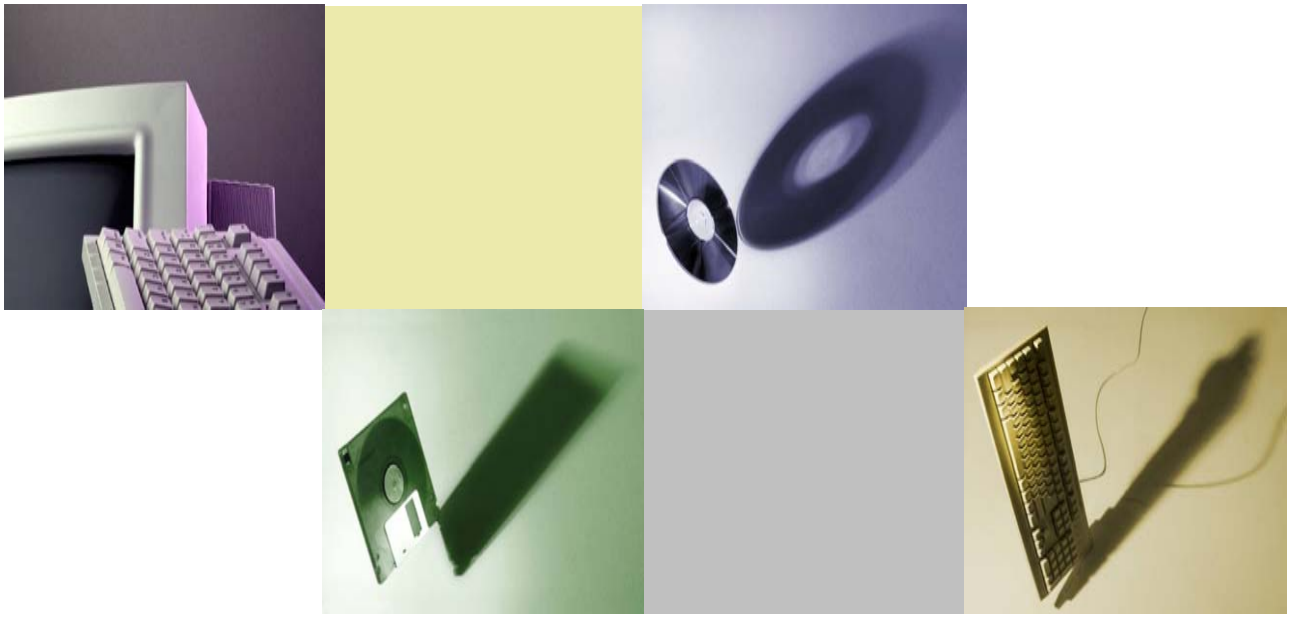
ネットワークシステムの安全性定量化に向けた新たな表現モデルとアクセス制御解析



◎金岡 晃（筑波大）、藤堂伸勝（筑波大）
加藤雅彦（IIJテクノロジー）、岡本栄司（筑波大）

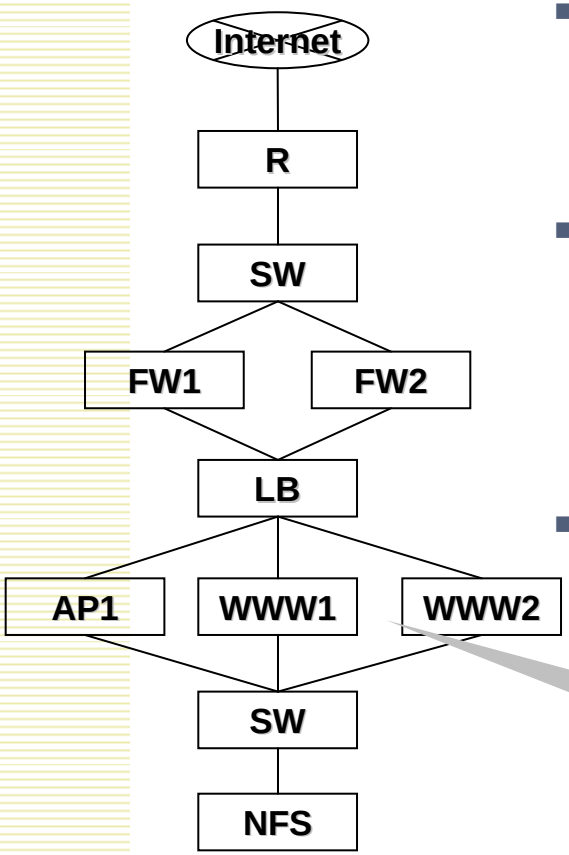
Outline

- ネットワークシステム設計時の考慮ポイントと現状
- ネットワークシステム表現モデルの提案
- 提案モデルによる実ネットワークシステム解析
- 解析用ツールデモ

本研究の目的と本論文の位置づけ

- **目的**
  - ネットワークシステムにおける安全な設計方法論確立のためのシステム定量評価
  - ネットワークシステム:
    - サーバやデータベース、ルータ、ファイアウォール、ロードバランサなど、各機能をそれぞれの機器で行って、全体として1つのサービスを提供するシステム
- **位置づけ**
  - 定量評価の基礎となるネットワークシステム表現モデルの提案と、提案モデルによるシステムの解析

ネットワークシステム設計時の考慮点と現状



現状の設計図例

- **ネットワークシステム構築において考慮されるポイント**
  - コスト、通信量、拡張性、アクセス制御、耐障害性、脆弱性の影響
- **最適化の困難性**
  - 小規模システムでさえ複雑
  - 現状は設計者の経験依存
  - **方法論や理論的アプローチが未開拓**
- **現状の設計における問題点**
  - 設計図と構築考慮ポイントの関連性が低い
  - 例：アクセス制御は適切にされるべきだが正確に反映されていない

