けいはんな情報通信オープンラボシンポジウム2004
～オープンラボによる産官学連携の成果～

グリッドアプリケーションWGテーマ#1

仮想マシン技術によるセキュリティ機能
～Grid環境におけるセキュアな実行環境～

NECシステムテクノロジー株式会社
横山恵一

もくじ

1.研究の背景と目的

背景

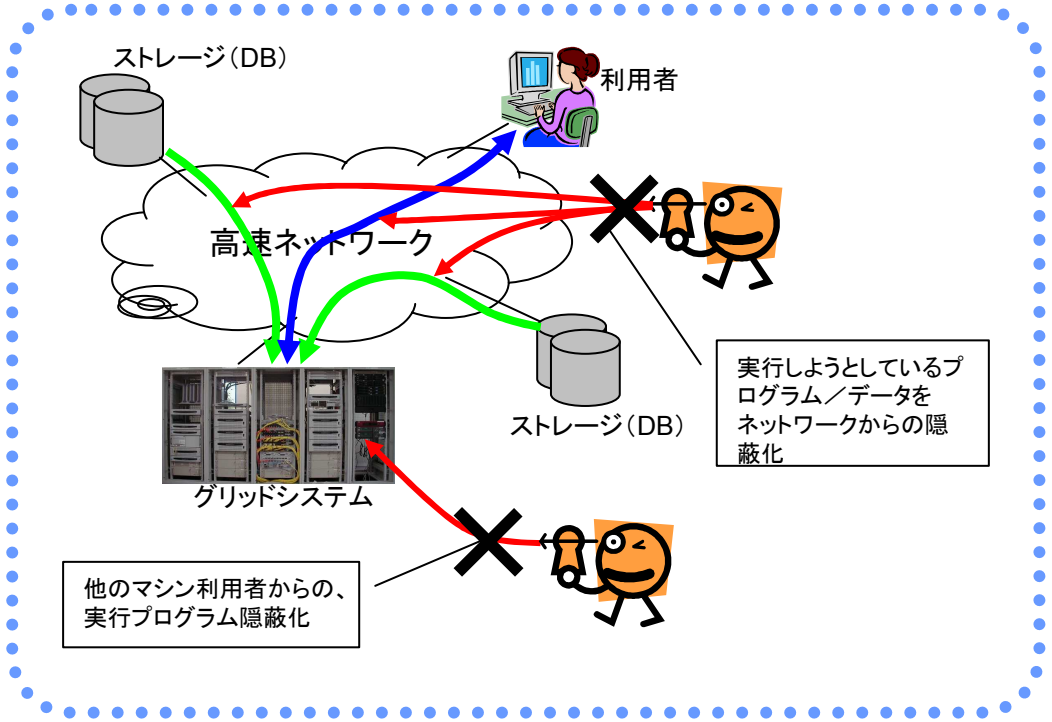
ネットワーク上に存在する、各種資源を活用して、プログラムを実行したい。

実行プログラム・データを第三者に知られる可能性がある

課題

目的

- 実行環境のセキュア化
  仮想マシンを用いた実行環境のセキュア化
- ネットワーク環境のセキュア化
  IPv6/Ipsecに準拠したP2P(PearToPear)技術を活用した通信のセキュア化



2.研究テーマと項目

- 研究テーマ
  IPv6/IPsecに準拠したGRID対応通信技術の開発
- プロジェクトの概要説明
  1）GRIDで接続された共同利用のハードウエア上で、機密を保持しながらプロセスを実行する機能を、バーチャルマシン技術により実現
  2）共同研究の推進の必要な、多地点に分散保管されたデータの共有や実験設備の遠隔利用を、セキュアな環境で行えるよう、IPv6／IPsecに準拠したP2P技術を開発

3.目標

２．１　技術面

１）機密を保持しながらプロセスを実行するための、バーチャルマシンの運用技術を獲得し、第三者であっても安全にプログラムを走行できるようにする。

２）多地点に分散保管されたデータの共有や実験設備の遠隔利用を、セキュアな環境で行えるよう、IPv6／IPsecに準拠したP2P技術による安全なファイアウォール越えを実現し、グリッド環境化での安全なプログラムやデータの通信を行うようにする。

２．２　ビジネス面

１）機密が確保されることにより、GRIDシステムを広範囲なビジネスに活用できる基盤(計算サービス、資源活用など)

