



アクセス制御の違いによる ネットワークシステムの特性変化 に関する考察

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

- 本研究の目的と本論文の位置づけ
- 背景
- これまでの成果
- ネットワークシステムのデータセット構築
- ネットワークシステムの特性解析
- まとめ



本研究の目的と本論文の位置づけ

■ 目的

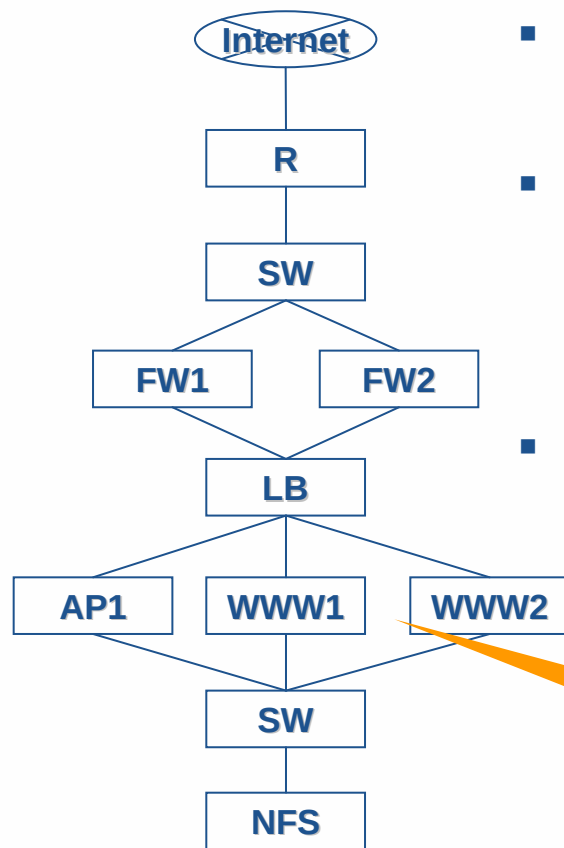
- 。ネットワークシステムにおける安全な設計方法論確立のためのシステム定量評価
- ◆ ネットワークシステム (Networked System) :
 - サーバやデータベース、ルータ、ファイアウォール、ロードバランサなど、各機能をそれぞれの機器で行って、全体として1つのサービスを提供するシステム

■ 位置づけ

- 。SCIS2008で提案した表現モデルを用いた、アクセス制御の面からのシステム特性解析



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

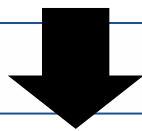


ネットワークシステム表現モデル (NSQモデル)

基本戦略

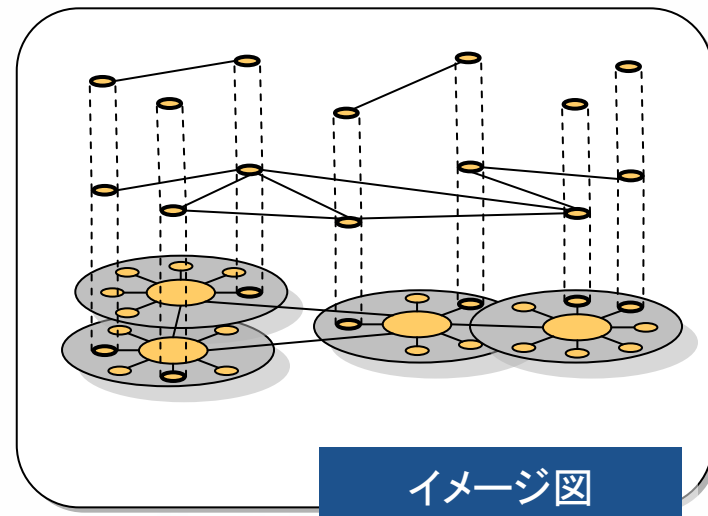
現状

物理的接続のみを反映したネットワーク表現



NSQ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

レイヤ 定義

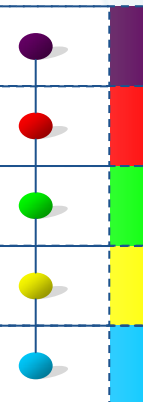
レイヤ5: 抽象化サービス (HTTP、DNS、SMTP等)

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]

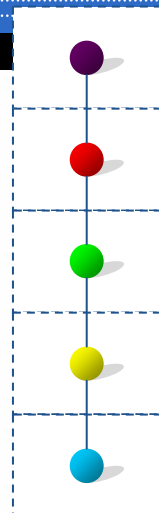
レイヤ1: 物理的接続





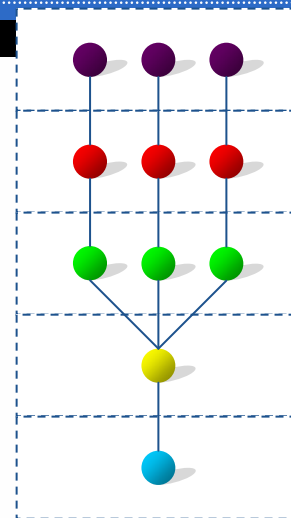
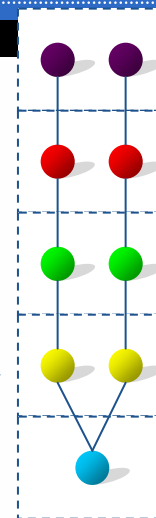
モジュール例

