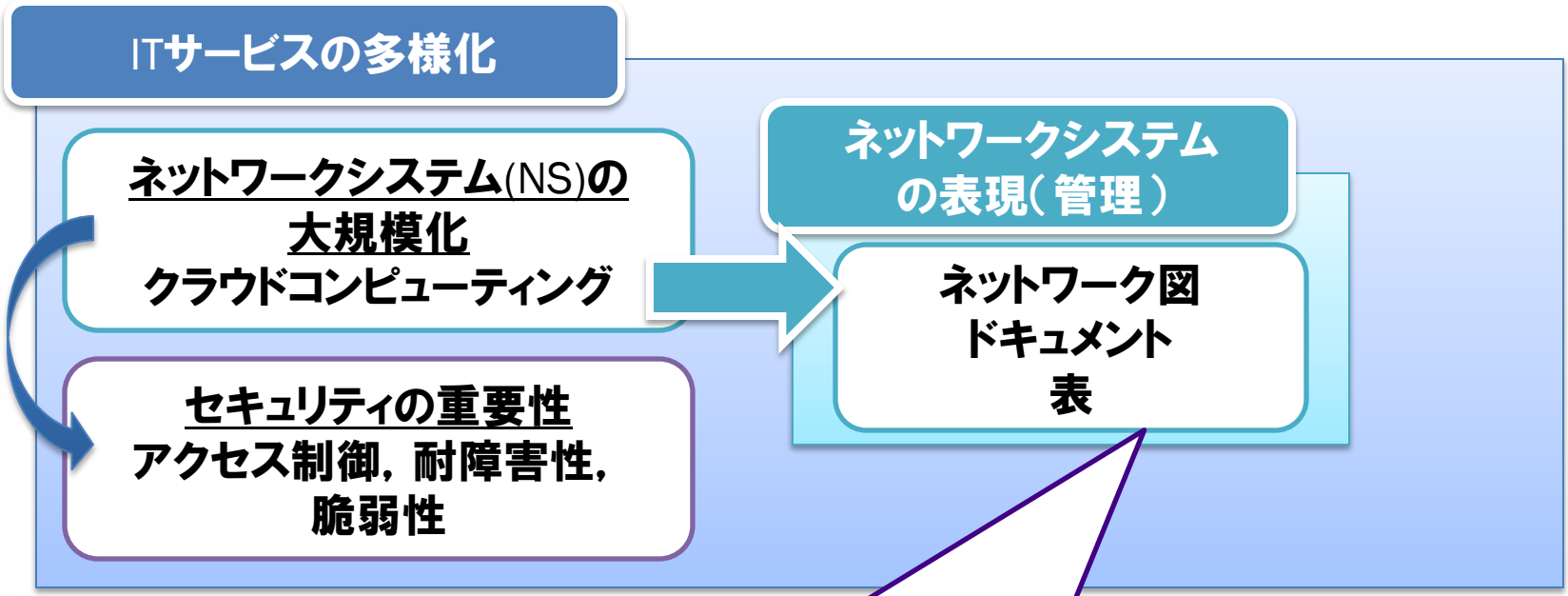
向きを持つマルチレイヤネットワークモデルの提案とセキュリティへの応用

金岡 晃(筑波大学)、原田敏樹(筑波大学)、
加藤雅彦(IIJ Tech.)、岡本栄司(筑波大学)

Outline

- 背景と目的
- これまでのアプローチ
- モデル化の応用と既存モデルの問題点
- モデルの改良
- 改良による利点
- まとめ

背景と目的



再利用できない情報
構造化されないExcelデータ
どこに何が書いてあるかわからない大量の紙
ドキュメントを中心とした情報伝達
以心伝心、ドキュメント化されない重要事項
人が変われば書き方変わる
人に依存した運用