２）セキュア環境下でのGRIDシステムを普及する基盤として、次世代ネットワークの普及に寄与する

２．３　政策面他

１）研究開発技術の標準化提案による国際貢献

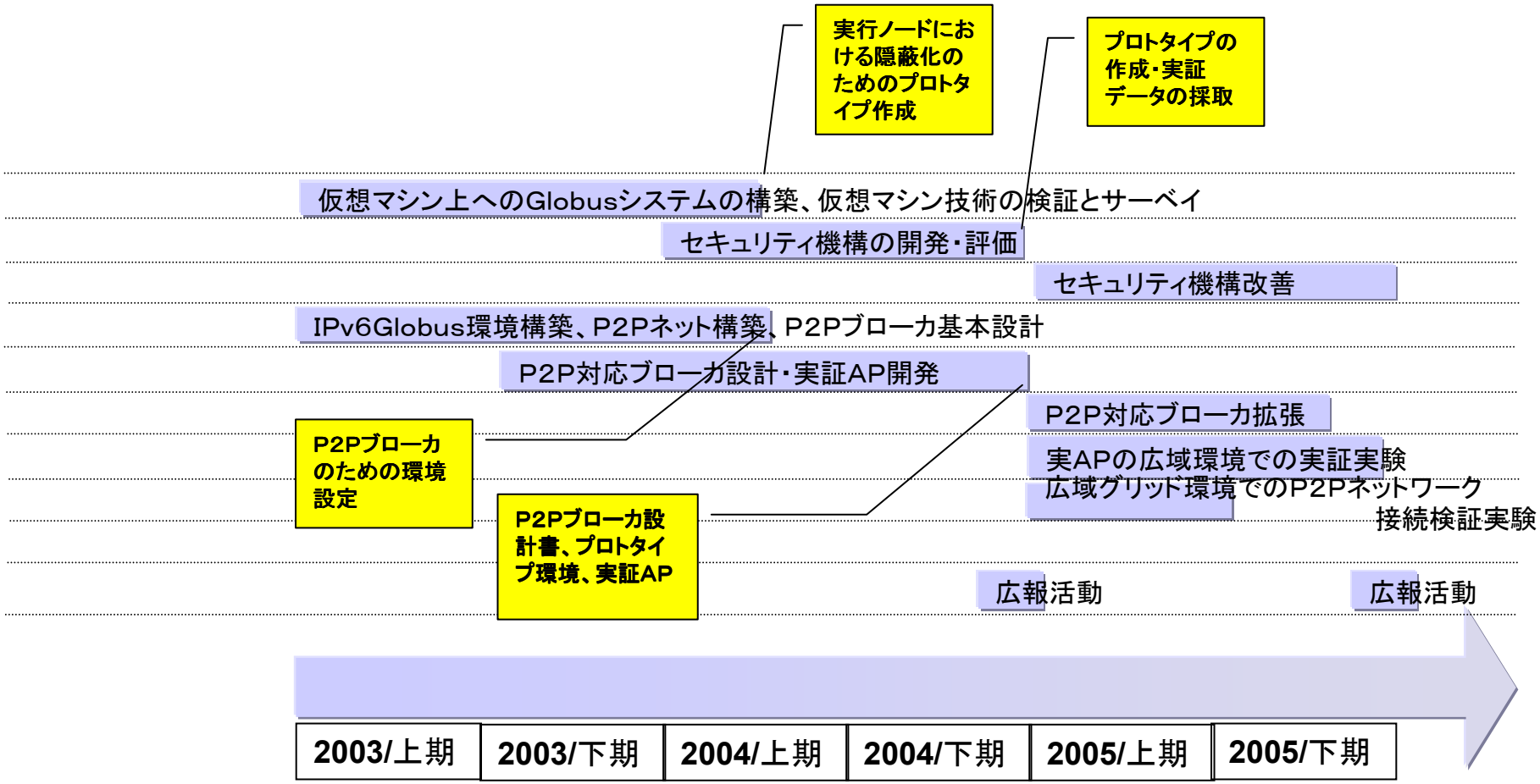
２）GRID分野における、国際的な競争力の確保

4.体制とスケジュール

□PJ体制

リーダ		高田　俊和（NEC）
	研究員	藤井　省吾（NECシステムテクノロジー）
	〃	齋藤　俊宏（〃）
	〃	横山　恵一（〃）

5. スケジュール


実行ノードにおける隠蔽化のためのプロトタイプ作成
プロトタイプの作成・実証データの採取
仮想マシン上へのGlobusシステムの構築、仮想マシン技術の検証とサーベイ
セキュリティ機構の開発・評価
セキュリティ機構改善
IPv6Globus環境構築、P2Pネット構築、P2Pブローカ基本設計
P2P対応ブローカ設計・実証AP開発
P2P対応ブローカ拡張
P2Pブローカのための環境設定
実APの広域環境での実証実験
広域グリッド環境でのP2Pネットワーク接続検証実験
P2Pブローカ設計書、プロトタイプ環境、実証AP
広報活動
広報活動
2003/上期
2003/下期
2004/上期
2004/下期
2005/上期
2005/下期