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)

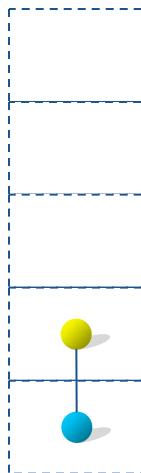


中継機器(機能)

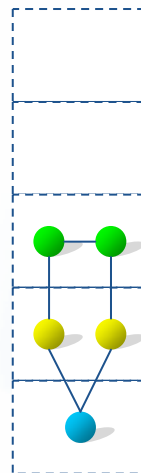
L1R
(ハブ)



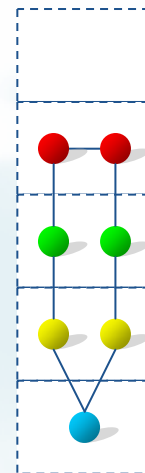
L2R
(スイッチ)



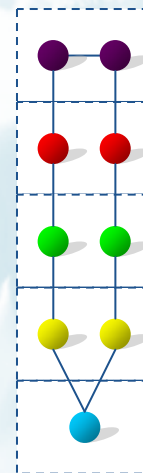
L3R
(ルータ)



L4R
(NAPT)

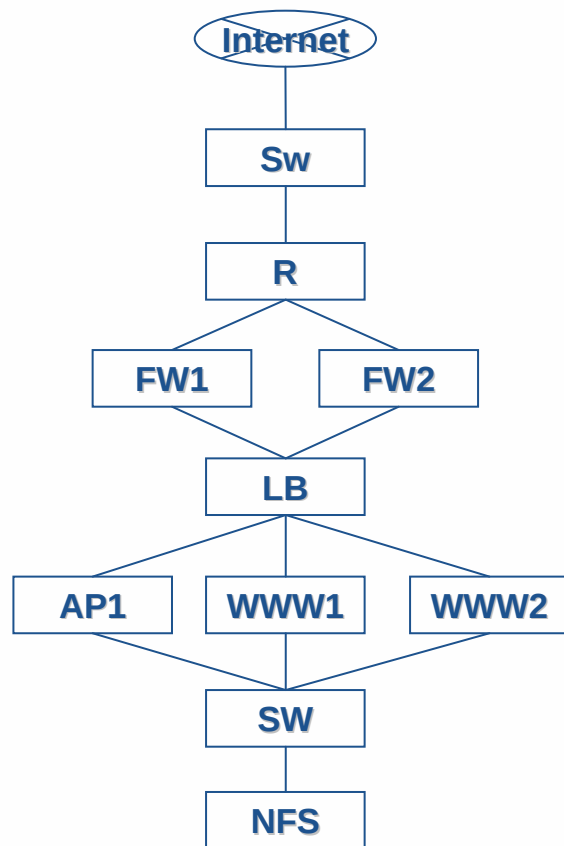


L5R
(プロキシ)

