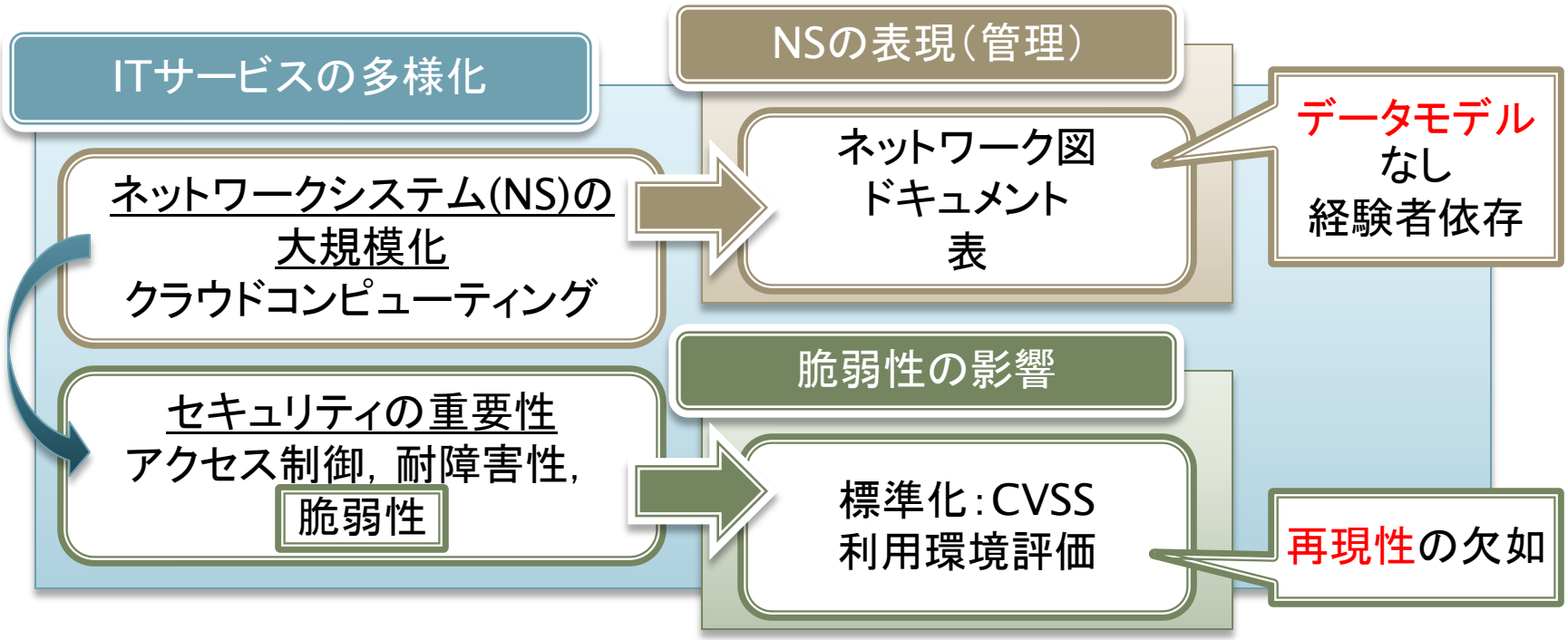
ネットワークシステムにおける CVSSを用いた脆弱性影響特定手法の検討

○原田 敏樹（筑波大）
金岡 晃　（筑波大）
岡本 栄司（筑波大）
加藤 雅彦（IIJテクノロジー）

Outline

1. 背景・目的
2. 脆弱性共通評価手法：CVSS
3. NSQモデル
   - 可用性影響範囲特定
4. 提案手法
5. テストケースによるシミュレーション
6. まとめと今後

背景と目的



CVSSとモデルを用いた再現性のある環境評価

CVSS
(Common Vulnerability Scoring System)

CVSS評価基準一部詳細

- CIA（機密性，完全性，可用性）の評価

なし(N: None)	CIAに影響はない
部分的(P: Partial)	対象のCIAの一部に影響
全面的(C: Complete)	対象のCIA全体に影響

- TD（対象システム範囲）の評価

なし	・対象が存在しない ・対象が物理的に隔離されている
小規模	・利用環境の1～25%にリスク
中規模	・利用環境の26～75%にリスク
大規模	・利用環境の76～100%にリスク

NSQモデル
(Networked-system Security Quantification)