6.オープンラボ（1L）研究設備

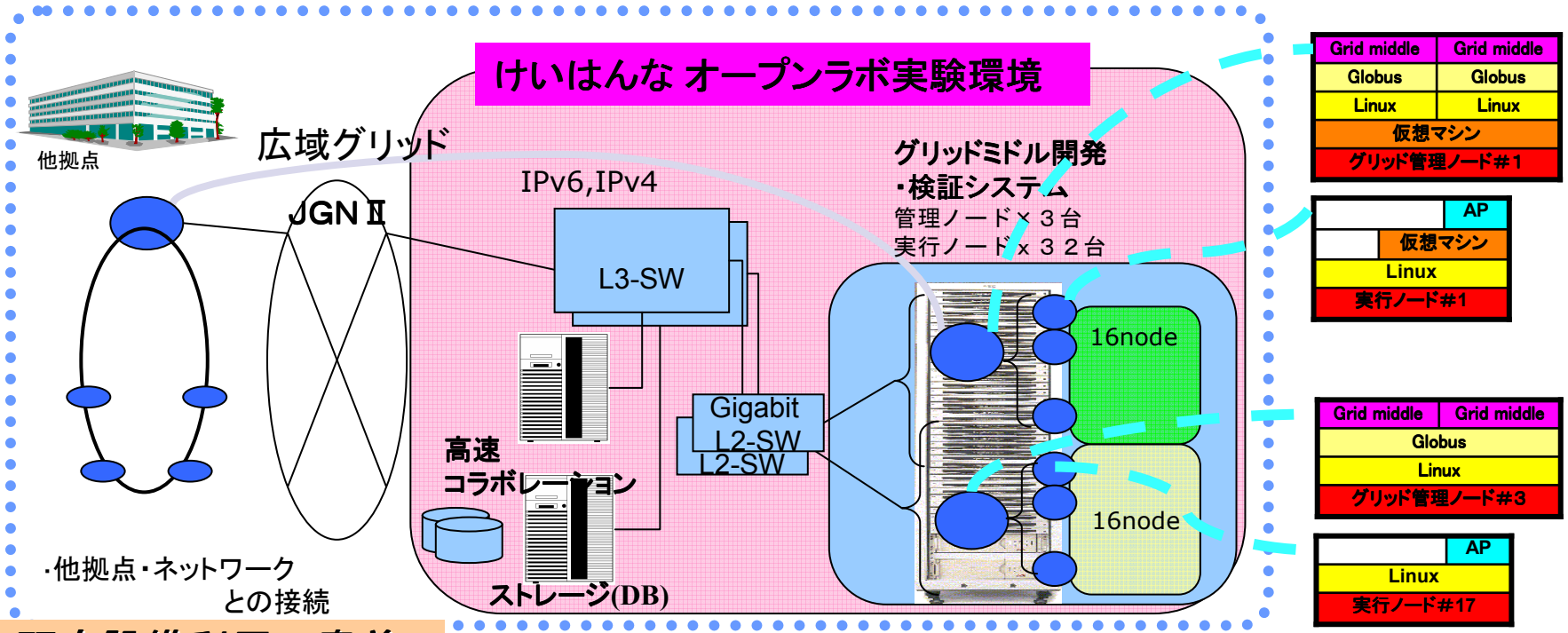
分散仮想ネットワークシステム

- 目的
  仮想的にネットワーク構成を変更し実験を行う設備
- 設置状況
  2004年3月に、1Lの部屋に設置。

外部ネットワーク接続状況

- 対JGNⅡ
  1Gで接続
- 接続プロトコル
  IPv4およびIPv6

7.オープンラボ研究設備と利用の意義



研究設備利用の意義：

- 計算資源の設定変更やデータ測定の容易さ
  →実験設備ならではの自由度
- JGNⅡの活用による他拠点との連携実験
  →容易なグリッドシステムの評価に高速ネットワーク
- 設備内での仮想的なネットワーク構成の設定
  →他拠点のネットワークポリシーに依存しない
  ネットワーク構成の設定