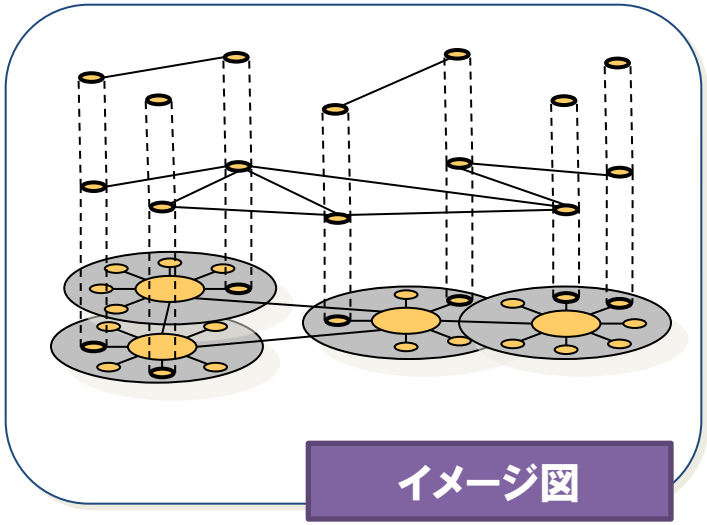
ネットワークシステム表現モデル（NSQモデル）

現状

物理的接続のみを反映したネットワーク表現

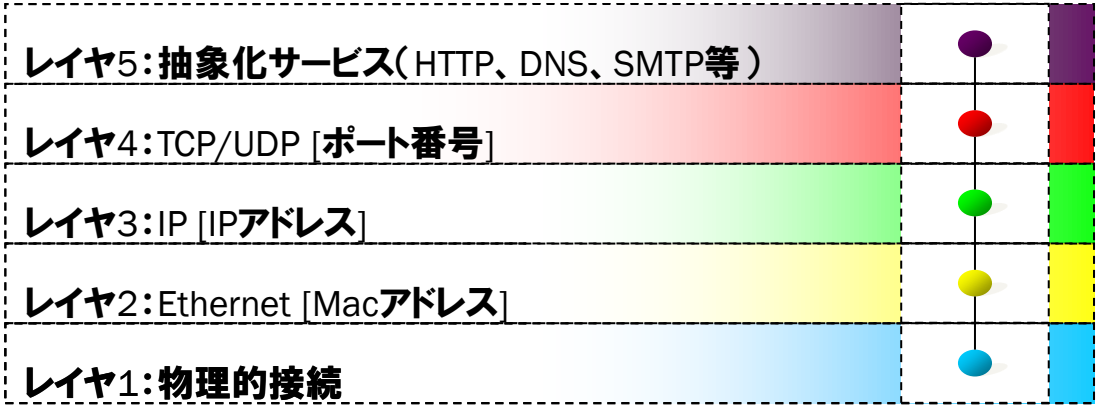
NSQモデル

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



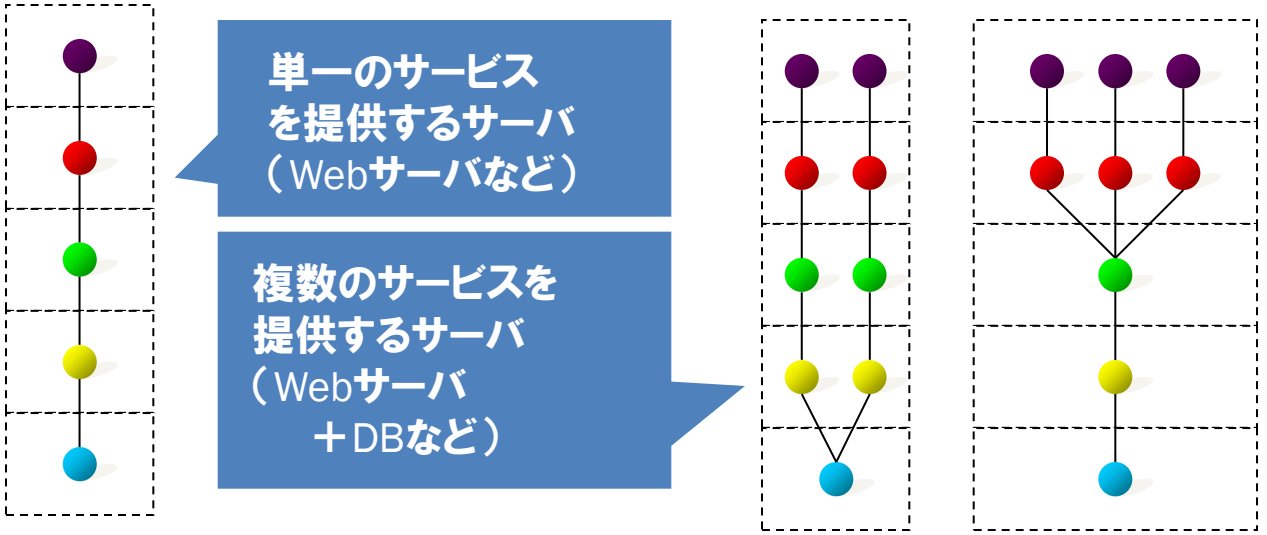
イメージ図

レイヤ定義

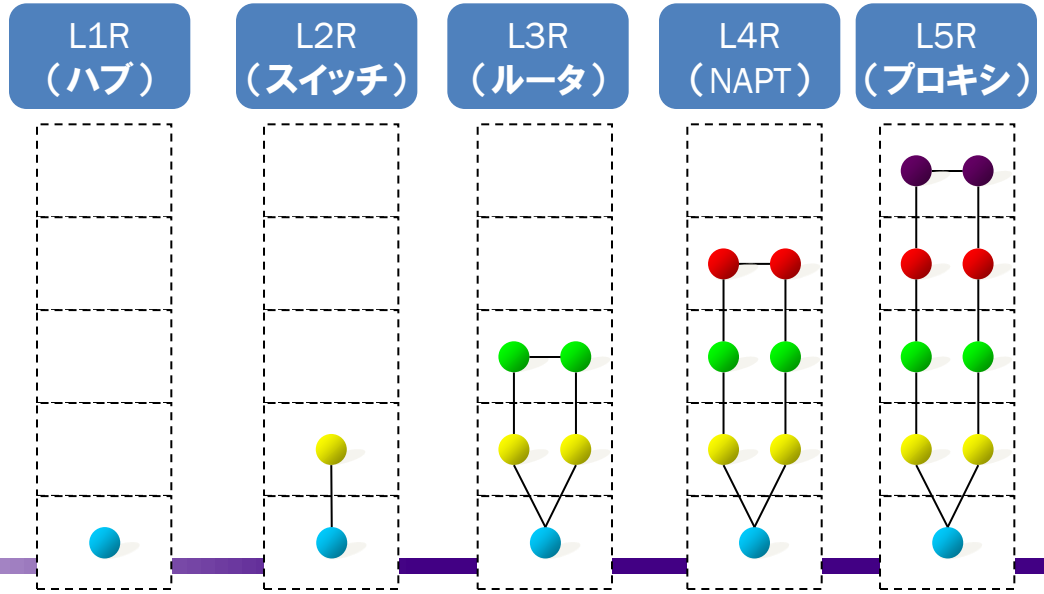


機器(モジュール)例

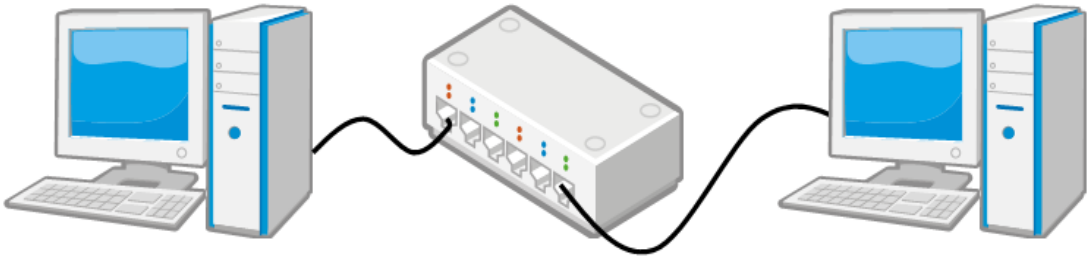
サーバ



中継機器(機能)



具体例

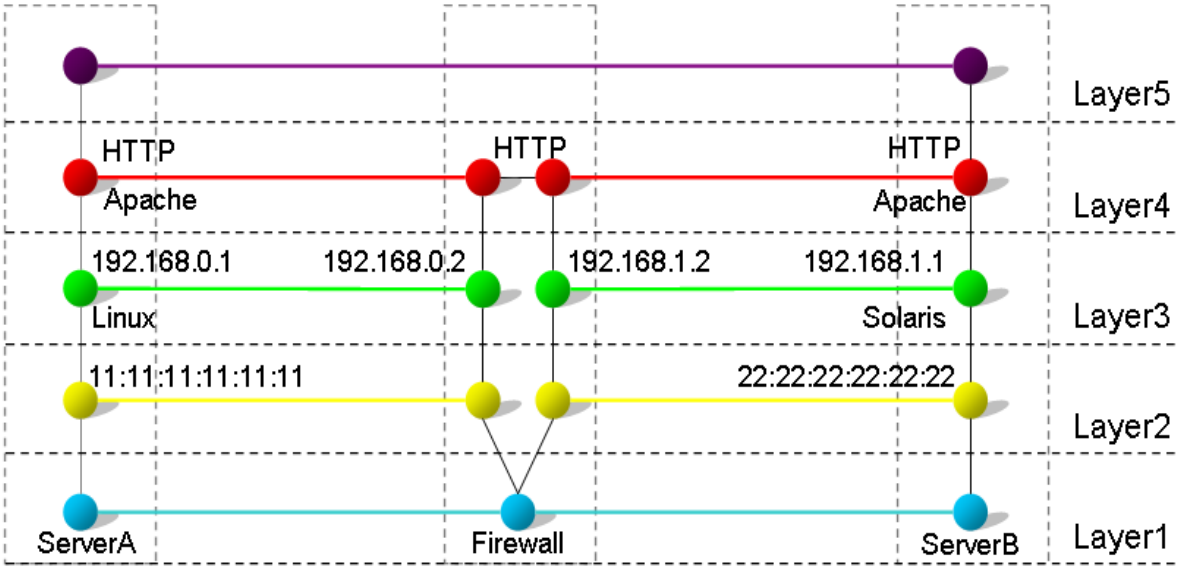


ServerA — Firewall — ServerB

ServerA
Service: HTTP
Application: Apache
OS: Linux
IP: 192.168.0.1
MAC:11:11:11:11:11:11