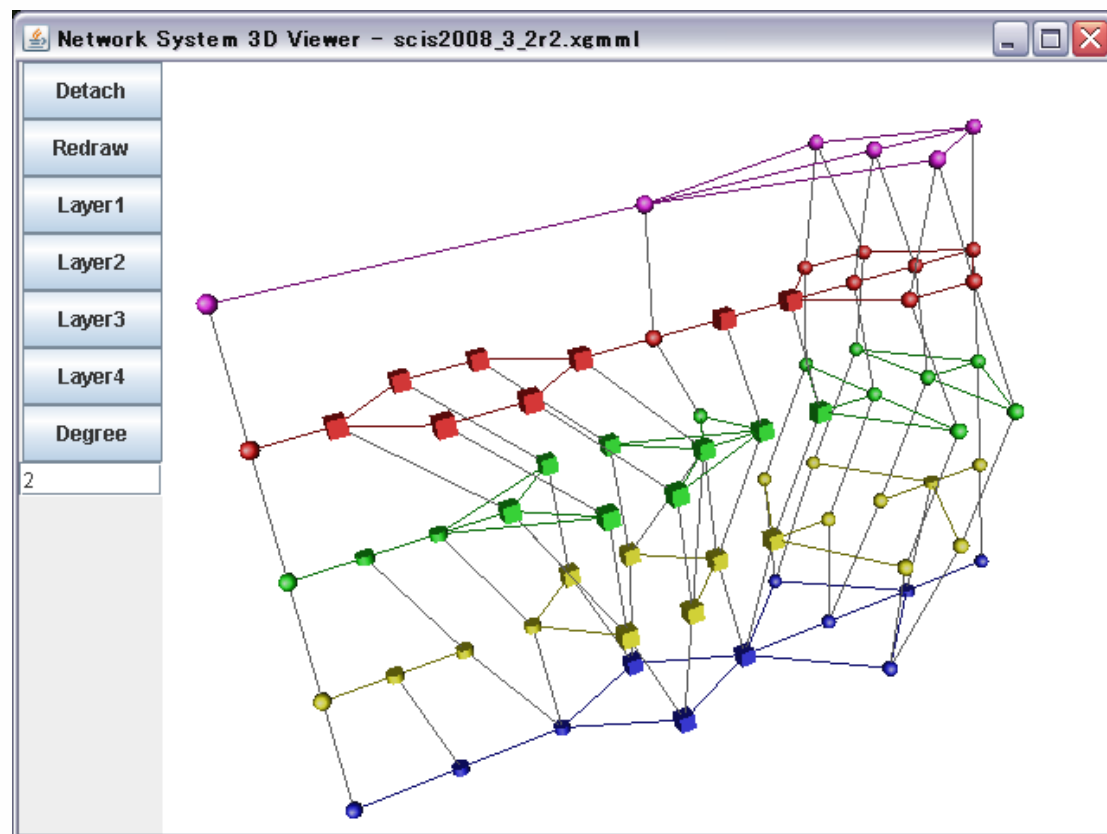




提案モデルによるネットワーク表現例



従来の表現

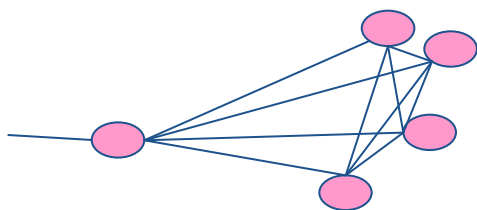


提案モデルによる表現

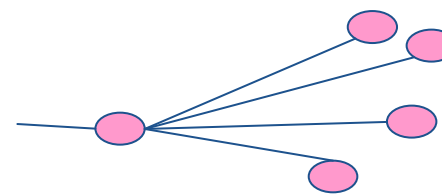


モデルが持つ特徴解析

- リンクがある＝ノード間が通信可能
- リンクの多さ＝必要となる通信パターンが多い 又は 不必要な通信が許可されている
- リンクの多さを見ることで、特徴がつかめないか
。各ノードが持つリンク数の分布(次数分布)を解析



次数	ノード数
4	4
5	1



次数	ノード数
1	4
5	1



データセットの構築





データセットの構築

- 多数のNSから共通する特徴の抽出を目指す
- どの「多数」を選ぶか
 - 。網羅性が問われる
 - 。理想的にはすべての種類
- 問題点
 - 。ある1つのレイヤ(L1とする)でのネットワークの取りうる種類数が膨大

ノード種類(計7種類)

S/Ss(Service)、
L1R(Hub)、L2R(Switch)、L3R
(Router)、L4R(NAPT)、L5R(Proxy)

リンク数が1のノードが少なくとも2つ以上

L1ネットワークの種類数

ノード数	グラフ数 (同型判定前)	グラフ数 (同型判定後)
2	1	1
3	6	6
4	42	27
5	474	294
6	12606	7121
7	470742	283482
8	26364210	N/A
9	2181981354	N/A
10	292914780702	N/A



モジュール間接続制限

- モジュールの接続に制限
 - 現実のシステムでは機器の多くはスイッチ(L2R)と接続されている
- 制限
 - リンク数が1のノードが少なくとも2つ以上
 - **モジュール間接続制限**
 - 各モジュールはL2Rに隣接
 - **多段L2R不許可**

	S	Ss	L1R	L2R	L3R	L4R	L5R
S	×	×	×	○	×	×	×
Ss	×	×	×	○	×	×	×
L1R	×	×	×	○	×	×	×
L2R	○	○	○	×	○	○	○
L3R	×	×	×	○	×	×	×
L4R	×	×	×	○	×	×	×
L5R	×	×	×	○	×	×	×

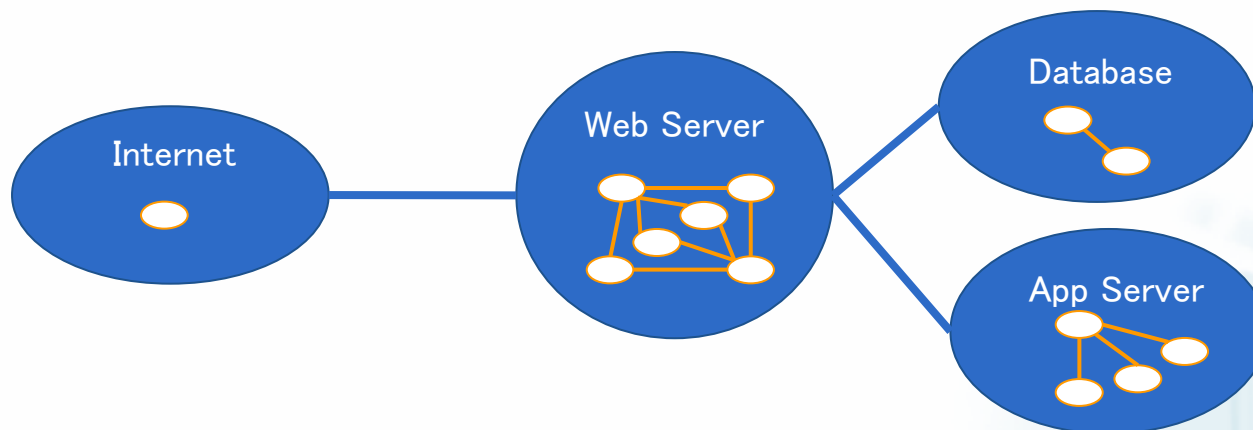
- ノード種類(計7種類)
 - リンク数 1 (1種類)
 - S
 - リンク数 複数 (6種類)
 - L1R、L2R、L3R、L4R、L5R、Ss