（金岡ら, “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”, SCIS2008 より）

NSQモデル
レイヤ定義

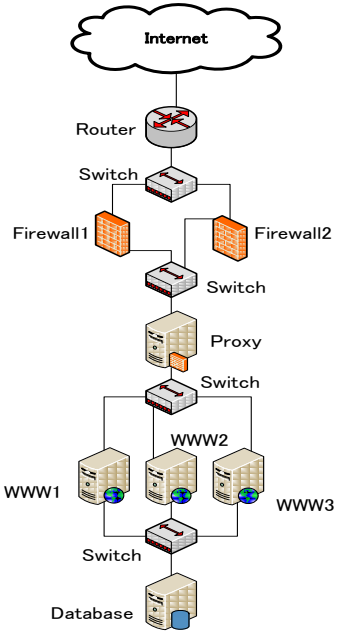
レイヤ5：抽象化サービス（HTTP、DNS、SMTP等）

レイヤ4：TCP/

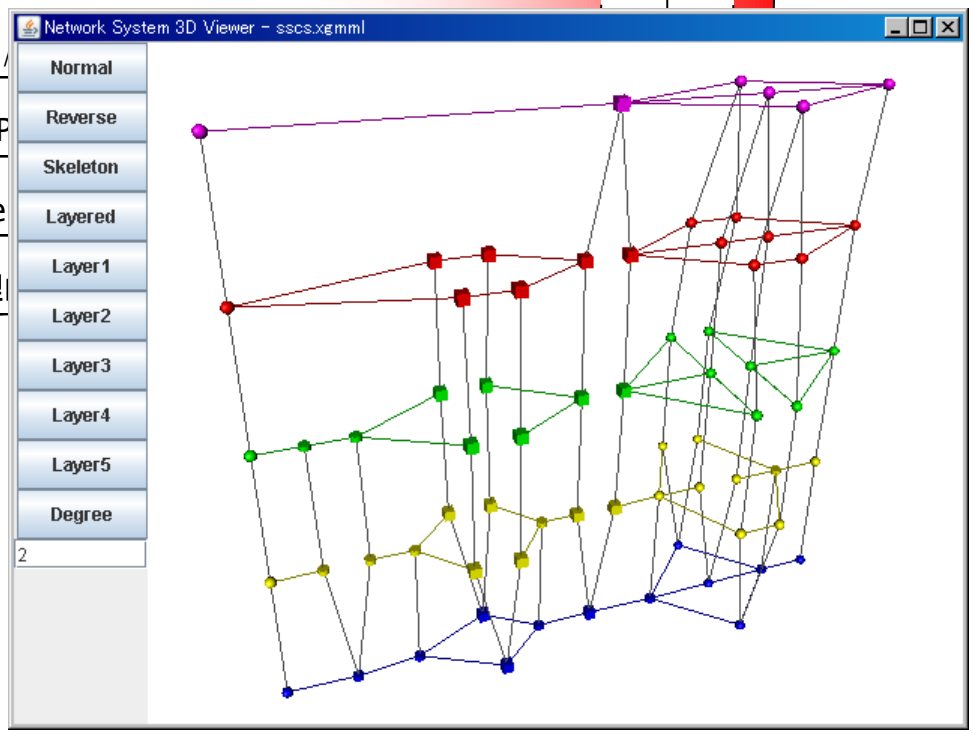
レイヤ3：IP [IP

レイヤ2：Ethe

レイヤ1：物理

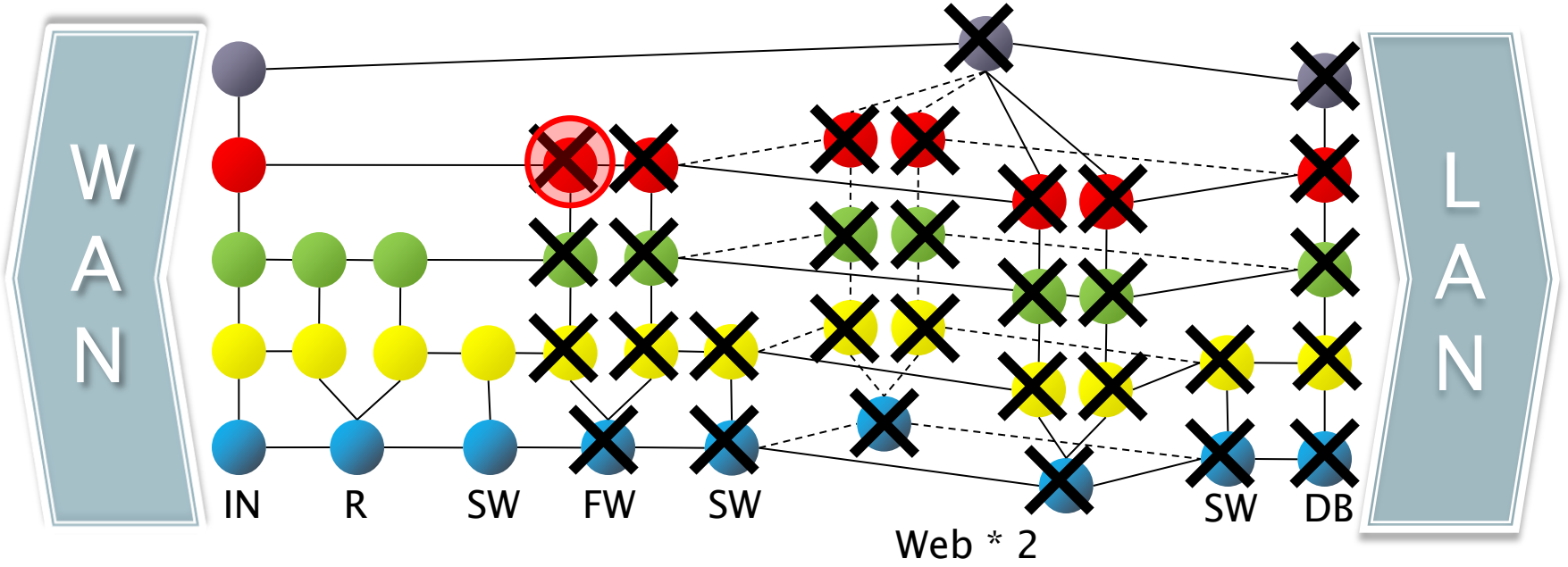


物理接続表現



NSQモデルによる表現

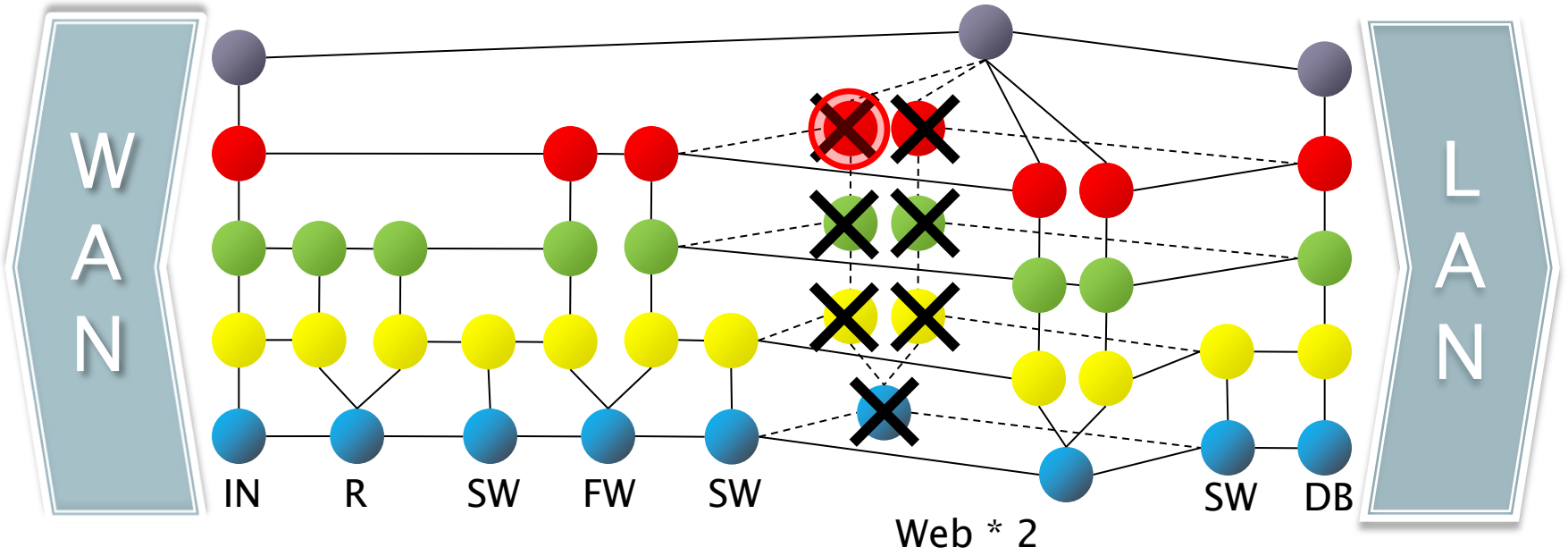
これまでの我々の研究
–可用性影響範囲特定（下流影響あり）–