WWW1-WWW2間の通信は？

各機器はそれぞれが持つ機能により特性が異なるが、それを1つの平面上に表現されているため

提案ネットワーク表現モデル

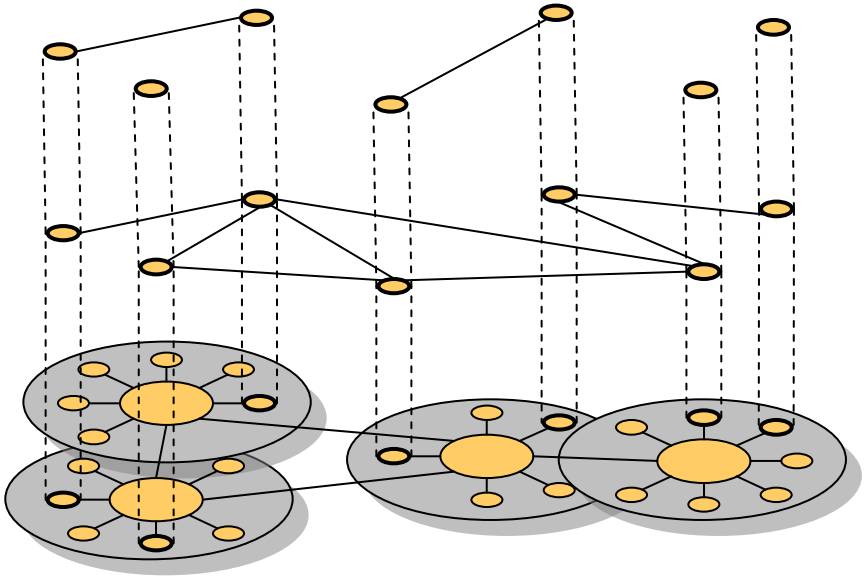
基本戦略

現状

物理的接続のみを反映した
ネットワーク表現

提案モデル

TCP/IPの階層ごとに作られる
論理ネットワーク
＋
階層ごとのネットワークの接続

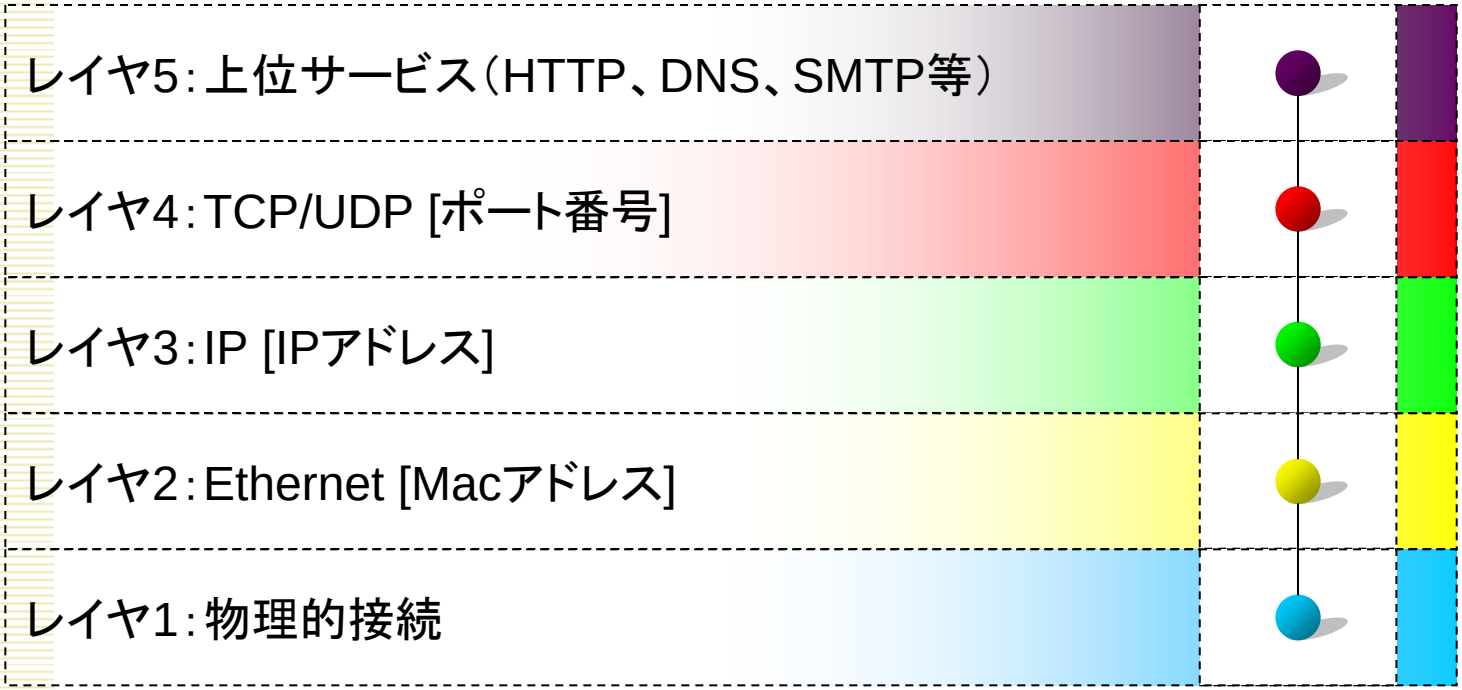


イメージ図

用語定義

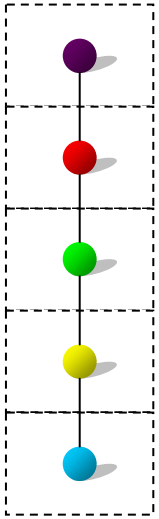
通信		情報の送受信
通信路		送信者（情報源）から受信者への情報伝達媒体であり、1つ以上のリンクにより構成される。
ノード		通信が行われる際の、送信者・受信者・中継者
レイヤ		同種情報が同種通信路で通信を行う際のノードとリンクの集まり
リンク		2つのノード間をつなぐもの
	レイヤ内リンク	同一レイヤにある2つのノードをつなぐリンク
	レイヤ間リンク	異なるレイヤにある2つのノードをつなぐリンク
モジュール		1つ以上のレイヤにまたがって機能を提供するもの
中継		当該レイヤの通信路を形成するにあたり、1つ下位のレイヤの通信路形成を決定する処理を行うこと