ノード数	グラフ 数	グラフ数 (同型判定後)
2	0	1
3	1	6
4	1	27
5	6	294
6	21	7121
7	121	283482
8	1061	N/A
9	10782	N/A
10	N/A	N/A



抽象化サービスノードが持つ 部分ネットワーク

- 抽象化した機能(L5ノード)による基本グラフからの拡大
 - L5ノードをそれぞれ複数のL1ノードへ分割
 - 異なるL5ノードに属するL1ノード群は、L5ネットワークの接続に従い接続される

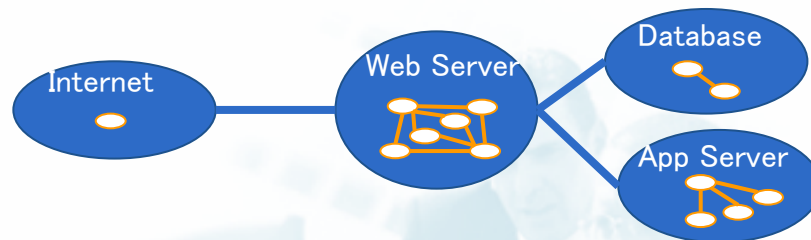


L1の構成	種類数
...	
1-1-5-5	7520
1-3-5-5	140
1-3-4-5	205
1-3-5-5	18020
1-4-4-5	140
1-4-5-5	18170
...	



各レイヤのネットワーク構築

- L5: 4つのサービス (Internet、Web Server、Database、Application Server) の組み合わせ
 - 27種類 (同型排除後)
- L1: L5の各4つのサービスに対して部分L1ネットワークを持ち、L5接続にあわせてL1同士を接続
 - 各部分L1ネットワークのノード数は1～5

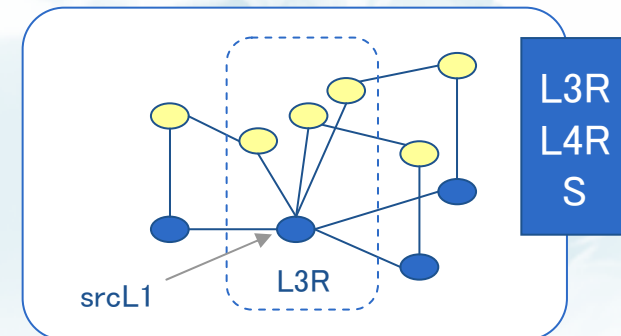
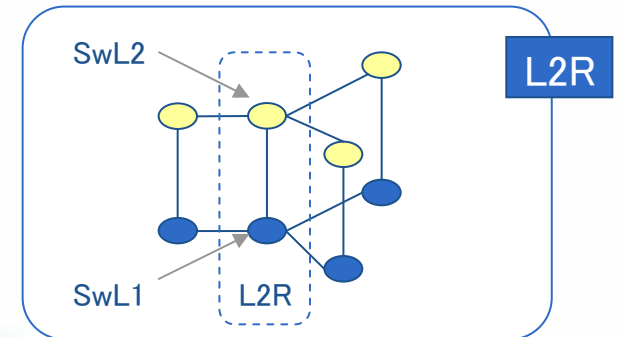
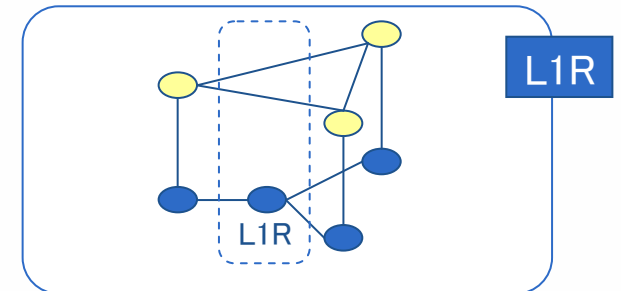


- L2、L3、L4
 - L2: L1の接続形態により決定
 - L3、L4: L2, L5の接続形態とアクセス制御ルールにより決定



各レイヤの構築:L1-L2接続

- L1R(Hub)
 - L1Rと接続されているL1ノード群を抽出
 - それらL1ノードと接続しているL2ノード同士をつかって完全グラフを構築
- L2R(Switch)
 - SwL1で接続されているL1ノードと接続しているL2ノードを、SwL2とつなぐ
- L3R、L4R、S
 - srcL1と接続されているL1ノード群抽出
 - L1ノード群のそれぞれのL2ノードと、srcL1のL2ノードを対応づける

