IPv6によるスケーラビリティに優れたセキュアグリッド環境の構築

史宏宇[1]，武田伸悟[1]，長谷川一郎[2]
伊達進[1]，水野（松本）由子[3]，下條真司[4]

1. 大阪大学情報科学研究科
2. NECシステムテクノロジー
3. 大阪城南女子短期大学幼児教育科
4. 大阪大学サイバーメディアセンター

背景

- Grid Computing への期待
  - 大規模計算能力を科学問題へ応用
    - バイオインフォマティクス、製薬、医学など
  - 新ビジネスを創出
    - 数万台のパソコンでグリッドを構築、計算力を売る
- Grid におけるセキュリティ要求の高まり
  - 医療データ、軍事データ、創薬データを扱う
  - 機密性の保持
- IPv4アドレスの枯渇

グリッドの急成長に耐えうる、また、機密データを扱うことのできるセキュアなグリッド環境が求められている

目的

- グリッドにデータ保護機能を統合し、機密データを保護できるセキュアなグリッド環境を構築する。
  - 機密保護による**安全性**
  - IPv6による**スケーラビリティ**

グリッド環境を構築する技術

Globus

- グリッド環境の構築に必要なサービスを提供
  - 認証機構 (GSI: Globus Security Infrastructure)
  - 計算資源の管理機構
  - 通信ライブラリ
  - システム情報を検索する機能
- グリッド環境構築のツールとしてデファクトスタンダードになりつつある

アプローチ

- 既存のシステムへの変更を最小限にする
  - Globus がデファクトスタンダードである
- 運用コストを最小減にする
- アドレス空間の拡張

設計と実装

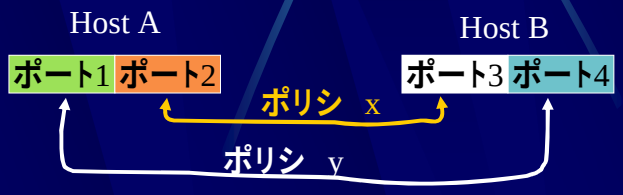
Globus へ暗号環境を提供

システムへの変更を
最小限に抑える

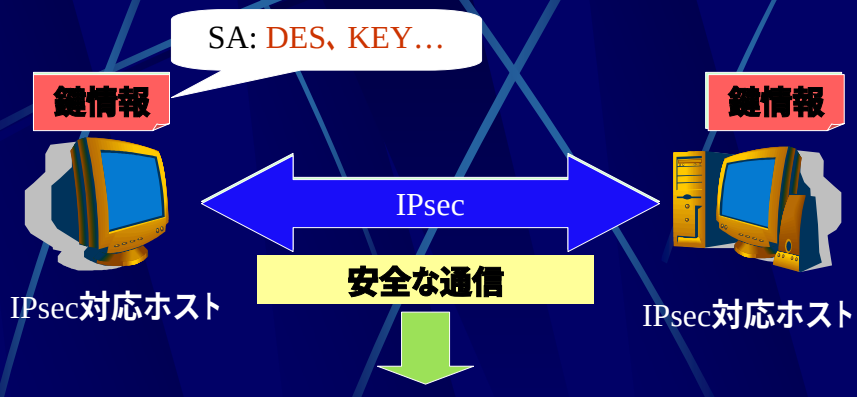
IPsec、IKE の利用

IPsec :IP Security

- IP 層での通信路暗号化プロトコル
- 特徴
  - アプリケーション層に依存しない
  - ポート-ポート間での暗号回線を実現
    → 柔軟なセキュア環境の構築が可能