レイヤ定義とノード


レイヤ5：上位サービス（HTTP、DNS、SMTP等）
レイヤ4：TCP/UDP [ポート番号]
レイヤ3：IP [IPアドレス]
レイヤ2：Ethernet [Macアドレス]
レイヤ1：物理的接続

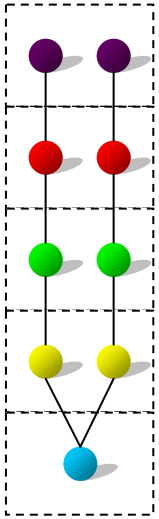
モジュール例

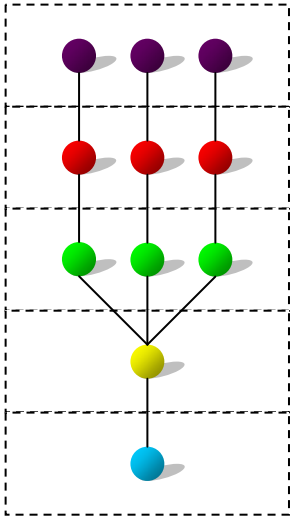
サーバ



単一のサービス
を提供するサーバ
（Webサーバなど）

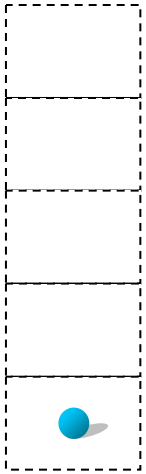
複数のサービスを
提供するサーバ
（Webサーバ
＋DBなど）

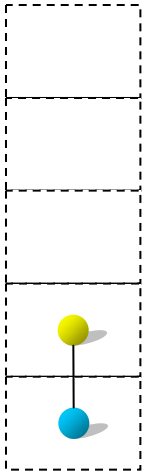


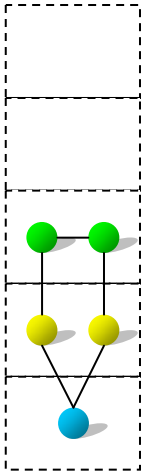


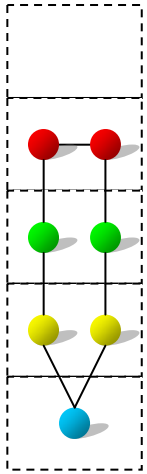
中継機器（機能）

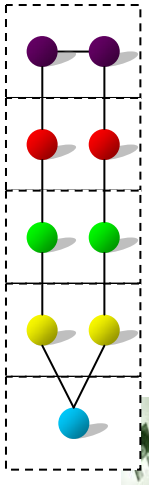
ハブ　スイッチ　ルータ　NAPT　プロキシ