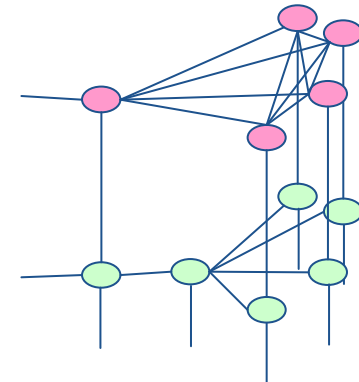




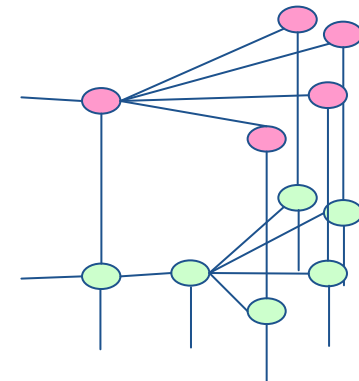
L3、L4接続：アクセス制御

- L3、L4ネットワーク
 - ノード間接続は、アクセス制御ルールに依存
- アクセス制御ルール
 - 無し (Looseケース)
 - 各セグメント内にあるモジュール間はずべて通信可能
 - 部分的な完全グラフを形成
 - 有り
 - 必要なモジュール間のみが通信可能
 - 「最適＝リンク数を最小」とし、リンク数を削減するアルゴリズムを提案 (Efficientケース)

アクセス制御無し



アクセス制御有り



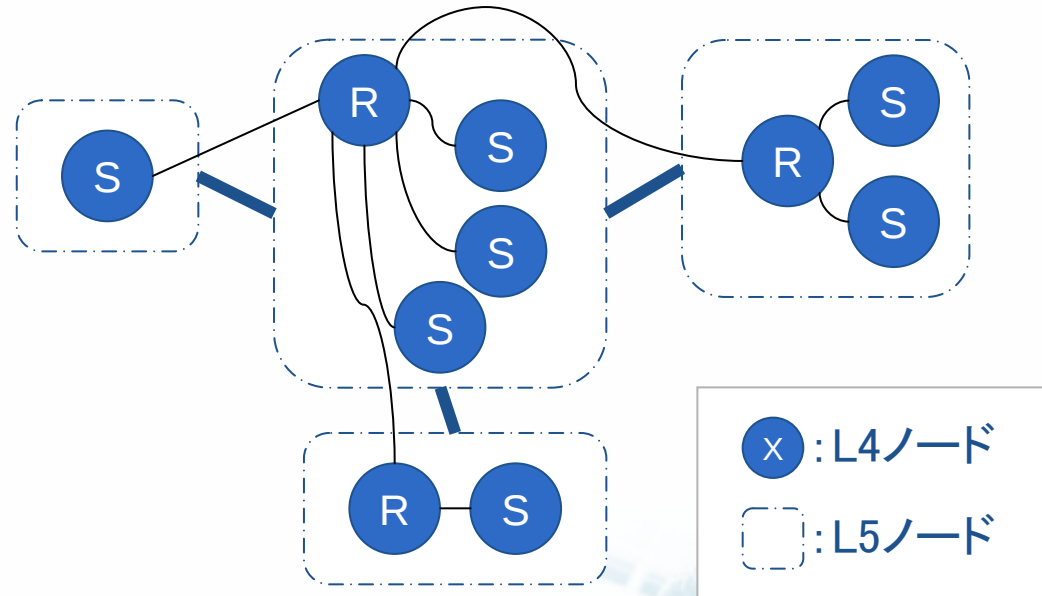


リンク数削減アルゴリズム

基本アイディア

上位レイヤ(右図ではL5)の他ノードとの接点:

- ・中継器がある場合は、中継器だけ
- ・内部サービスモジュールは、中継器に接続



アルゴリズム

＜上位ノードA-B間の接続の場合＞

1) 接続候補抽出(A)

抽象ノードA内に下位中継モジュール(LxR)がある場合

LxRのレイヤxノード(のうち1つだけ)を接続候補ノード群に追加(Cand_A)

他のノード(Sなど)はLxR群と内部接続

ない場合

他のノード(Sなど)をCand_Aに追加

2) 接続候補抽出(B)

上記と同様にCand Bを抽出

3) 接続候補同士の接続(A-B)

Cand AとCand B間を接続



特性解析





次数分布比較

■ 比較対象

- LooseケースとEfficientケースの違い
 - NSの構築手法により次数分布に差が現れるか
- モジュール有無の違い
 - 特定モジュールの存在が次数分布にどのような違いを生じさせるか
 - L1RとL3Rについて提示

■ 比較方法

- 全NSを、ノード数ごとにグループ分けを行いそれぞれの次数分布を求める
- グループに含まれるNS数が少ない(<300)のものを除き比較(ノード数が35以上)