8.研究内容

仮想マシン技術によるセキュアなGrid環境実験

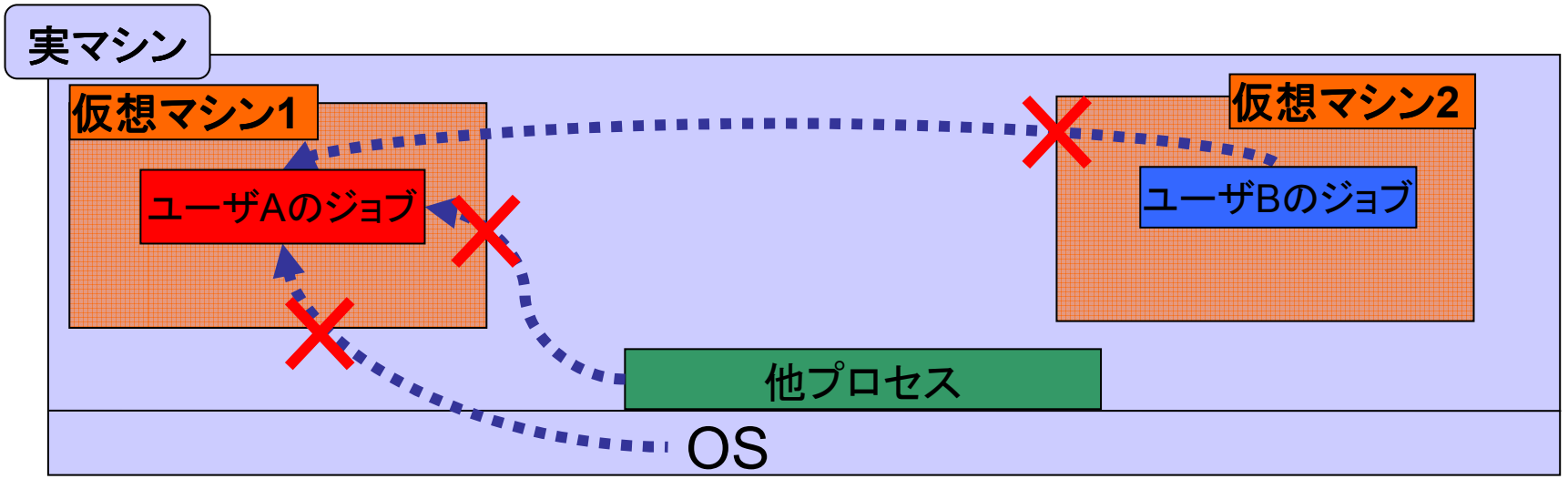
- 調査検討
  - 利用仮想マシンの検討と予備調査
  - 実装方式の検討
- 実装機能
  - 実行ノードにジョブ単位での仮想マシンUML(User Mode Linux)を実装
  - 管理ノードから、ジョブスケジューラ(OpenPBS)により実行ノードの仮想マシンにジョブを投入するシステムを構築
  - 管理ノードのグリッドミドルウェア(Globus)経由で、ジョブスケジューラを呼び出すGrid環境を構築
- 実験項目
  - 仮想マシンによるクラスタシステムの実行性能の測定と分析