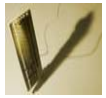




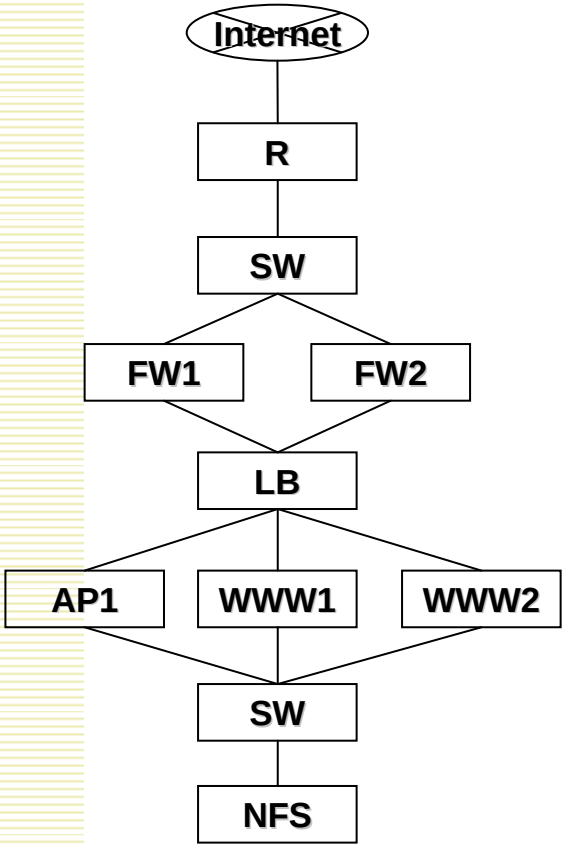




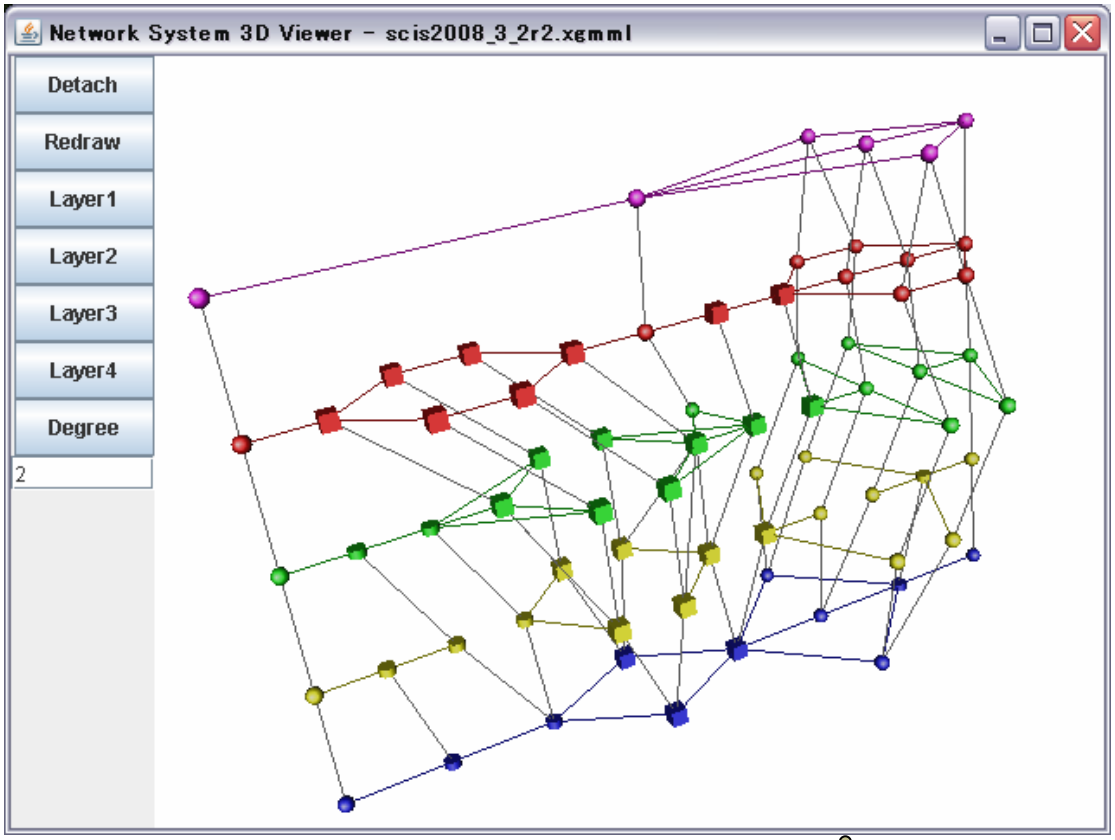




提案モデルによるネットワーク表現例



従来の表現



提案モデルによる表現

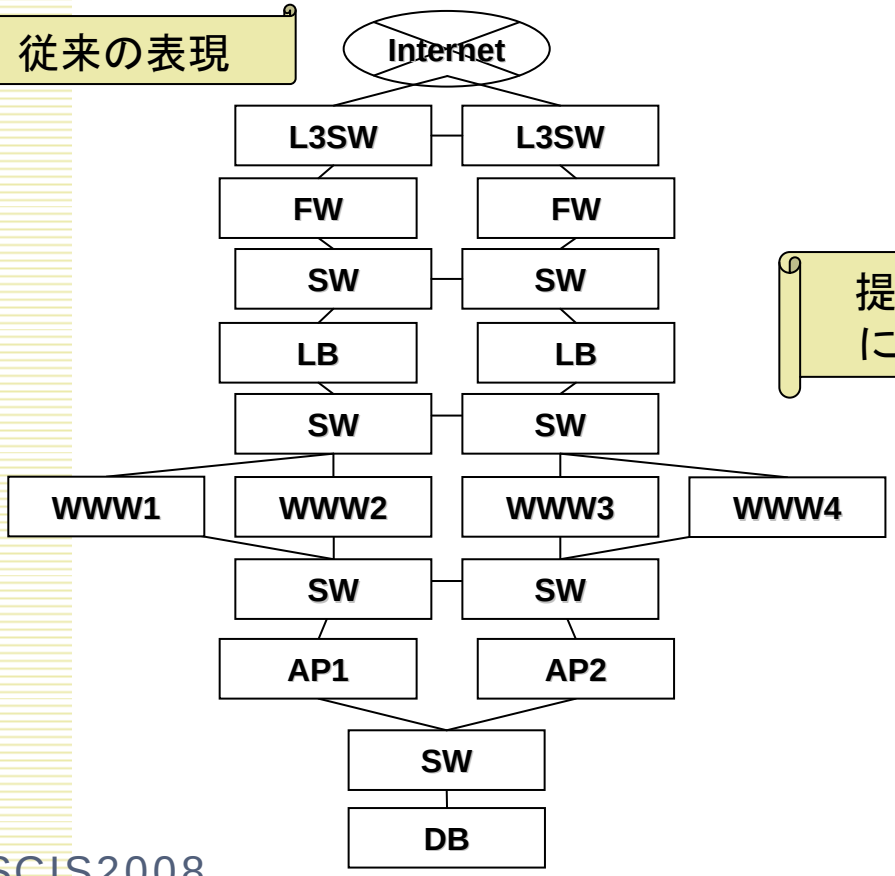
ネットワークシステム解析

- いくつかの例をもとにネットワークシステムを解析
- 解析
  - 各ノードの持つリンク数分布とアクセス制御状態の関係性
    - リンクの存在は通信可能な状態を表す
    - 同一ネットワークシステムにおいてアクセス制御状態の変化がリンク数分布にどういう変化をもたらすか
- 解析対象
  - 階層構造を持つネットワークシステム
  - フロント：Webサーバ
  - バックエンド：DB、アプリケーションサーバ

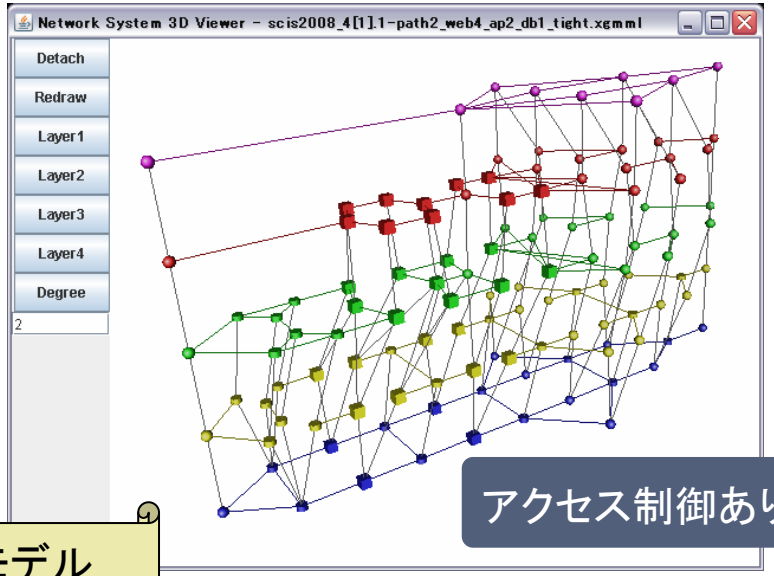
ネットワークシステム解析(1)