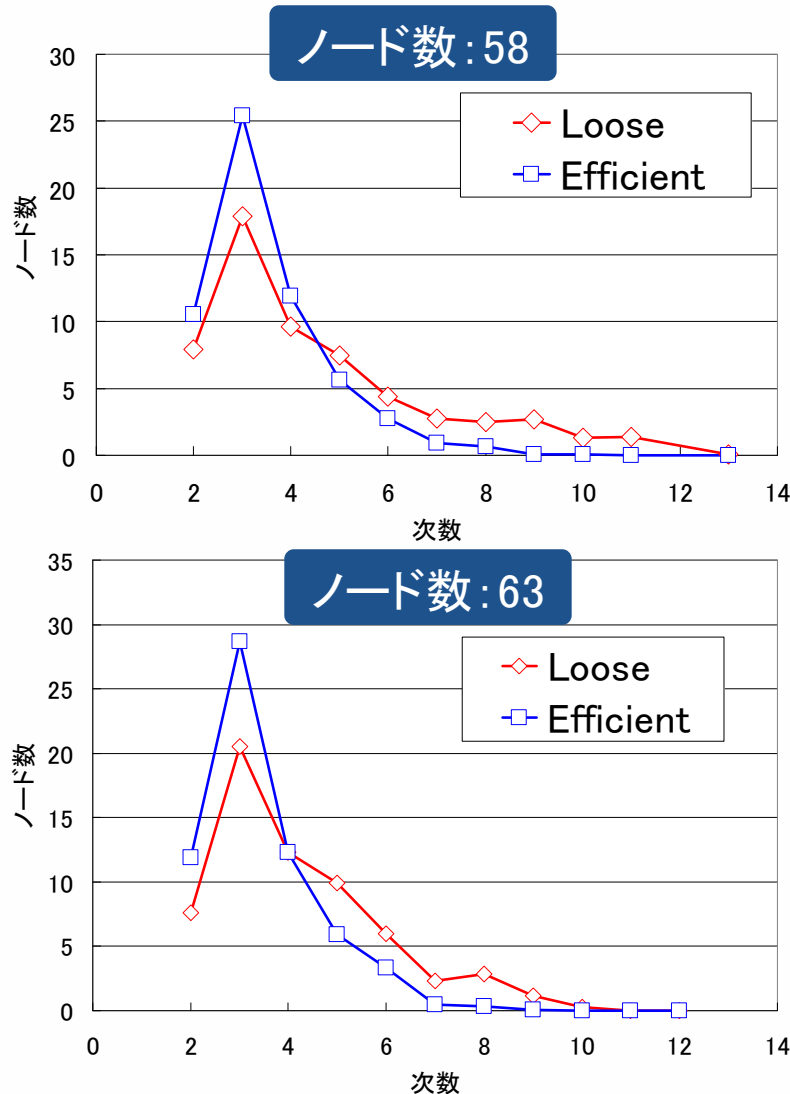
➡ 最初に…
比較結果から得た1つの仮説を

**最適なアクセス制御状態にあるネットワークシステムは
NSQモデル上の次数分布において一定の分布形状を持つ**



LooseとEfficientの違い

ノード数: 58、63

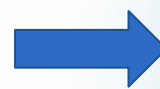


Loose、Efficient共通

- ・ 次数は3で最大
- ・ 次数4以上は減少傾向

Loose、Efficient差異

- ・ Efficient: 次数4以上の減少がなだらか
- ・ Loose: 次数4以上の値が上下
- ・ Loose: Efficientと比較して平坦

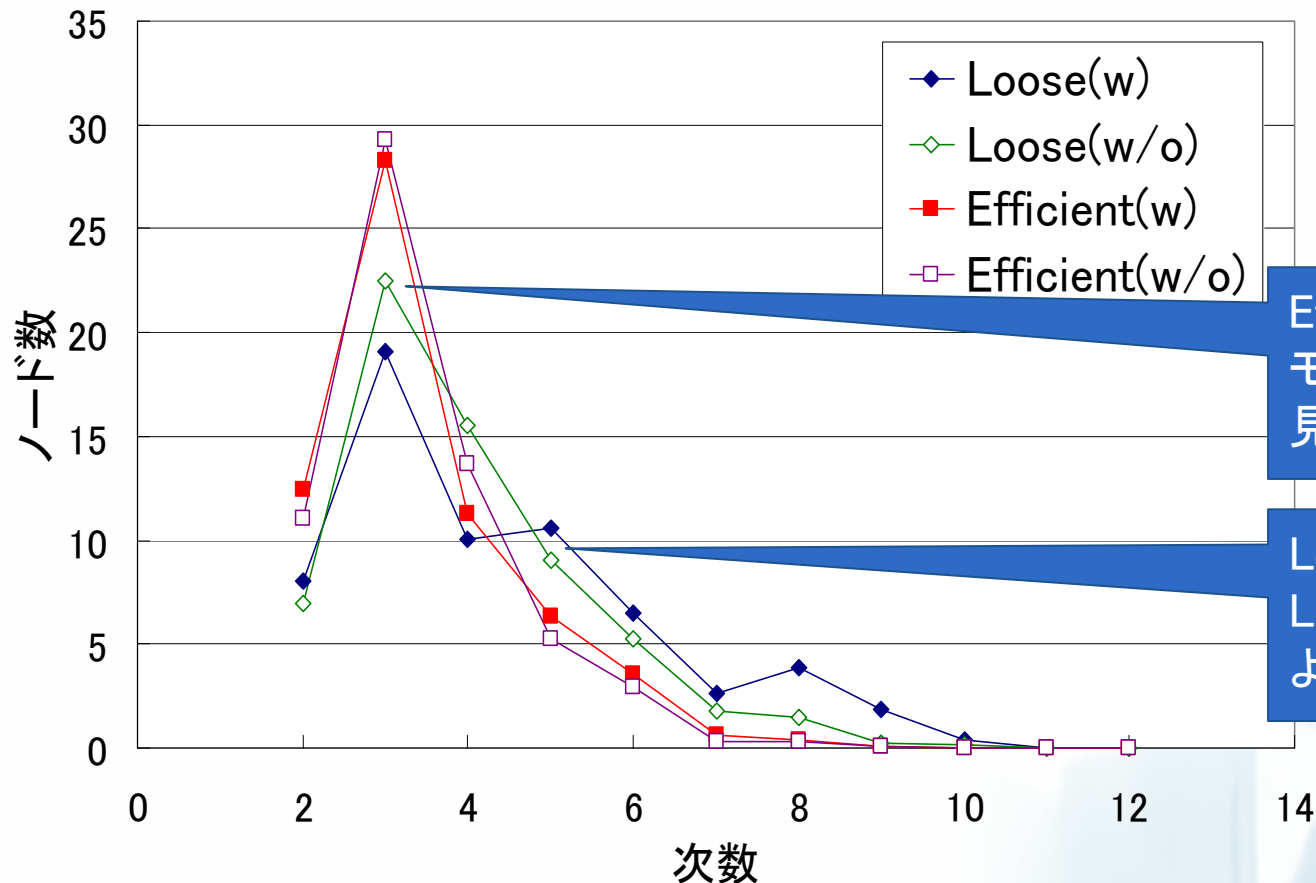


他のノード数においても
同様の傾向



特定モジュールの影響 (L1R)