ネットワーク環境のセキュア化

- 現在は調査段階

8.1 仮想マシン利用の目的と実験内容

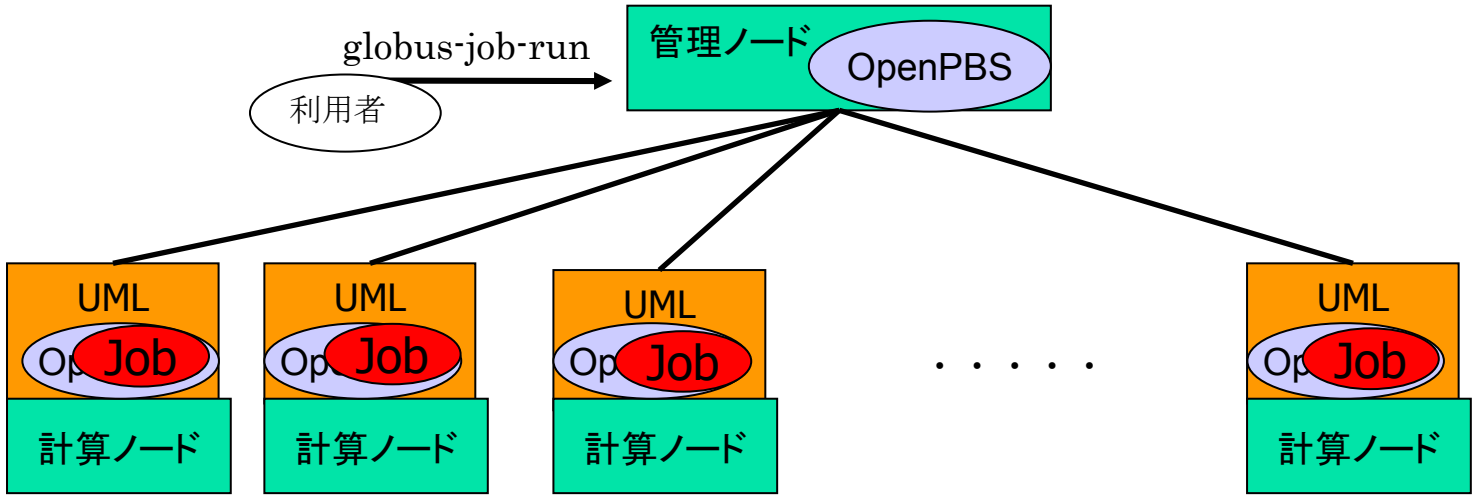
- ユーザプログラムの他プロセスからの隠蔽
  →セキュリティの検証



8.2 仮想マシンのセキュリティ・運用性向上

- 1UML上に1アプリケーション
  →1アプリケーションが1つのLinuxを占有
- スケジューラ(OpenPBS)を利用
  →スケジューラからUML上に直接ジョブ投入

8.3 仮想マシンによる実現方式



1. ホストOS起動時に自動的にUML起動
2. OpenPBSを使用しUMLへジョブ実行
3. ジョブ終了時にUMLを終了、初期化
4. UMLの再起動後、次のジョブ実行を待つ

9.評価結果

9.1 *UMLの評価(セキュリティなど)*

- そのままLinux上で走行するよりは強固なセキュリティ(完全とは言えない)
- UML自身のセキュリティ問題
- SMP未対応
- 使用メモリ量の制約
  →使用できるのは、475M
  ※メモリ拡大オプション(HIGHMEM)があるが、非常に遅い

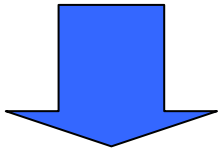
UMLの一層の改善が必要。

9.2 *性能面の評価(1)*

- 評価環境
  - CPU　　Xeon2.8G
  - OS　　Redhat7.3 kernel2.4.25
  - コンパイラ gcc2.96
  - MPI　　mpich1.2.5.2

9.2 *性能面の評価(2)～まとめ～*

- ネットワーク性能は、実マシンより大きく低下
- ネットワークのボトルネック
  - 実マシン→Gigabit Etherの性能
  - UML→CPU性能



UMLは、ネットワークに多くの計算資源を使用している

10.成果と課題

- ***仮想マシンを活用したクラスタ、グリッド環境の構築***
  - 実行ノードにジョブ単位での仮想マシンUML(User Mode Linux)を実装
  - 管理ノードから、ジョブスケジューラ(OpenPBS)により実行ノードの仮想マシンにジョブを投入するシステムを構築
  - 管理ノードのグリッドミドルウェア(Globus)経由で、ジョブスケジューラを呼び出すGrid環境を構築
- ***上記環境での実験により、セキュリティの構造を確認するとともに、実行性能を測定・分析し今後の課題が明確になった。***
  - 仮想マシンの性能については、他の仮想マシンによる検証も必要
    →UML固有の問題かどうかの判断材料必要
  - UMLによるセキュア化は、現時点ではまだ完全ではない。
    →対処にはUMLカーネルの改造が必要

⇒データ通信量が少ないプログラムでの活用可能

11.今後の実験～オープンラボの一層の活用～

- ***仮想ネットワーク構築環境を用いたセキュアなGrid グリッドネットワークシステム実験***
  - 各種リソース検索・通信セキュア化を行うため、オープンラボ設備を用いた仮想的なネットワーク環境構築し、グリッドミドルの研究・開発・実験を実施
  - さらに、JGNⅡを用いた他拠点との連携実験を実施
- ***仮想マシンを用いた実験の継続***
  - UMLの一層のセキュア化、スケーラビリティの向上。
  - 他仮想マシンでの実験(セキュリティ、性能)
  - 他のスケジューラの適用(ミドルウェアとしての成果)

謝辞

オープンラボ利用に際し、関係各位のご配慮に御礼申し上げます。

以上