- **構成**
  - Webサーバ4台、アプリケーションサーバ2台、データベース1台

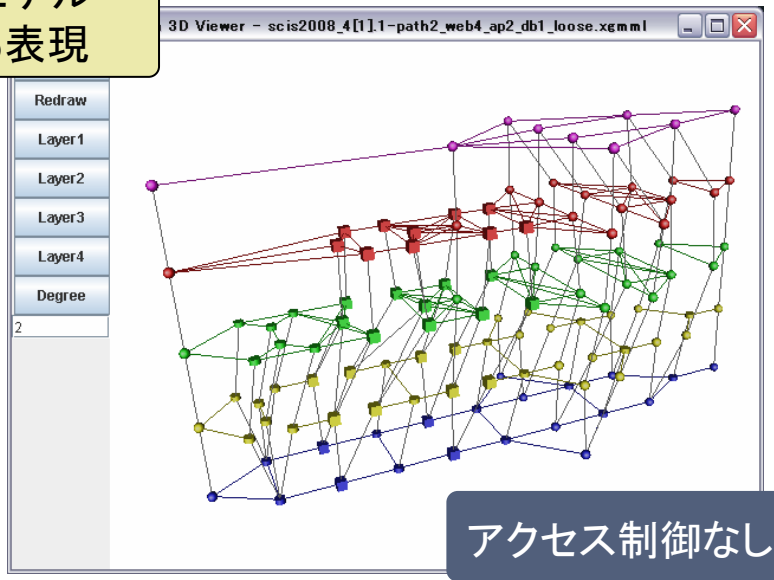
従来の表現



提案モデルによる表現

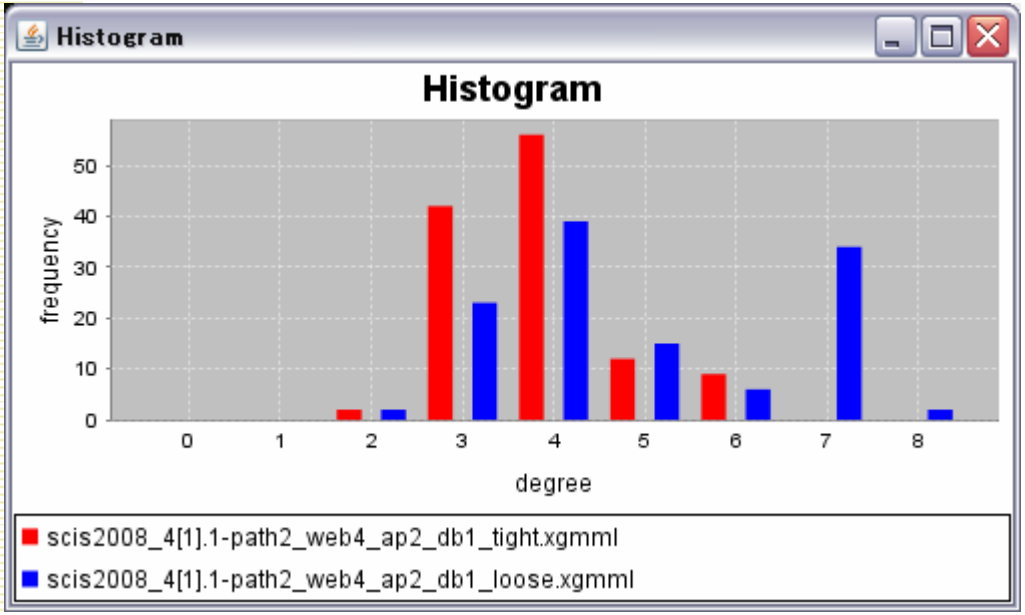


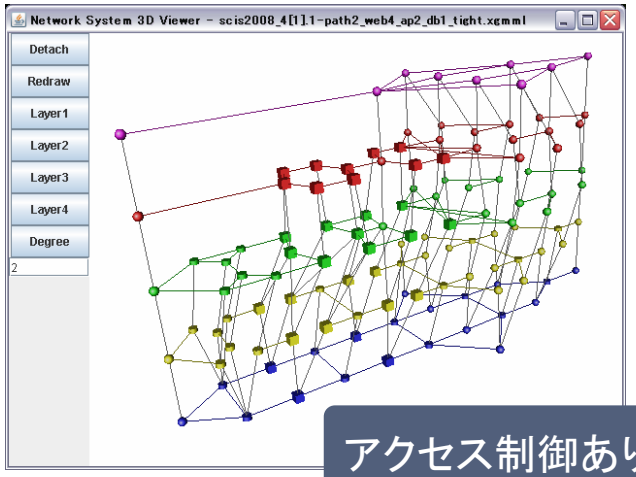
アクセス制御あり



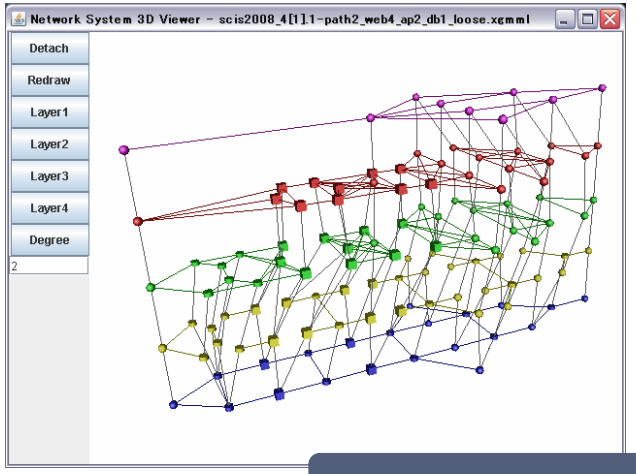
アクセス制御なし

リンク数分布(1)