ノード数: 63



Efficientケースでは
モジュール有無の差が
見られない

Looseケースでは
L1Rを持つNSは
より平坦な分布を持つ

他のノード数においても
同様の傾向

最適なアクセス制御状態にあるNSは
次数分布において一定の分布形状を持つ

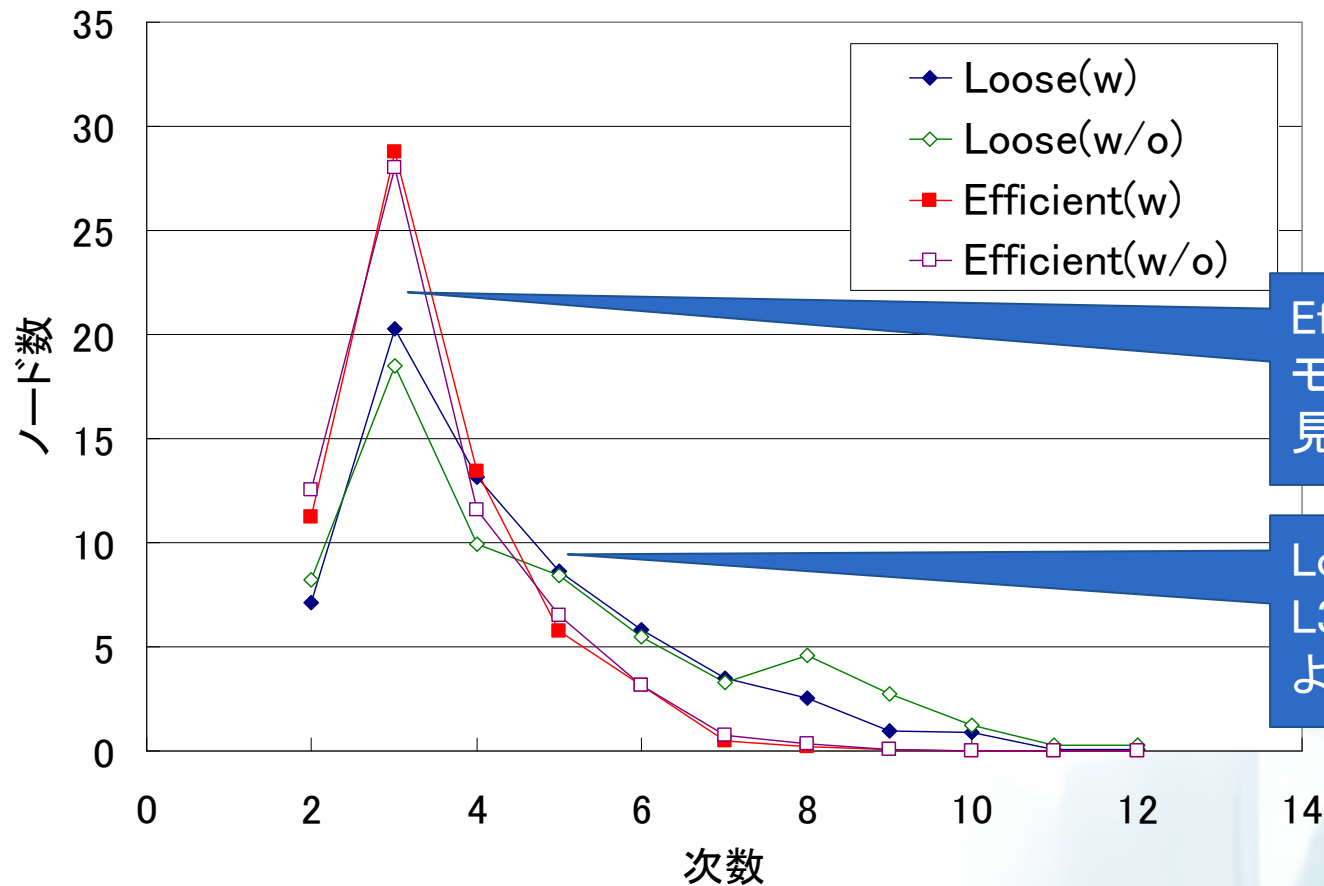


仮説を支持する結果



特定モジュールの影響 (L3R)

ノード数: 63



Efficientケースでは
モジュール有無の差が
見られない

Looseケースでは
L3Rを持たないNSは
より平坦な分布を持つ

他のノード数においても
同様の傾向

最適なアクセス制御状態にあるNSは
次数分布において一定の分布形状を持つ

➡ 仮説を支持する結果

- SCIS2008で提案したモデルを用いた、ネットワークシステムの特性解析
 - 。アクセス制御に注目
- 多数のネットワークシステムの次数分布を調査
 - 。アクセス制御の違いとして「Loose」と「Efficient」2つのケースを比較
 - 。特定モジュールの有無による次数分布の違いを調査
- Efficientなケースでは、一定分布を取ると言える
 - 。モジュールの有無には依存しない
 - 。「最適ケース」でも一定分布を取ると仮定することが可能
- 今後
 - 。一定分布の近似曲線を求めることで、数値パラメータとして表現
 - 成功: CSS2008
 - 。数値パラメータを利用することで、NSのアクセス制御状態の評価指標の策定を目指す

0	1	2	3	4	5
0	0	5	15	42	9
0	0	5	25	64	11
0	0	4	46	80	8
0	0	4	44	77	8

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

PowerLaw Table

0	1	2	3	4	5