IPsec の動作



鍵情報の更新には管理コストがかかる

IPsec の鍵交換による問題

- 数多くのホストがグリッドに参加している
  - IPsec の鍵交換はスケラービリティに欠けている

m: 鍵情報の更新回数

n: ホスト数

IKE: Internet Key Exchange

認証情報を共有する必要がある

IKE の問題点

- 認証情報（共有秘密鍵）を予め交換する必要がある
  - $O(n^2)$のコストがかかる

設計と実装

システムへの変更を最小限に抑える → IPsec、IKE の利用

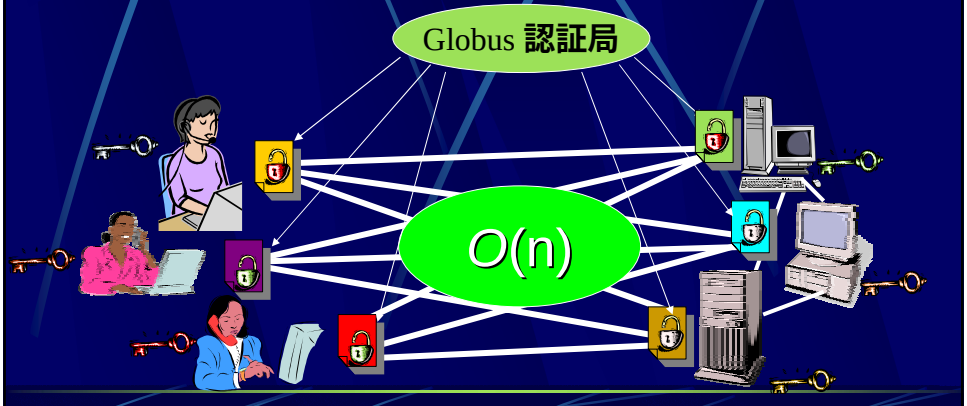
運用コストの低減 → Globus の認証機構 (GSI) と一元化

GSI：Grid Security Infrastructure

- 参加ホスト･ユーザの認証機構
- 証明書に基づいている公開鍵認証方式
  - スケーラビリティが高い

IKE+GSI

- 証明書による認証を用いる
- 運用コストを$O(n^2)$ から $O(n)$ まで削減



グローバルコンピューティングへの対応

- セキュリティの強化
  - P2P的な認証
  - IPv6 のグリッドへの導入
- IPv4 アドレス不足問題の解決
  - IPv6 のグリッドへの導入

現在は

NAT による解決：

Globus と NAT の併用が難しい

NAT は制限なく、計算資源の動的な結合を妨げる

設計と実装

システムへの変更を最小限に抑える	→	IPsec、IKE の利用
運用コストの低減	→	Globus の認証機構 (GSI) との統合
グローバルコンピューティングへの対応	→	IPv6 へ拡張

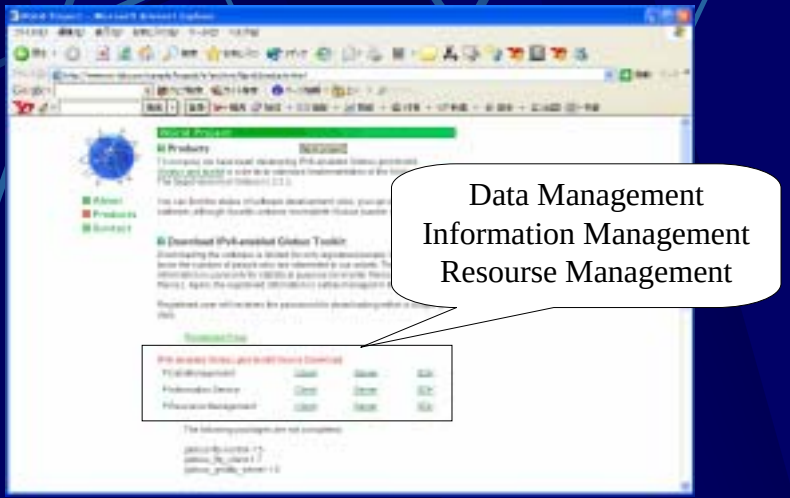
Globus を IPv6 への拡張

- 主に、通信機能を提供するモジュールを拡張
  - Globus_io、Nexus
- デュアルスタックノード上でも動作するように拡張

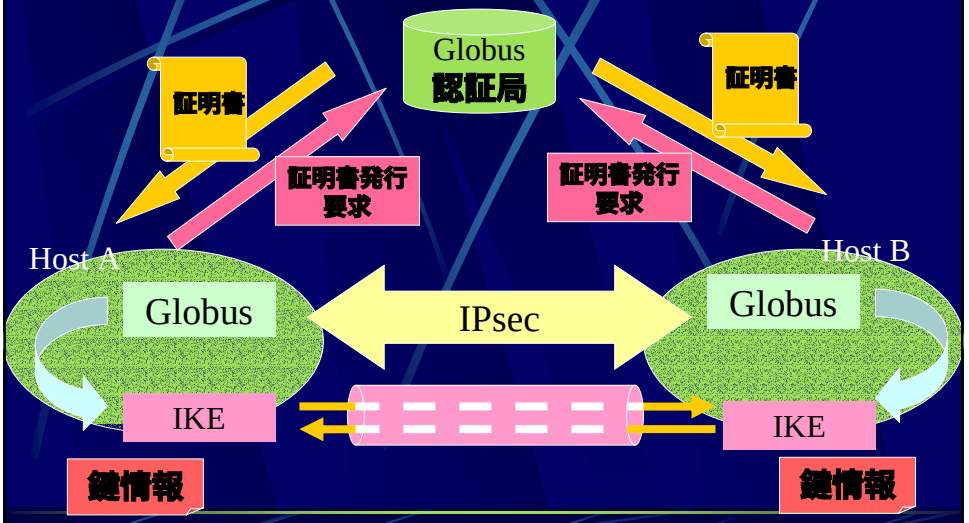
```
if(strcmp(listenerpf, "IPv4") == 0)
        hints.ai_family = PF_INET;
else if(strcmp(listenerpf, "IPv6") == 0)
        hints.ai_family = PF_INET6;
else
        hints.ai_family = PF_UNSPEC;

    hints.ai_flags = AI_PASSIVE;
    hints.ai_socktype = SOCK_STREAM;
```


IPv6 の実装の現状

http://www.biogrid.jp



セキュアグリッド環境



まとめ

- IPsec と IKE を用いて IPv6 上のセキュアなグリッド環境について提案した
  - 既存のシステムへの変更が少ない
  - 運用コストが少ない
  - スケーラビリティが高い
- Globus を IPv6 に対応させたことによって、巨大なアドレス空間を利用できる
- GSI、IPsec、IKE という三つのセキュリティ技術をシームレスに統合することによって、一貫性のある、ロバストなセキュリティを提供
- 提案したセキュアグリッド環境を用いることで、ユーザは安全に機密データを扱うことができる

今後の課題

- 実際の広域環境上でこのセキュアグリッド環境を適用し、暗号化通信のパフォーマンスの測定と定量的な評価
  - アプリケーション層の暗号化機能と比較
  - アプリケーション層の暗号化機能と併用する際のオーバヘッドの測定