アクセス制御あり



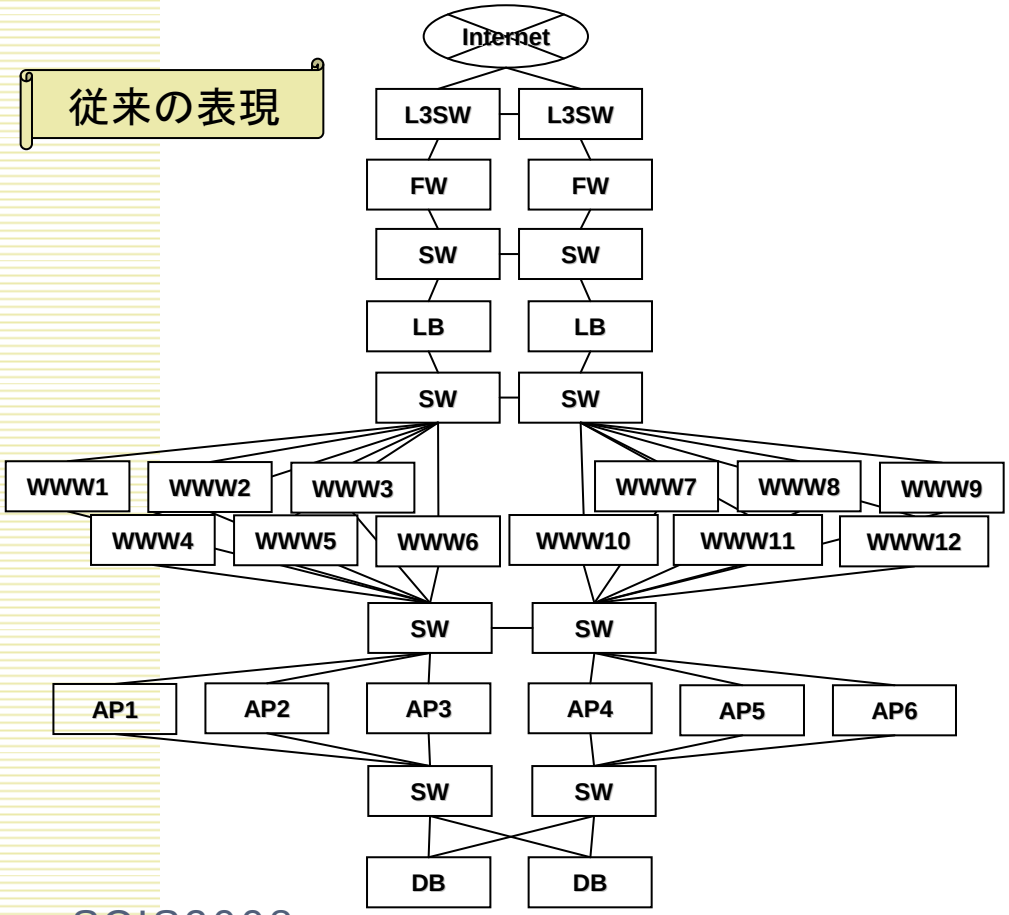
アクセス制御なし

リンク数	アクセス制御あり	アクセス制御なし
3	42	23
4	56	39
7	0	34

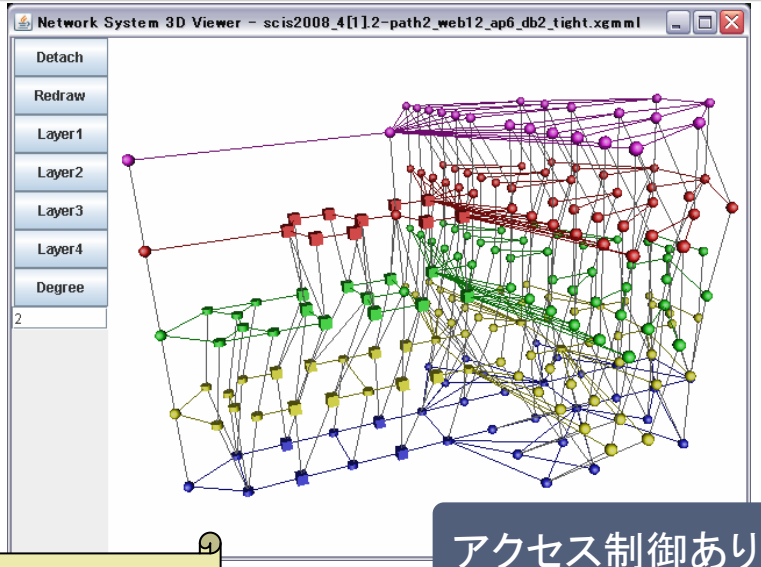
ネットワークシステム解析(2)