Firewall
IP:192.68.0.2
IP:192.168.1.2

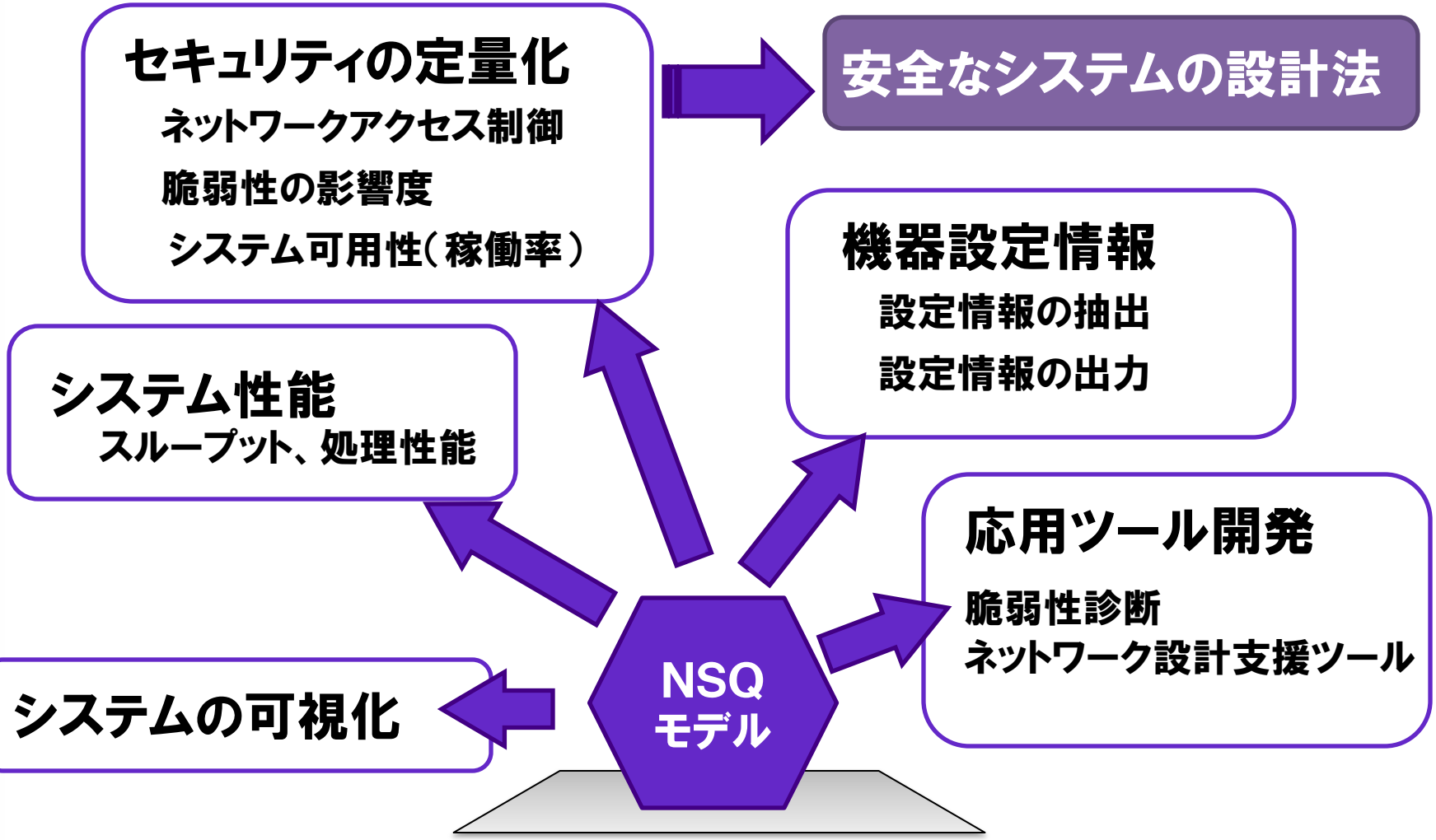
ServerB
Service: HTTP
Application: Apache
OS: Solaris
IP: 192.168.1.1
MAC:22:22:22:22:22:22



