秘匿性･信頼性を保証した広帯域自律分散ストレージシステムの構築（1/2）

（プロジェクト番号JGN-P341015）

研究機関：　大阪大学大学院工学研究科、高知工科大学情報システム工学科
大阪大学サイバーメディアセンター、医誠会病院

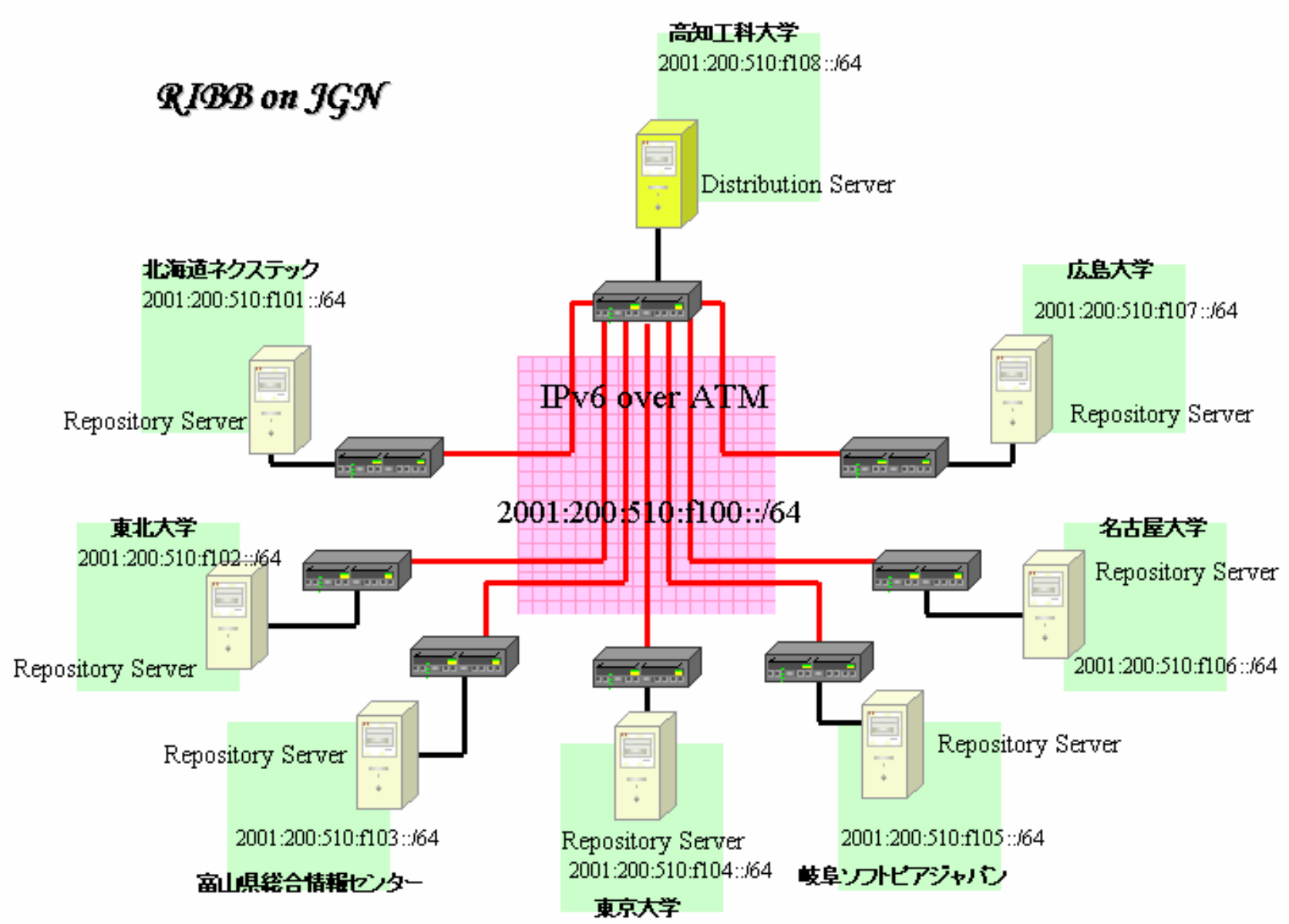
研究の概要：

秘密分散法(Secret Sharing Scheme: SSS)とエージェント技術を融合して、ネットワーク上に分散したストレージノードにより仮想的な1つのストレージシステムを構築する。

研究の目的：

医療、金融、行政等の領域においては、秘匿性・頑健性・信頼性に優れたストレージシステムの必要性がますます増大している。秘密分散法を用いたストレージシステムを構築すれば、重要データを分散管理することができる。そのため、秘匿性・頑健性の向上につながる。また、エージェント技術を使うことによりストレージシステムとしての使いやすさ･頑健性・信頼性を向上させることができると考えられる。そこで、本研究プロジェクトでは、暗号理論とエージェント技術を融合することにより、秘匿性・信頼性を保証した自律分散型ストレージシステムのための基盤技術の構築と実システムの開発をめざす。

実験機器構成：



秘匿性･信頼性を保証した広帯域自律分散ストレージシステムの構築（2/2）

（プロジェクト番号JGN-P341015）

研究機関：　大阪大学大学院工学研究科、高知工科大学情報システム工学科
大阪大学サイバーメディアセンター、医誠会病院

研究開発状況：

(1)　秘密分散法の開発[1]

・(k, n)しきい値秘密分散法の実装

　UNIX コマンドレベルで実装した。また、ライブラリの作成を行った。そして、UNIX ファイルシステムとして実装するための技術的要件を調査・整理した。

・(k, n)しきい値 SSS 計算を行うためのアルゴリズムの改良

　現在のコンピュータネットワークでの利用に適した、2 の拡大体上での (k,n)しきい値 SSS の実現のためのアルゴリズムを検討した。

(2) エージェントの仕様設計及び仮実装[2]

　ネットワークストレージ上に分散配置される秘匿データを管理するためのエージェント間通信プロトコルの策定を行った。まず、分散型ストレージシステムを実現するために最低限必要な機能の検討を行った。これらの機能をクライアントに提供するためのサーバエージェントの基本設計を行った。基本機能を実現するサーバエージェントを、分散マルチエージェントシステム開発環境（マルチエージェントネット）上に実装した。

研究開発成果：

[1] 菊池、舟橋、福本, “秘密分散法実用化への課題”, NORTH Internet Symposium 2002, pp.87-94, 2002.

[2] D. Hayashi, T. Miyamoto, S. Doi, and S. Kumagai, “Agents for Autonomous Distributed Secret Sharing Storage System”, Proc. of ITC-CSCC 2002, pp.482-485, 2002.

今後の予定：

- JGN で IPv6 による実験ネットワークの構築。
- SSS アルゴリズムの改良。
- エージェントシステムに SSS ライブラリを組み込み、目的システムの構築。
- 医療データベースのプロトタイプの構築

将来の展望：

　本研究プロジェクトで開発する仮想ストレージシステムを通して、従来よりもはるかに安全かつ災害に強く、ミッションクリティカルかつセーフクリティカルな業務の要求を満たすデータベースシステムを超高速ネットワーク上で実現することができる。