1. Aに影響のある脆弱性をもつノードに被害
2. リソースが枯渇 ⇒ モジュール全体に被害
3. 冗長化されている？

されていない → 下流（LAN側）の全モジュールに影響

これまでの我々の研究
–可用性影響範囲特定（下流影響なし）–



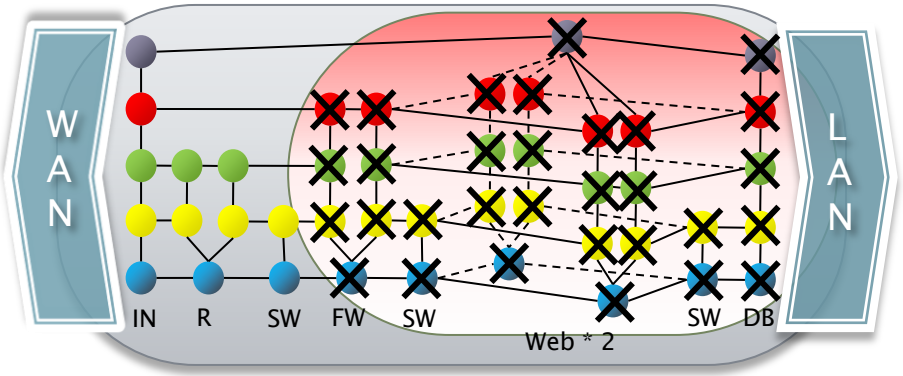
1. Aに影響のある脆弱性をもつノードに被害
2. リソースが枯渇 ⇒ モジュール全体に被害
3. 冗長化されている？

されている ⇒ 下流影響なし

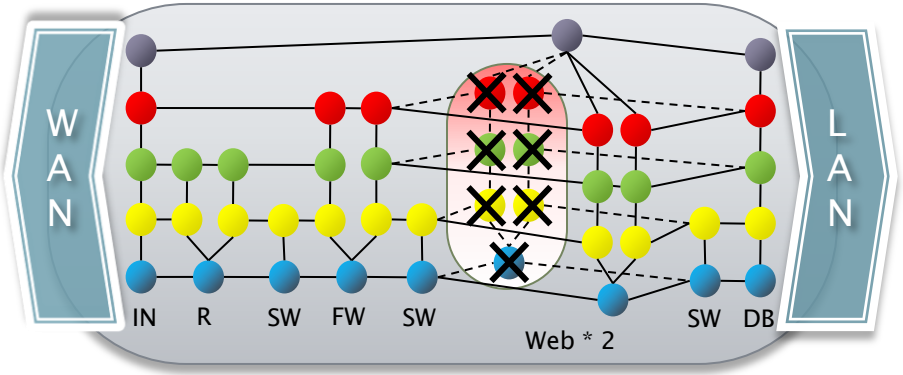
これまでの我々の研究
-TD算出-

N=(全体ノード数)−(INモジュールノード数)＝37
N_A=(可用性影響ノード数)

- 下流影響ありのケース
  - N_A＝30
  - TD＝N_A/N＝30/37
    ＝0.81



- 下流影響なしのケース
  - N_A＝7
  - TD＝N_A/N＝7/37
    ＝0.19



提案手法

- 目的
  - A(可用性)以外の脆弱性影響に対する影響範囲特定
    - C(機密性), I(完全性)
- 手順
  1. 脆弱性情報の実態調査
     - NVD(National Vulnerability Database)の情報を利用
       - 4万件弱の脆弱性情報の一部
     - 脆弱性情報の内容を確認
  2. NSQモデル上での影響範囲を定義

機密性影響調査結果

- C:C (Confidentiality: Complete)
  - サービス停止を引き起こす内容を含む
    - デーモンの停止
    - クラッシュやハングアップ
    - デバイスのリセット