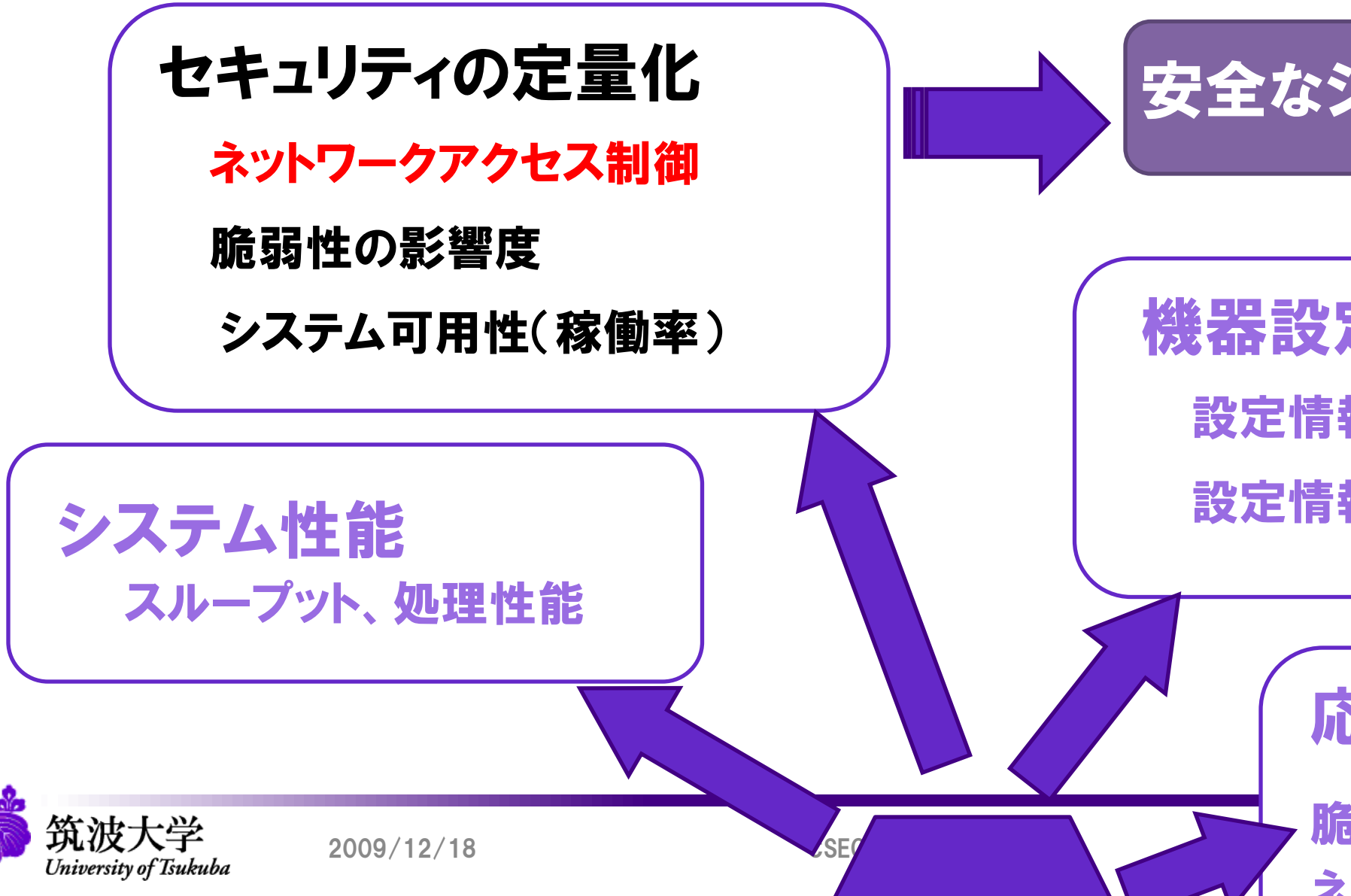
XMLデータ

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<graph label="Network 0" id="Network 0" xmlns:dc="http://purl.org/dc/elements/1.1/"
xmlns="http://www.cs.rpi.edu/XGMML" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <att name="documentVersion" value="1.0"/>
  <att name="networkMetadata">
</att>
  <att name="backgroundColor" value="#ccccff"/>
  <att type="string" name="documentVersion" label="documentVersion" value="1.0"/>
  <att type="real" name="GRAPH_VIEW_ZOOM" label="GRAPH_VIEW_ZOOM"
value="0.7863989678939893"/>
  <att type="real" name="GRAPH_VIEW_CENTER_X" label="GRAPH_VIEW_CENTER_X" value="-
1306.070674486478"/>
  <att type="real" name="GRAPH_VIEW_CENTER_Y" label="GRAPH_VIEW_CENTER_Y" value="-
220.6134203804719"/>