- **構成**
  - Webサーバ12台、アプリケーションサーバ6台、データベース2台

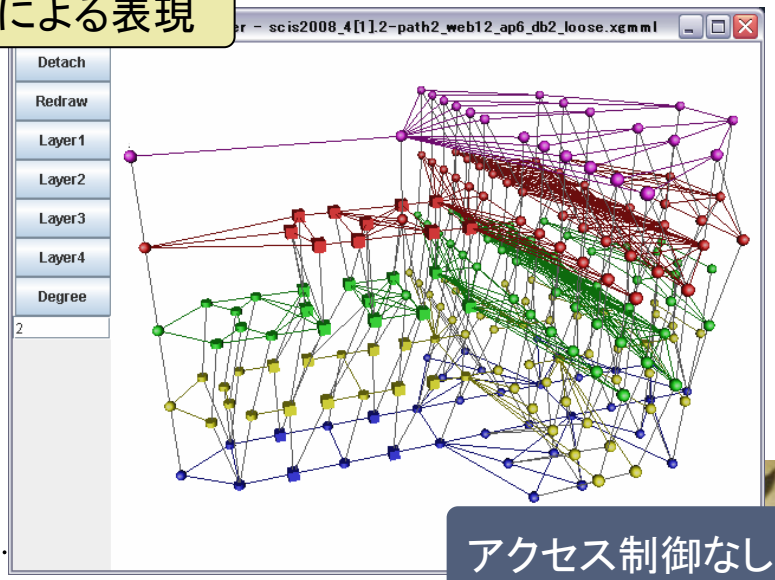
従来の表現



提案モデルによる表現

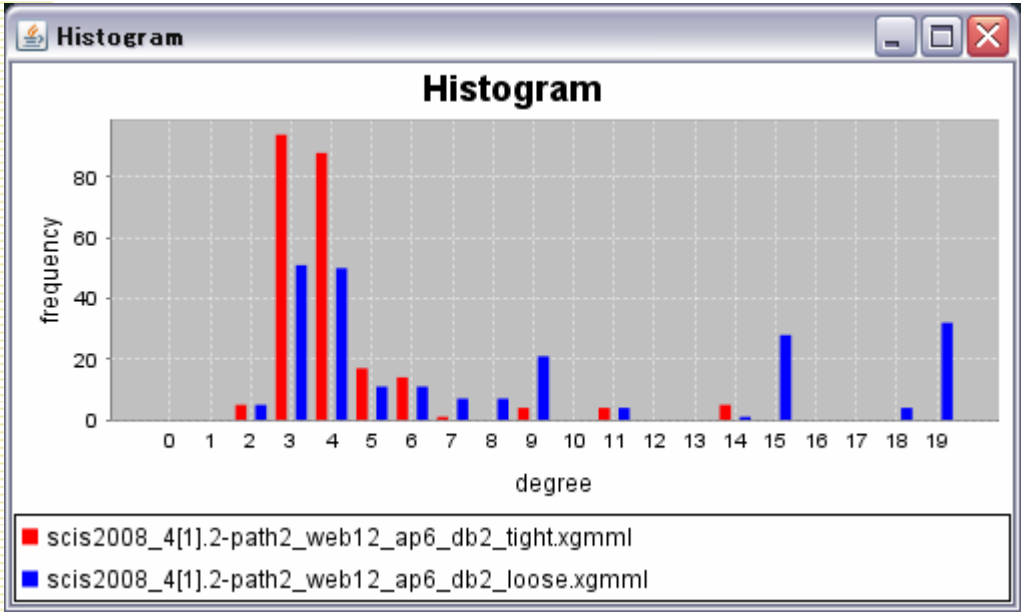


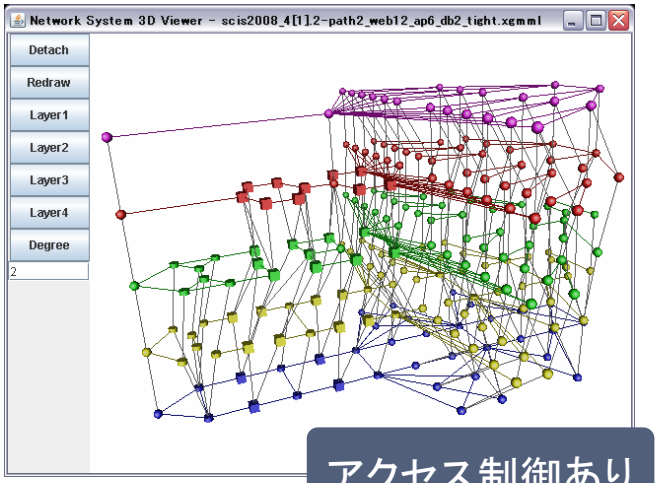
アクセス制御あり



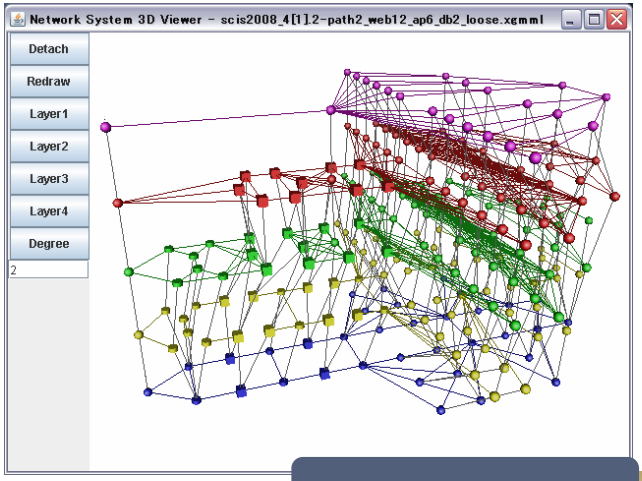
アクセス制御なし

リンク数分布(2)





アクセス制御あり

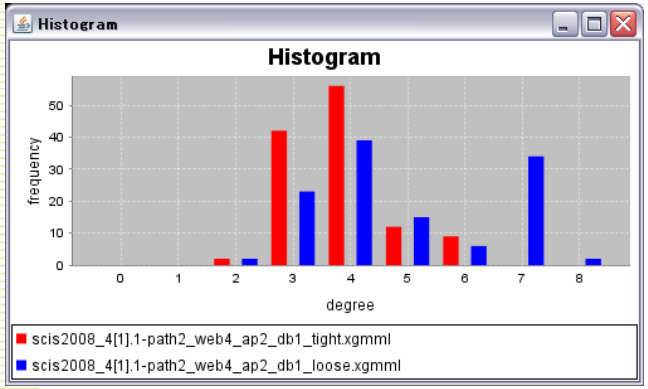


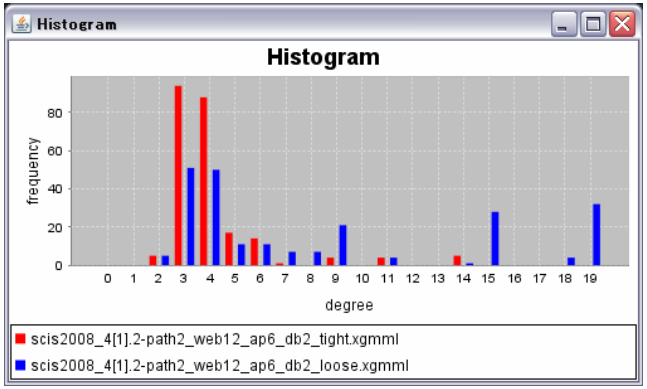
アクセス制御なし

リンク数	アクセス制御あり	アクセス制御なし
3	94	51
4	88	50
15	0	28
19	0	32

まとめ

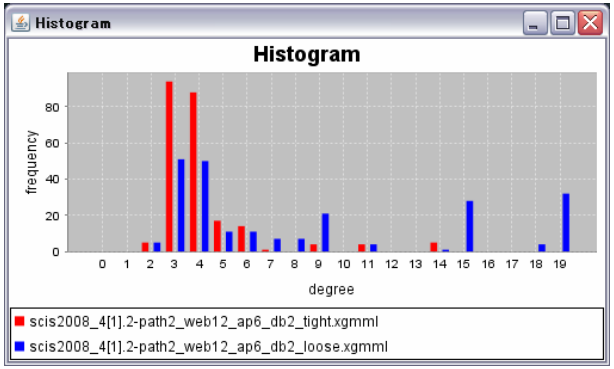
- **ネットワークシステム表現モデルの提案**
  - 各機器・機能を表現可能かつ システム全体を表現可能なモデル
  - レイヤ毎の論理ネットワークと、レイヤネットワーク間の接続
  - 機器は、ネットワーク機能モジュールの集まり
- **提案モデルによるシステムの解析**
  - アクセス制御状態の良否が与えるネットワーク構造の変化