    → 可用性(A)への影響が考えられる
  - その他ソースコードやパスワードの閲覧など(C:Pと同様)
- C:P (Confidentiality: Partial)
  - 被害は情報漏洩にとどまる
    - 任意のファイルの閲覧
    - データベースファイルのダウンロード
    - 機密情報の漏洩など

    → サービスへの影響

完全性影響調査結果

- I:C (Integrity: Complete)
  - 任意ファイルの新規・上書き
  - スプーフィング
  - メールの改ざんなど
- I:P (Integrity: Partial)
  - クロスサイトスクリプティング

対象もしくは対象より上位の機能・サービスへの影響
サービス利用者への影響

各影響範囲の定義

	全面的 (Complete)	部分的 (Partial)
C (機密性)	モジュール全体(L1～L4) 冗長化有無で下流影響	攻撃対象ノード以上 (冗長性関わらずL5を含む)
I (完全性)	攻撃対象ノード以上 (冗長性関わらずL5を含む)	攻撃対象ノード以上 (冗長性関わらずL5を含む)
A (可用性)	モジュール全体(L1～L4) 冗長化有無で下流影響	モジュール全体(L1～L4) 冗長化有無で下流影響

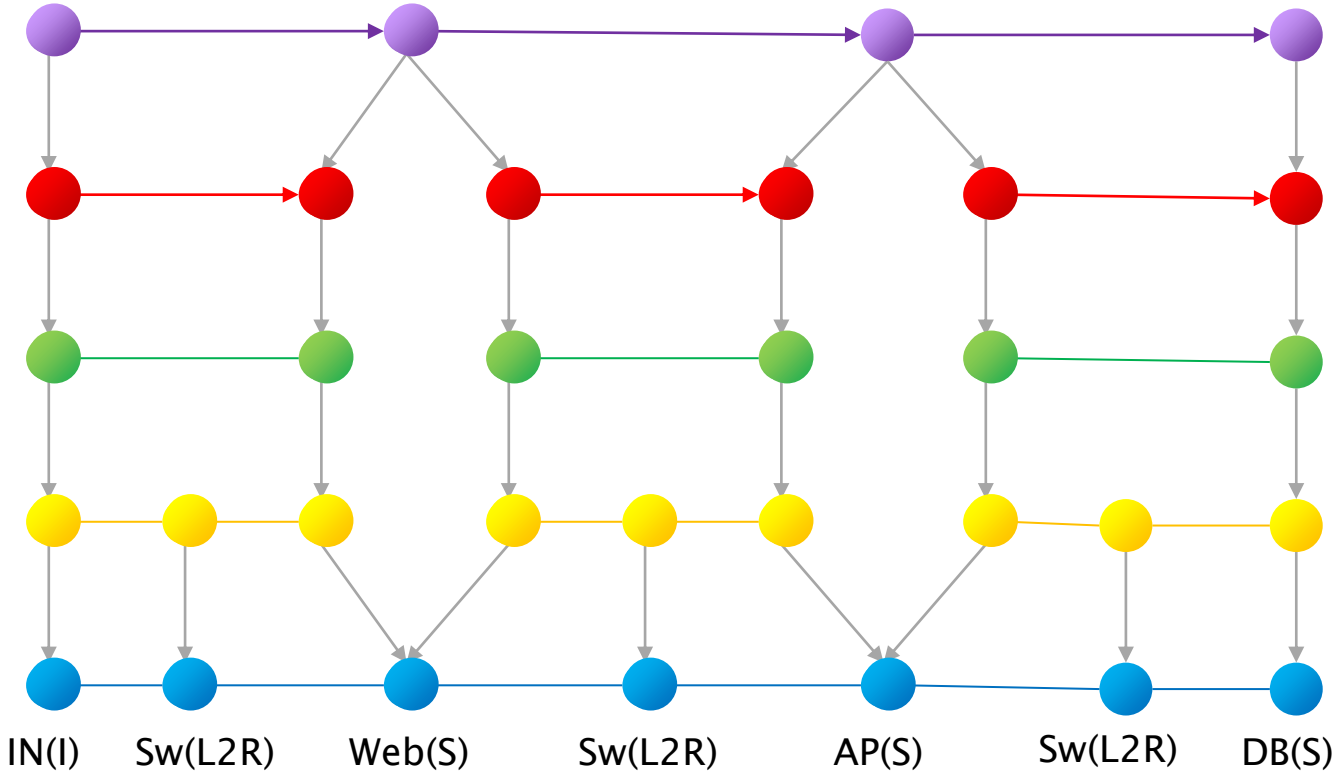
脆弱性影響範囲のタイプを2種に分類

1. 可用性影響あり (C:C, A:C, A:P)
2. 可用性影響なし (C:P, I:C, I:P)