  <node label="node8_937" id="-67">
    <att type="boolean" name="center" label="center" value="false"/>
    <att type="string" name="canonicalName" label="canonicalName" value="node8_937"/>
```

モデル化とデータを中心にした応用

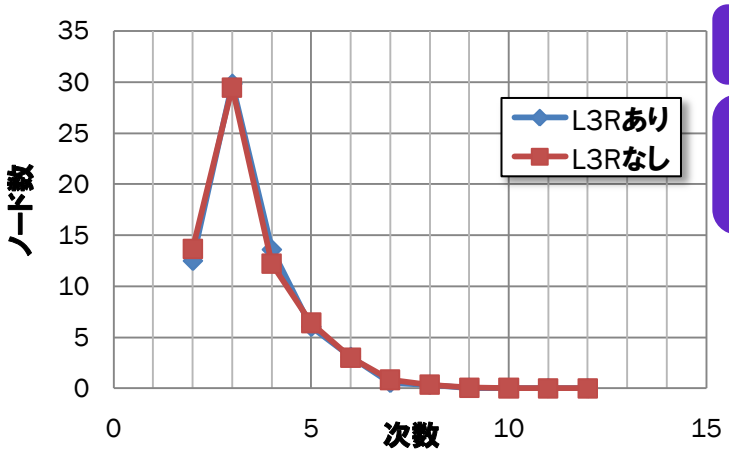


モデル化とデータを中心にした応用



次数分布に共通する特徴

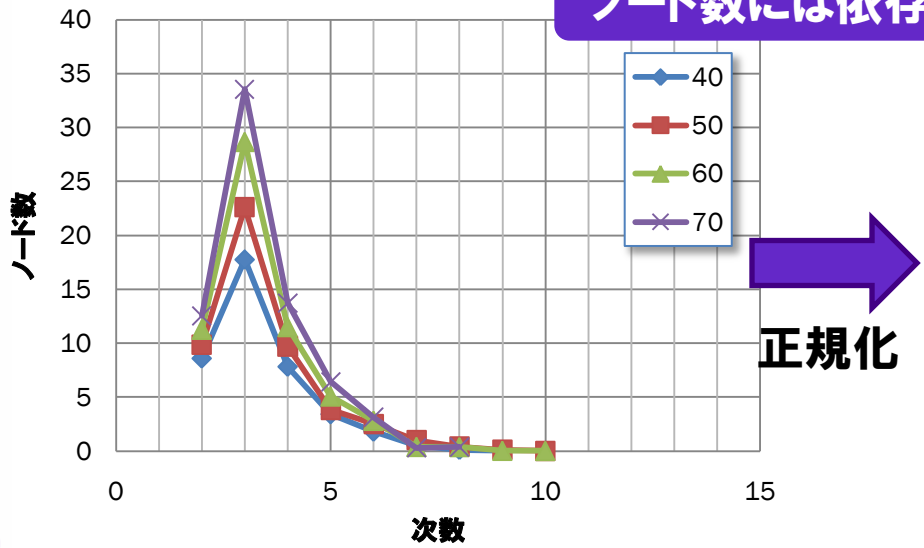
無駄なネットワークパスを省いた
ネットワークシステムは、
特定モジュールの有無にかかわらず
次数分布がほぼ一致する



ノード数：69

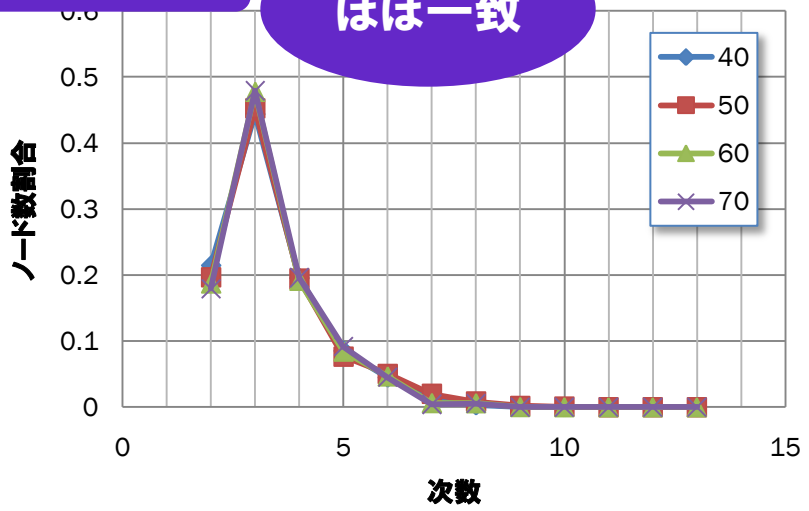
L3Rの有無を比較

ノード数には依存しない特徴



正規化

ほぼ一致

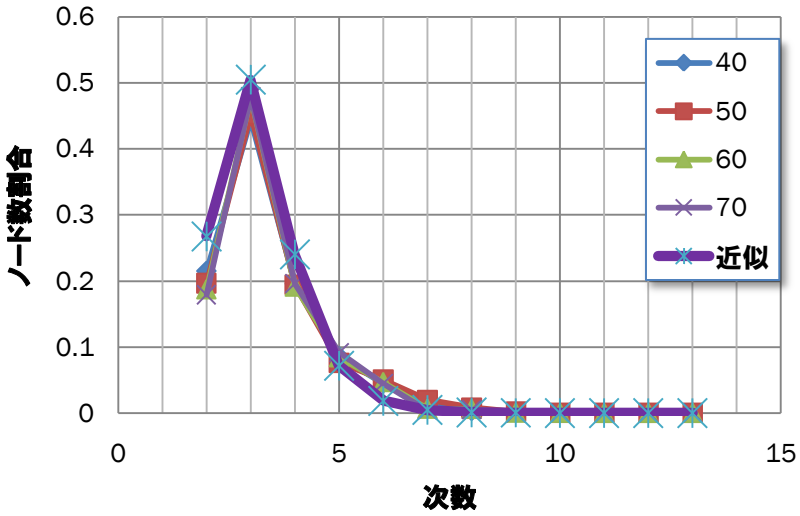


共通特性のパラメータ化と評価尺度

関数で近似

$$f(x) = \Theta \frac{x^{29.526}}{(1+0.518x)^{50.019}}$$

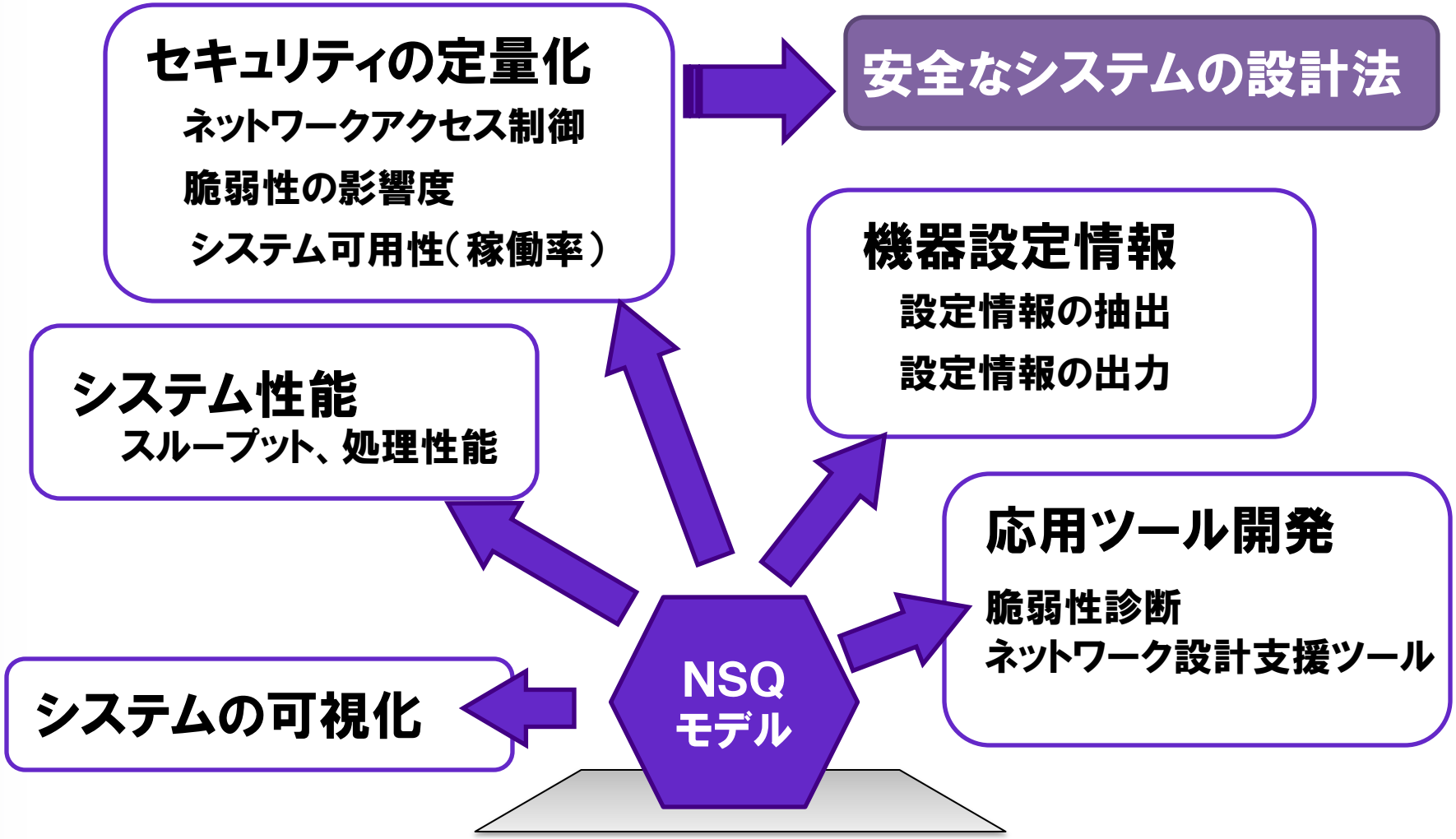
$$\left(\Theta = \frac{(1+0.52391649 \cdot 3)^{52.29806} \cdot 0.43859}{3^{30.11228}} \cdot N \right)$$



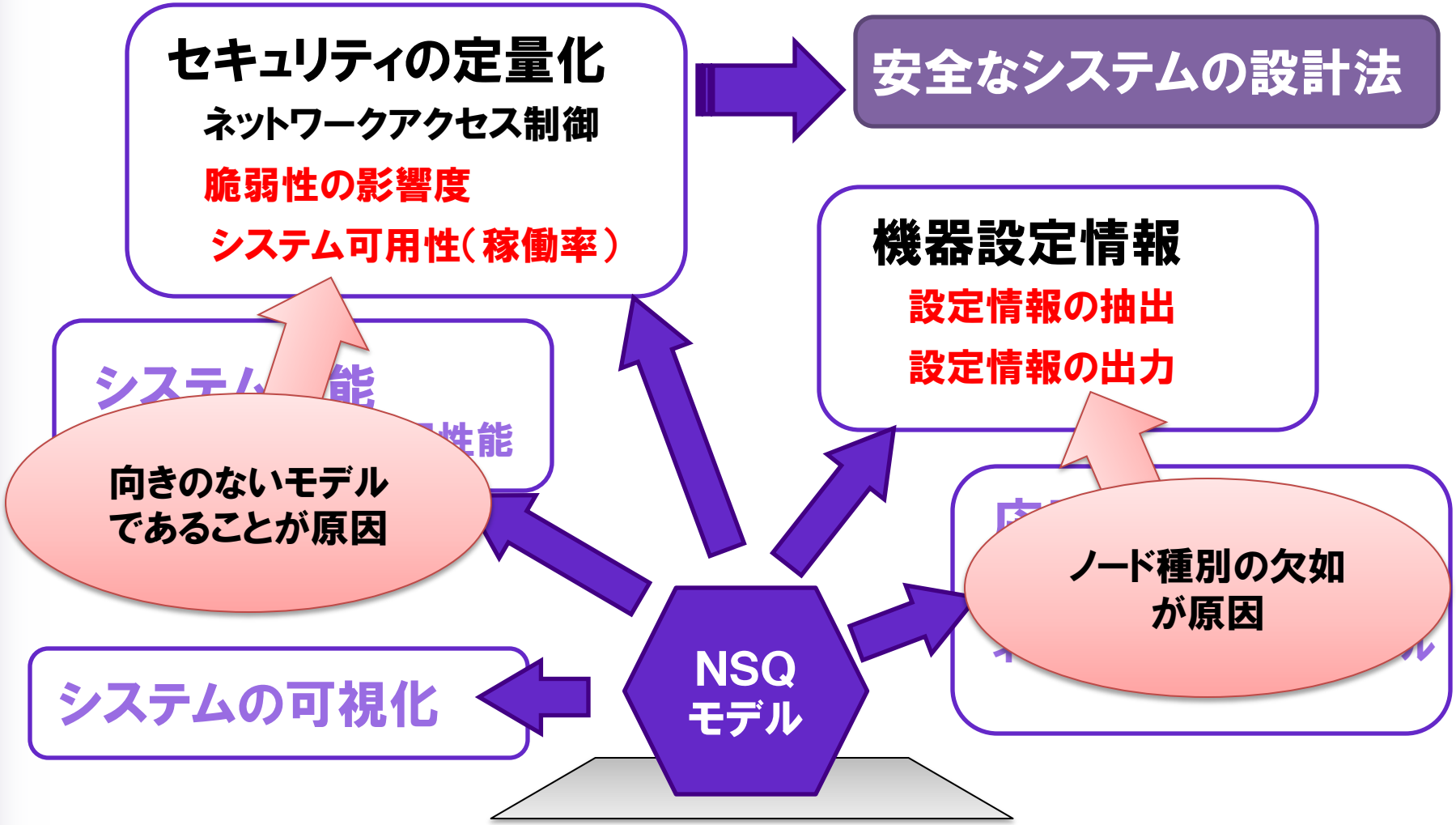