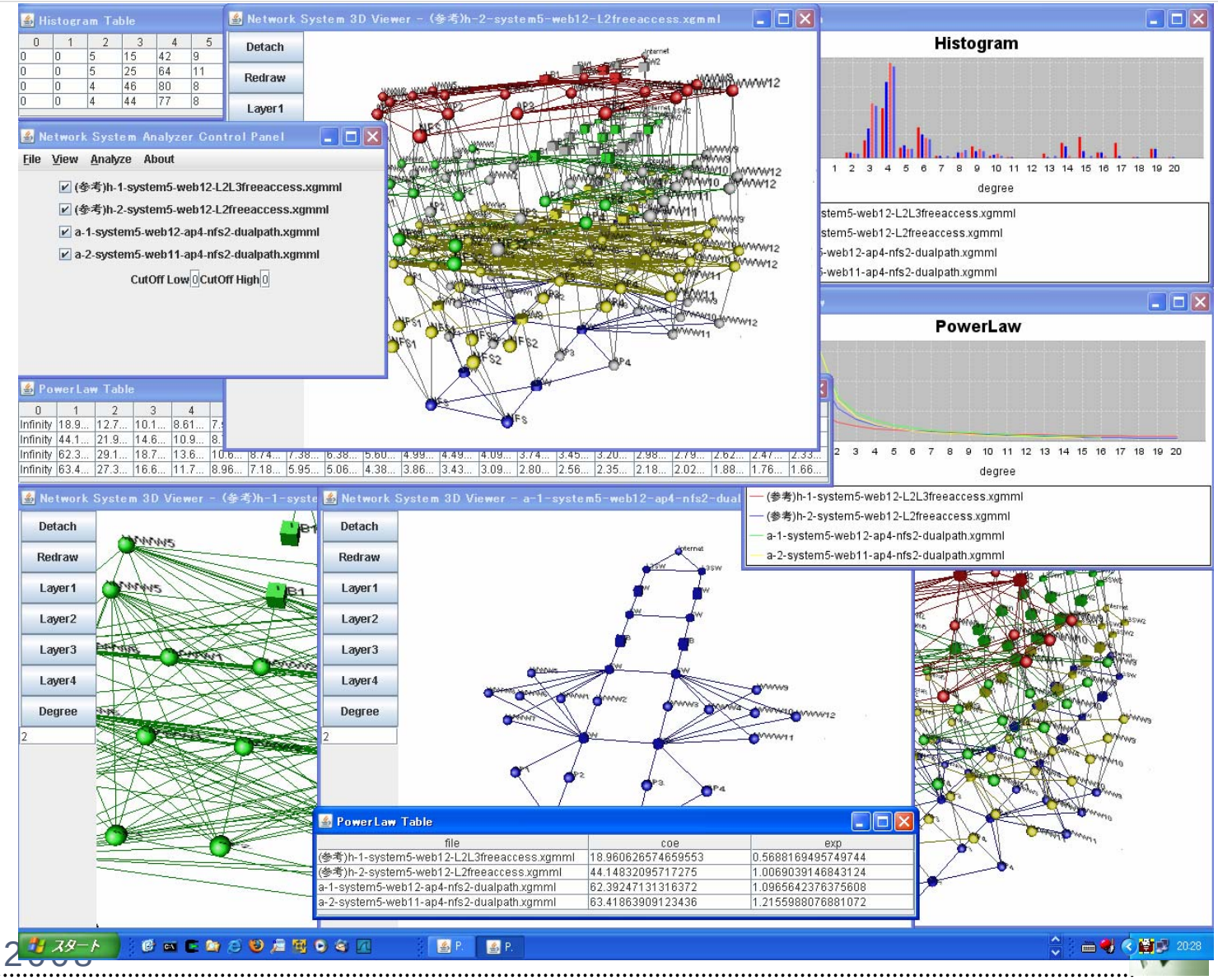
今後

- 提案モデルのさらなる解析
  - リンク分布における共通特性の抽出
  - レイヤ毎のネットワーク特性解析
  - 多方面からの解析
    - データ流量
    - 脆弱性とウイルス/ワームの影響



- 提案モデル解析を基にした定量指標
- 定量指標を基にした、安全なネットワークシステム自動構築アルゴリズム

解析用ツールデモ


Histogram Table
Network System 3D Viewer - (参考)h-2-system5-web12-L2freeaccess.xgmml
Detach
Redraw
Layer1
Network System Analyzer Control Panel
File View Analyze About
(参考)h-1-system5-web12-L2L3freeaccess.xgmml
(参考)h-2-system5-web12-L2freeaccess.xgmml
a-1-system5-web12-ap4-nfs2-dualpath.xgmml
a-2-system5-web11-ap4-nfs2-dualpath.xgmml
CutOff Low 0 CutOff High 0
Histogram
degree
PowerLaw
PowerLaw Table
Network System 3D Viewer - a-1-system5-web12-ap4-nfs2-dual
Detach
Redraw
Layer1
Layer2
Layer3
Layer4
Degree
PowerLaw Table
file coe exp
(参考)h-1-system5-web12-L2L3freeaccess.xgmml 18.960626574659553 0.5688169495749744
(参考)h-2-system5-web12-L2freeaccess.xgmml 44.14832095717275 1.0069039146843124
a-1-system5-web12-ap4-nfs2-dualpath.xgmml 62.39247131316372 1.0965642376375608
a-2-system5-web11-ap4-nfs2-dualpath.xgmml 63.41863909123436 1.2155988076881072