Infinity	18.9...	12.7...	10.1...	8.61...	7.5...
Infinity	44.1...	21.9...	14.6...	10.9...	8.1...
Infinity	62.3...	29.1...	18.7...	13.6...	10.6...
Infinity	63.4...	27.3...	16.6...	11.7...	8.96...

Network System 3D Viewer - (参考)h-1-system5-web12-L2L3freeaccess.xgmml

Detach

Redraw

Layer1

Layer2

Layer3

Layer4

Degree

2

Network System 3D Viewer - a-1-system5-web12-ap4-nfs2-dualpath.xgmml

Detach

Redraw

Layer1

Layer2

Layer3

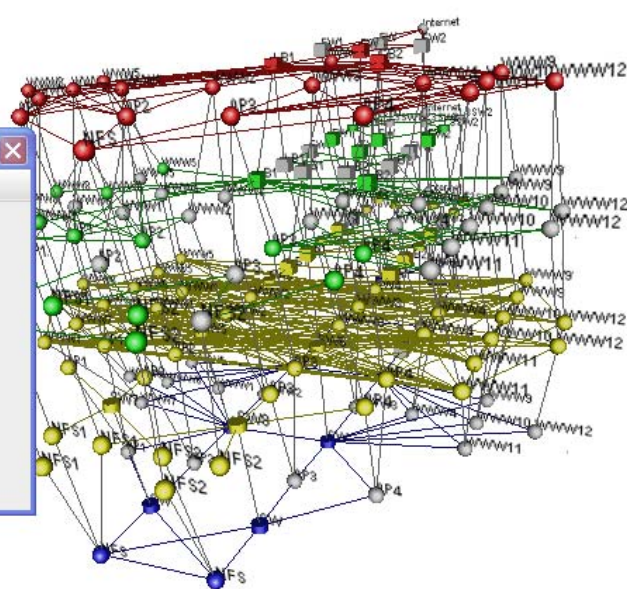
Layer4

Degree

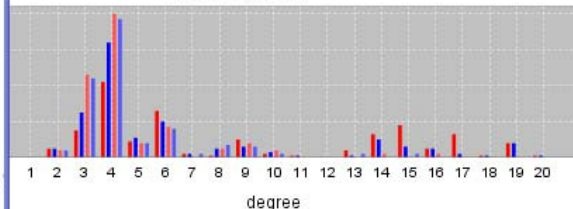
2

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



Histogram



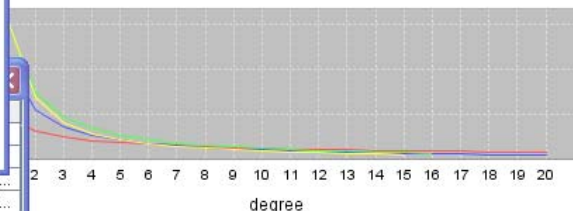
stem5-web12-L2L3freeaccess.xgmml

stem5-web12-L2freeaccess.xgmml

5-web12-ap4-nfs2-dualpath.xgmml

5-web11-ap4-nfs2-dualpath.xgmml

PowerLaw



- (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