近似関数とのズレを基に評価

$$V = 1 - \varepsilon \frac{\sum_i (y_i - f(x_i))^2}{\sum_i f(x_i)^2}$$

モデル化とデータを中心にした応用



既存モデルの問題点

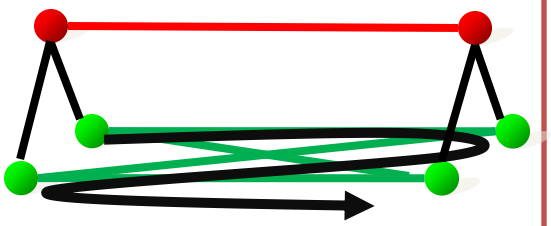

セキュリティの定量化
ネットワークアクセス制御
脆弱性の影響度
システム可用性（稼働率）
安全なシステムの設計法
機器設定情報
設定情報の抽出
設定情報の出力
向きのないモデル
であることが原因
ノード種別の欠如
が原因
NSQ
モデル
システムの可視化

既存モデルの問題点

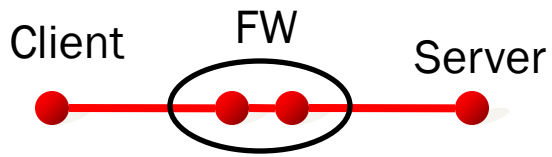
向きのないモデル
であることが原因

脆弱性影響の伝搬ノード探索時に
本来は起きえないループ検知

レイヤ間の依存関係抽出時に
本来は起きえないループ検知



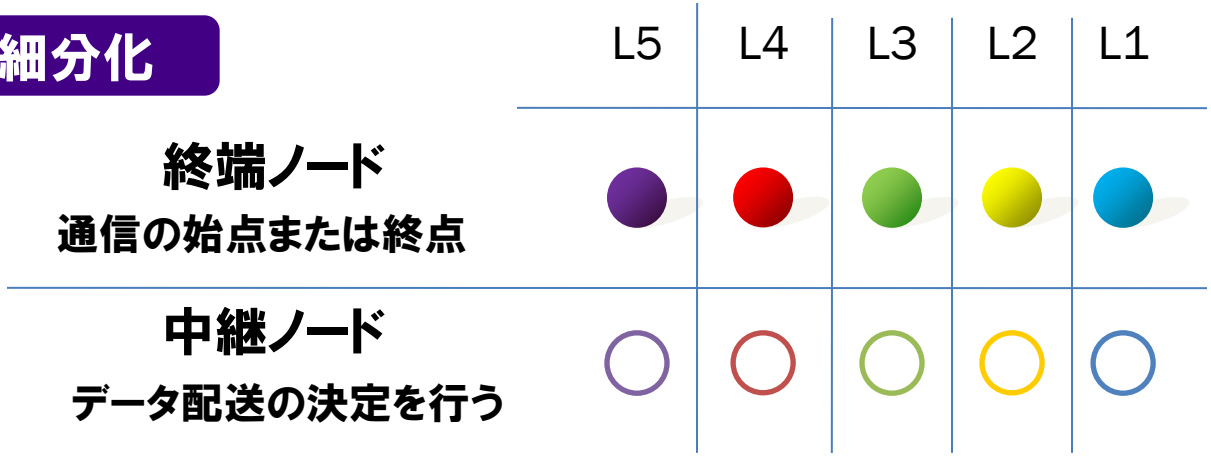
ノード種別の欠如
が原因



Src:Client Dst:Serverの通信を許可/不許可したいが、
FWノードが「中継ノード」である明示がされていないため、
自分自身をSrc／Dstとしてルール排出する

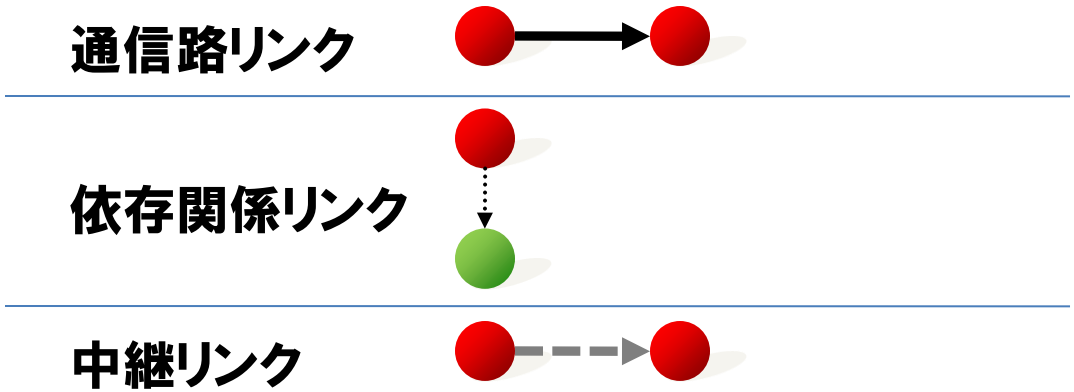
モデルの改良

ノード種別の細分化



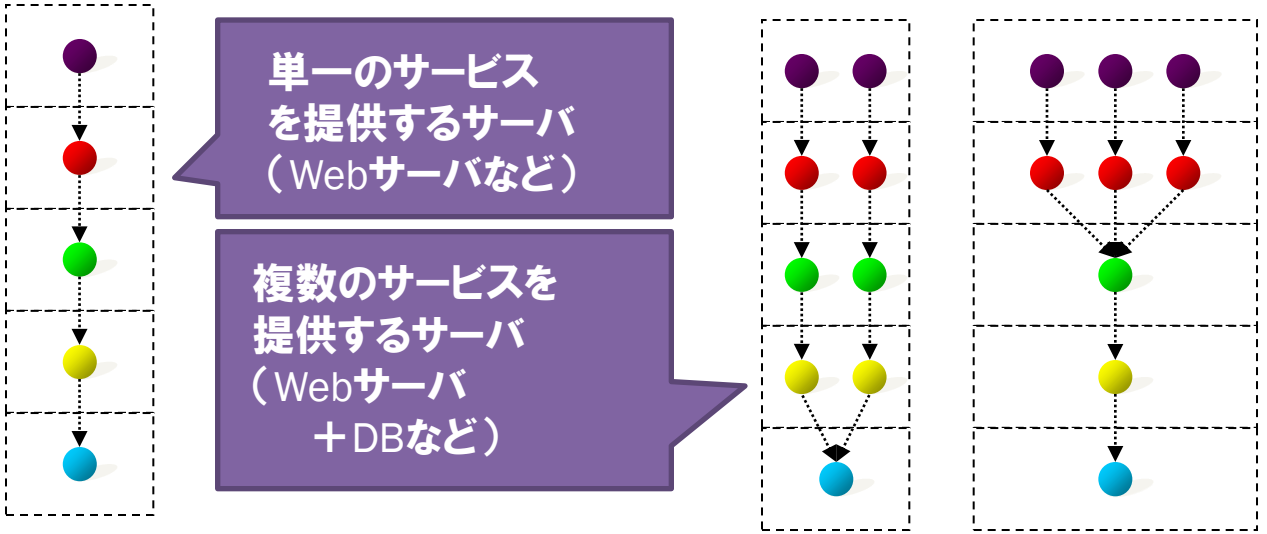
リンク種別の細分化

各リンクの有向化

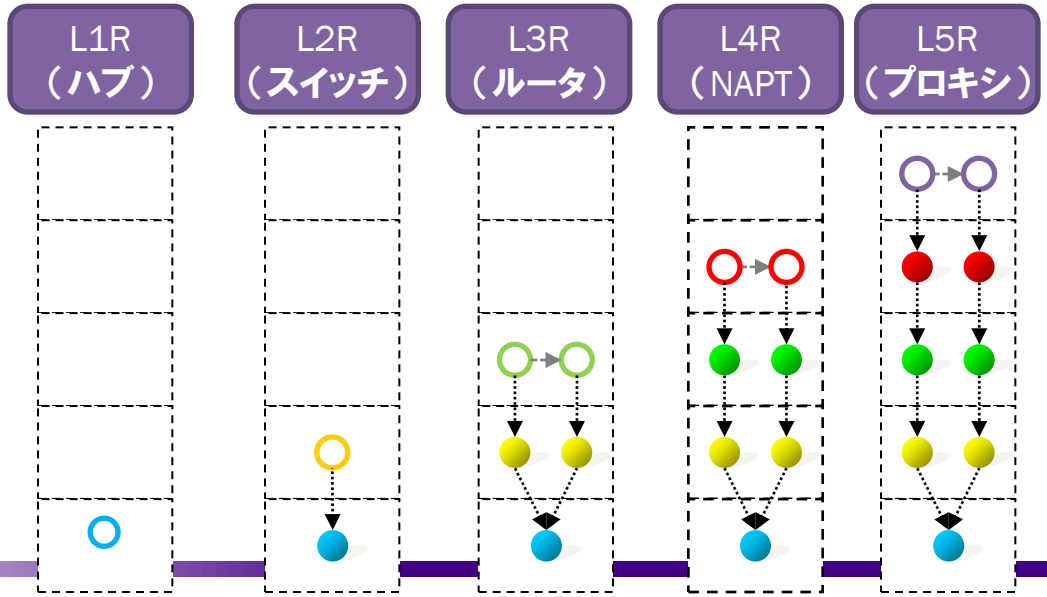


機器(モジュール)例

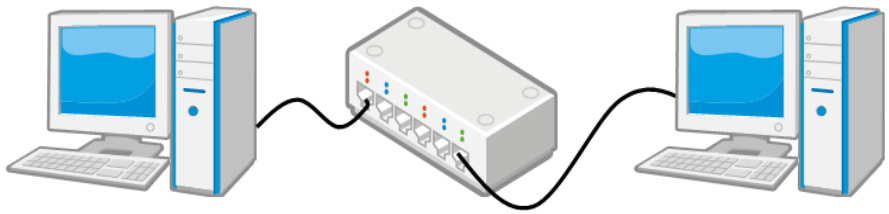
