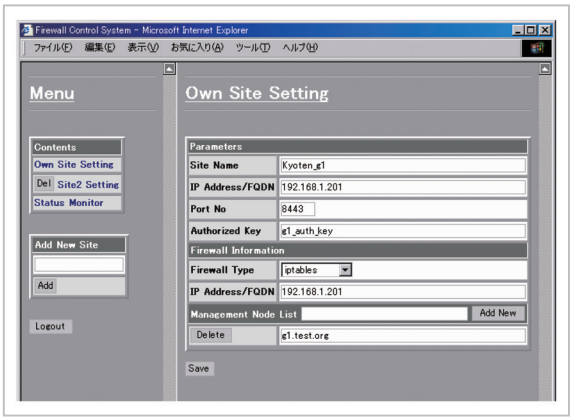


図5 設定を行うための GUI

4 評価

提案方式に基づくプロトタイプシステムは、接続元の要求に応じて拠点間の通信に必要なポート、アドレス及び期間を制限して接続先のファイアウォールの設定を動的に変更することができる。

Globus Toolkit に含まれる globusrun コマンドを実行したときのファイアウォール制御リクエストメッセージの送受信の様子を図 6 に示す。globusrun コマンドを実行したホストと gatekeeper が動作しているホストとの間で、相互

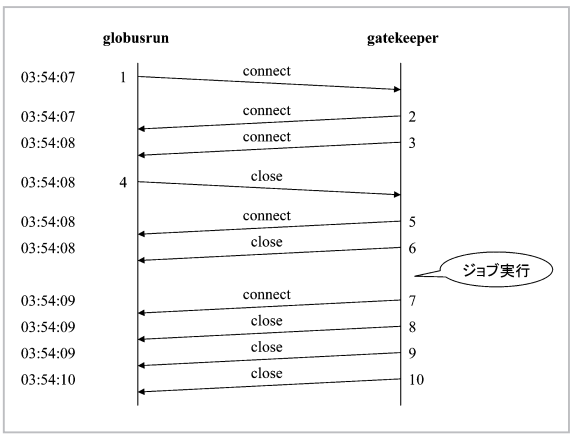


図6 globusrun コマンド実行時のファイアウォール制御リクエストメッセージ

に接続・切断のリクエストメッセージが交わされ、各々のリクエストに応じてそれぞれのホストで動的にファイアウォールの設定が変更される。1〜4 ではユーザ認証が行われており、5〜6 ではユーザジョブを転送している。gatekeeper 側でジョブの実行が終了した後、7〜10 でジョブの実行結果を転送している。

本提案方式では、ジョブの実行時にグリッドミドルウェアによってファイアウォール制御のための一連の処理を動的に行うため、各拠点のファイアウォールに対しては拠点間の通信に必要な最低限の設定だけを施すことができ、かつ、システム管理者はファイアウォールの存在を意識する必要がない。

従来の方法で、同等のことを実現しようとした場合、(1) ファイアウォールを制御できる機会は人間が管理できる事実上の最小の単位であるジョブ単位であること、(2) 接続許可の対象となるホストは、実際にどのホスト間で通信が発生するかをジョブ実行前に知ることができないのであれば、ジョブの実行が割り当てられるホストすべてが対象であること、(3) 対象となるポートは、ジョブ実行時の拠点間の通信に使用されるポートが事前に分からないのであれば、すべてのポート番号が対象であること、(4) ファイアウォールの設定はジョブの実行にかかわるすべての拠点について行われなければならないこと、(5) その際、ジョブを実行するユーザは、そのジョブが利用するすべての資源の管理者らと連絡をとり、ジョブを実行する予定時刻を知らせ、ジョブ終了時にはその旨を知らせること、(6) 各拠点のシステム管理者は、ジョブを実行するユーザからジョブの開始及び終了の知らせがあるまで待機し、連絡があれば速やかにファイアウォールの設定を変更すること、以上すべての処理が拠点のセキュリティを維持するために必要であり、これらを正しく実現することは実際には極めて困難であるということが予想できる。さらに、ジョブの実行が長期にわたる可能性もあることを考えると、ジョブの実行に伴う各拠点のセキュリティの悪化が懸念される。

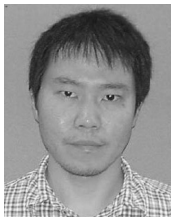
なお、本提案方式は、資源構成の変更にも柔軟に対応でき、システム管理者の煩雑なファイアウォールの設定作業を削減できるため、センサーデバイスを共有して利用するような場合に特に有効である。

5　むすび

セキュアな拠点間の連携を実現する動的ファイアウォール制御技術の開発とその有効性を検証した。提案方式である動的ファイアウォール設定機構は、連携した多拠点間でアプリケーション要求に応じてファイアウォールの設定を動的に変更するための機能拡張をグリッド通信ライブラリに適用することで、アドレス、ポート、期間を限定する細粒度のファイアウォールの接続許可の設定を可能にする。提案方式に基づくプロトタイプシステムでは、ミドルウェア層によるファイアウォール制御のための一連の処理が、ユーザにファイアウォールの存在を意識させることなく、多拠点間での連携をセキュアに実施できることを検証した。本機構により、従来は環境構築の複雑さゆえにちゅうちょされていた各種資源を活用したデータ処理が容易に実現でき、各種研究開発や実業務への幅広い適用が期待できる。

参考文献

1 The Globus Alliance, http://www.globus.org/
2 Ian Foster, Carl Kesselman, and Steven Tuecke, "The Anatomy of the Grid", Enabling Scalable Virtual Organizations, http://www-unix.globus.org/alliance/publications/papers/anatomy.pdf (2001).
3 Von Welch: Globus Toolkit Firewall Requirements: Version 7, http://www.globus.org/toolkit/security/firewalls/Globus%20Firewall%20Requirements-7.pdf (2005).



長谷川一郎（はせがわいちろう）
拠点研究推進部門大阪 JGNⅡリサーチセンター専攻研究員
グリッドコンピューティング

馬場健一（ばばけんいち）
拠点研究推進部門大阪 JGNⅡリサーチセンター専攻研究員　博士（工学）
広帯域通信網，コンピュータネットワーク、光ネットワークシステムの性能評価に関する研究

下條真司（しもじょうしんじ）
拠点研究推進部門大阪 JGNⅡリサーチセンター専攻研究員（大阪大学サイバーメディアセンター長・教授）工学博士
マルチメディア応用システム、Peer-to-Peer、インターネット、ユビキタスネットワーク、グリッド技術