サーバ



中継機器(機能)

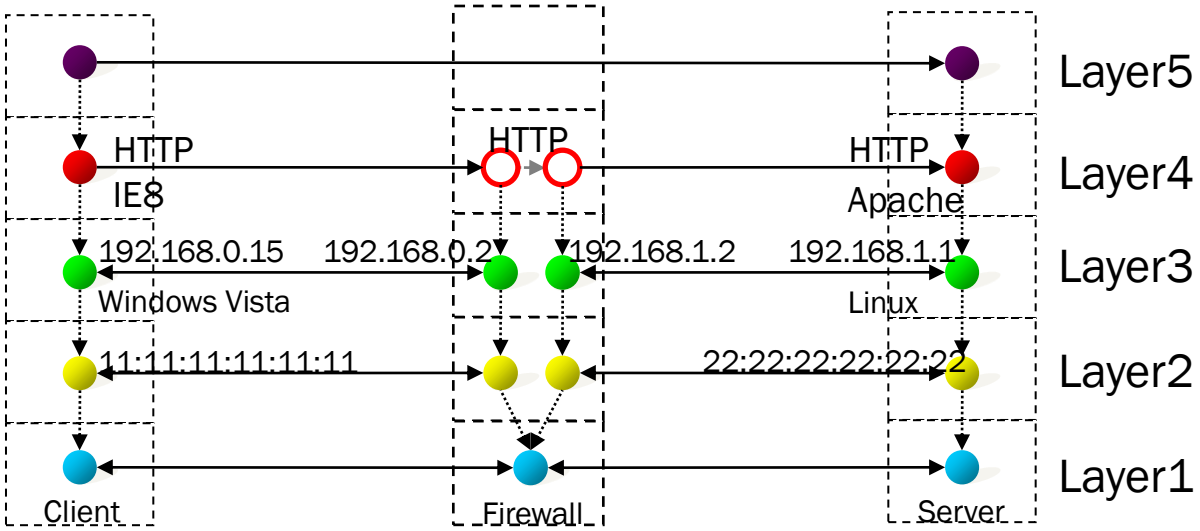


具体例

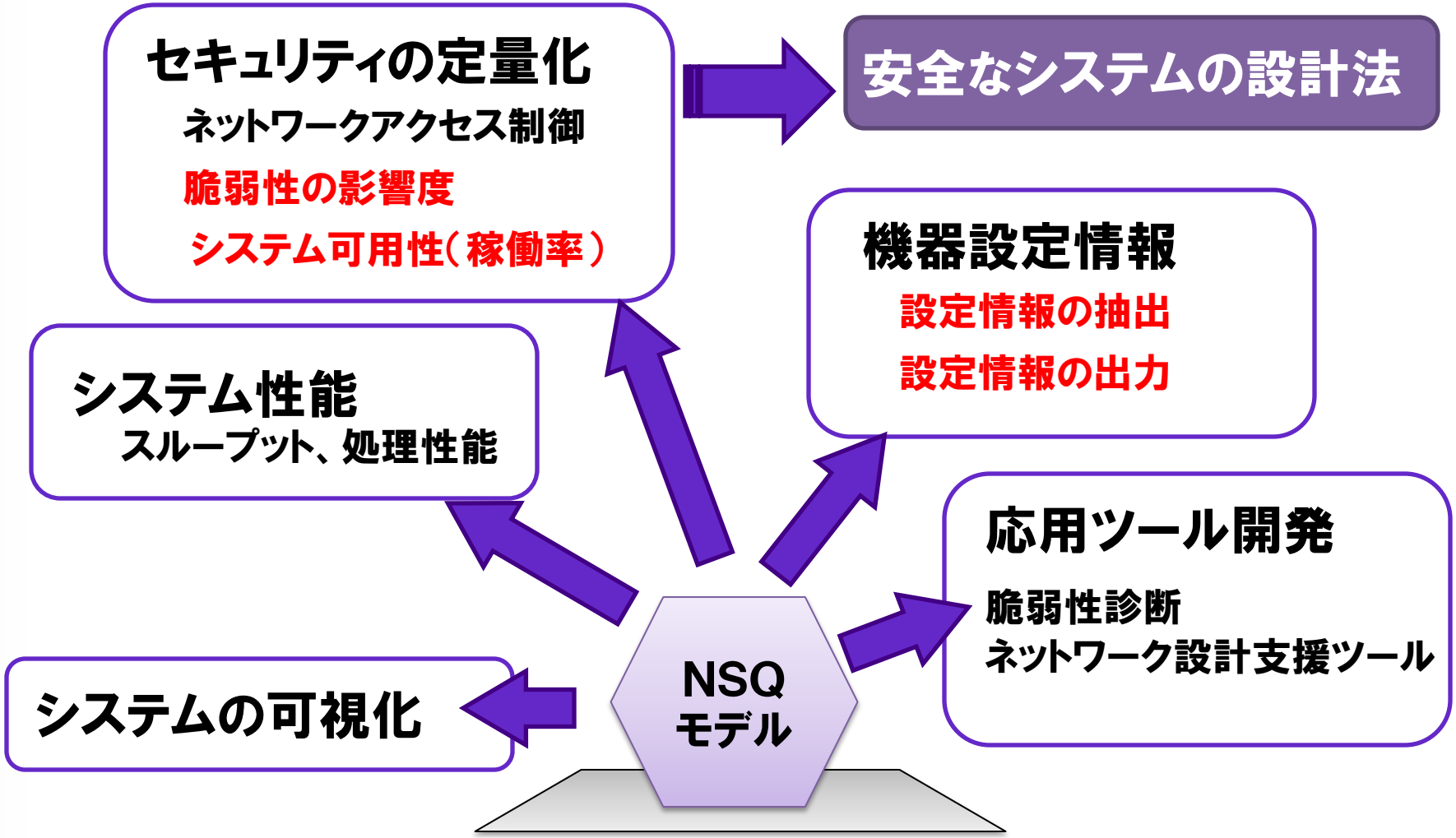


Application: IE8
OS: Windows Vista
IP: 192.168.0.15
MAC: 11:11:11:11:11:11

Service: HTTP
Application: Apache
OS: Linux
IP: 192.168.1.1
MAC: 22:22:22:22:22:22

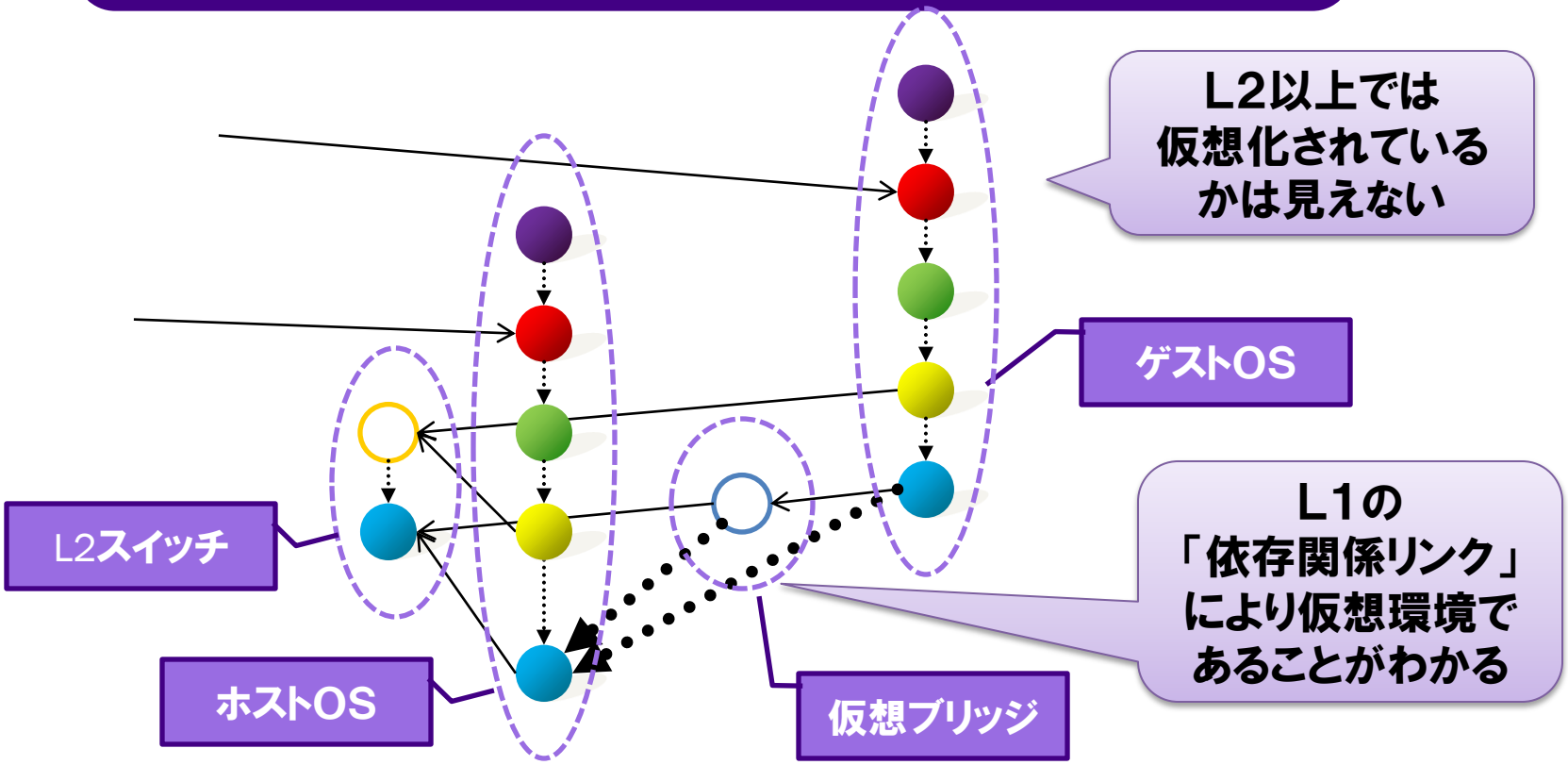


改良による利点


セキュリティの定量化
ネットワークアクセス制御
脆弱性の影響度
システム可用性（稼働率）
安全なシステムの設計法
機器設定情報
設定情報の抽出
設定情報の出力
システム性能
スループット、処理性能
応用ツール開発
脆弱性診断
ネットワーク設計支援ツール
NSQ
モデル
システムの可視化

改良による利点：仮想化への対応

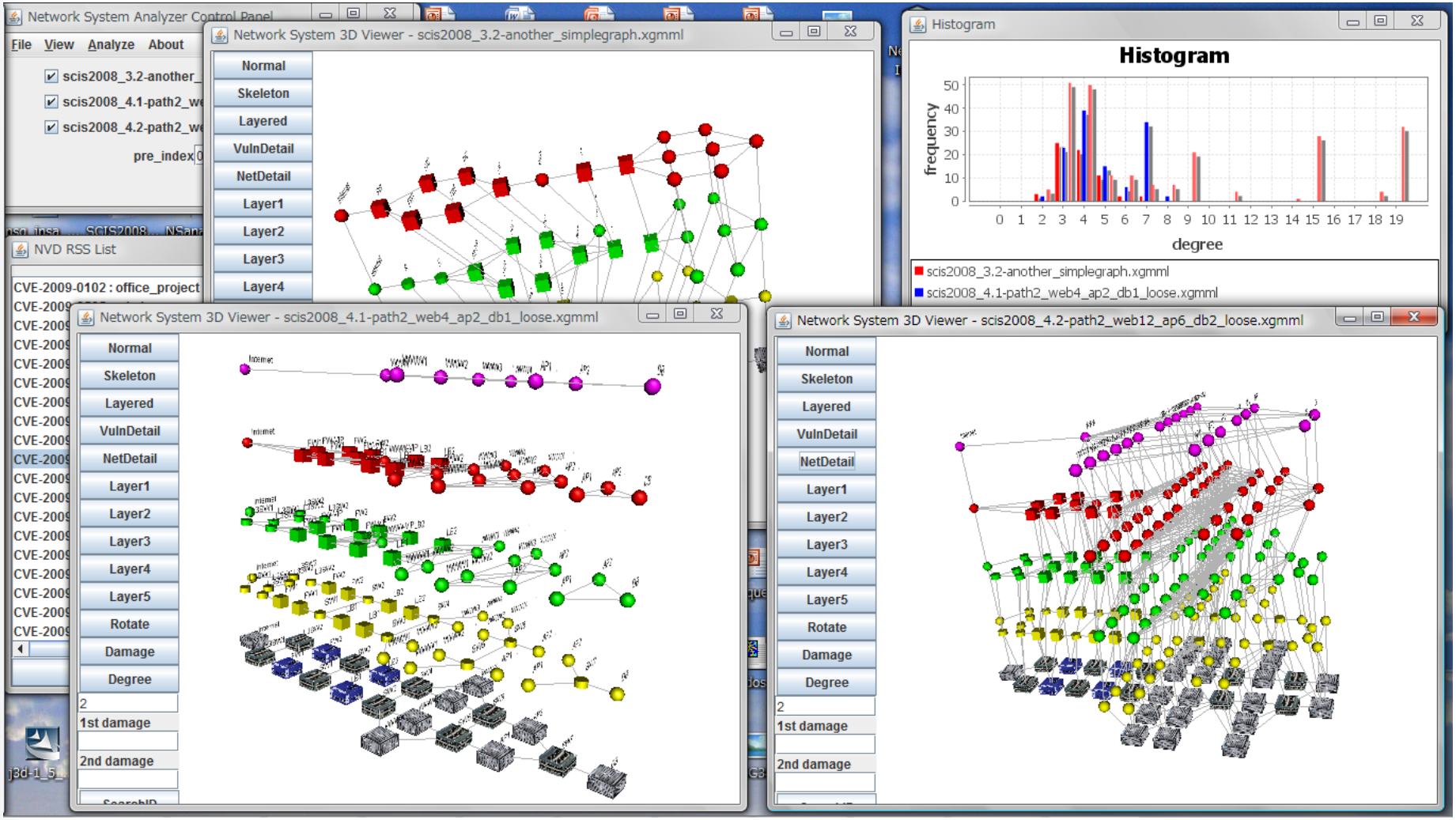
申し訳ありません。この部分は予稿集で
「5.3 仮想化環境への対応」と章立てしてありますが、
文章が書かれておりませんでした。



まとめ

- ネットワークシステムのモデル化と応用
  - マルチレイヤモデル、XMLデータモデル
  - セキュリティの定量評価利用
- 既存モデルの問題点
  - 無向モデルとノード種別の粗さによる、機能実現の困難性
- モデルの改良と改良による利点
  - 有向化、ノード種別・リンク種別の細分化
  - 困難だった機能の実現
  - 仮想化環境への対応

可視化ツールデモ


Network System Analyzer Control Panel
File View Analyze About
scis2008_3.2-another_
scis2008_4.1-path2_we
scis2008_4.2-path2_we
pre_index
NVD RSS List
CVE-2009-0102 : office_project
Network System 3D Viewer - scis2008_3.2-another_simplegraph.xgmml
Normal
Skeleton
Layered
VulnDetail
NetDetail
Layer1
Layer2
Layer3
Layer4
Histogram
Histogram
frequency
degree
scis2008_3.2-another_simplegraph.xgmml
scis2008_4.1-path2_web4_ap2_db1_loose.xgmml
Network System 3D Viewer - scis2008_4.1-path2_web4_ap2_db1_loose.xgmml
Layer5
Rotate
Damage
Degree
1st damage
2nd damage
Network System 3D Viewer - scis2008_4.2-path2_web12_ap6_db2_loose.xgmml

twitter

ホーム　プロフィール　友だちを検索　設定　ヘルプ　ログアウト

ありがとうございました

- メールアドレス
  - kanaoka@cs.tsukuba.ac.jp
- Twitter
  - akirakanaoka

返信

akirakanaoka

Akira KANAOKA