テストケースによるシミュレーション

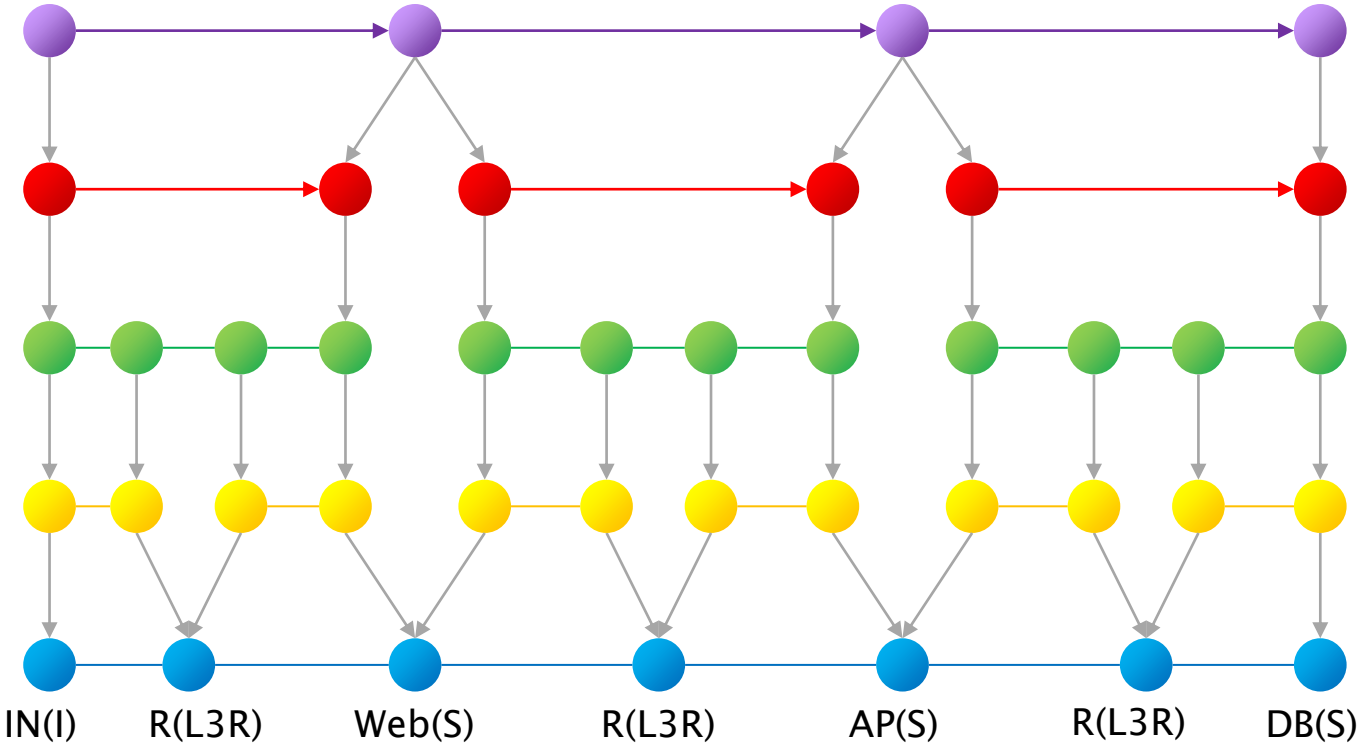
- 目的
  - 提案手法により特定される影響範囲の調査
  - 影響範囲の観点から，重要性の高い機器を考察
- 対象
  - Webサーバ，アプリケーションサーバ，データベースサーバの3つのサーバからなる三層構造のNS
  - 中継機器の種別，冗長性の有無により4つのケースに分類
    - ケースX, ケースY, ケースZ, ケースZ’
- 内容
  - 上記4つのテストケースのL3およびL4ノードに脆弱性が存在した際の影響範囲（影響ノード数）を測定

ケースX



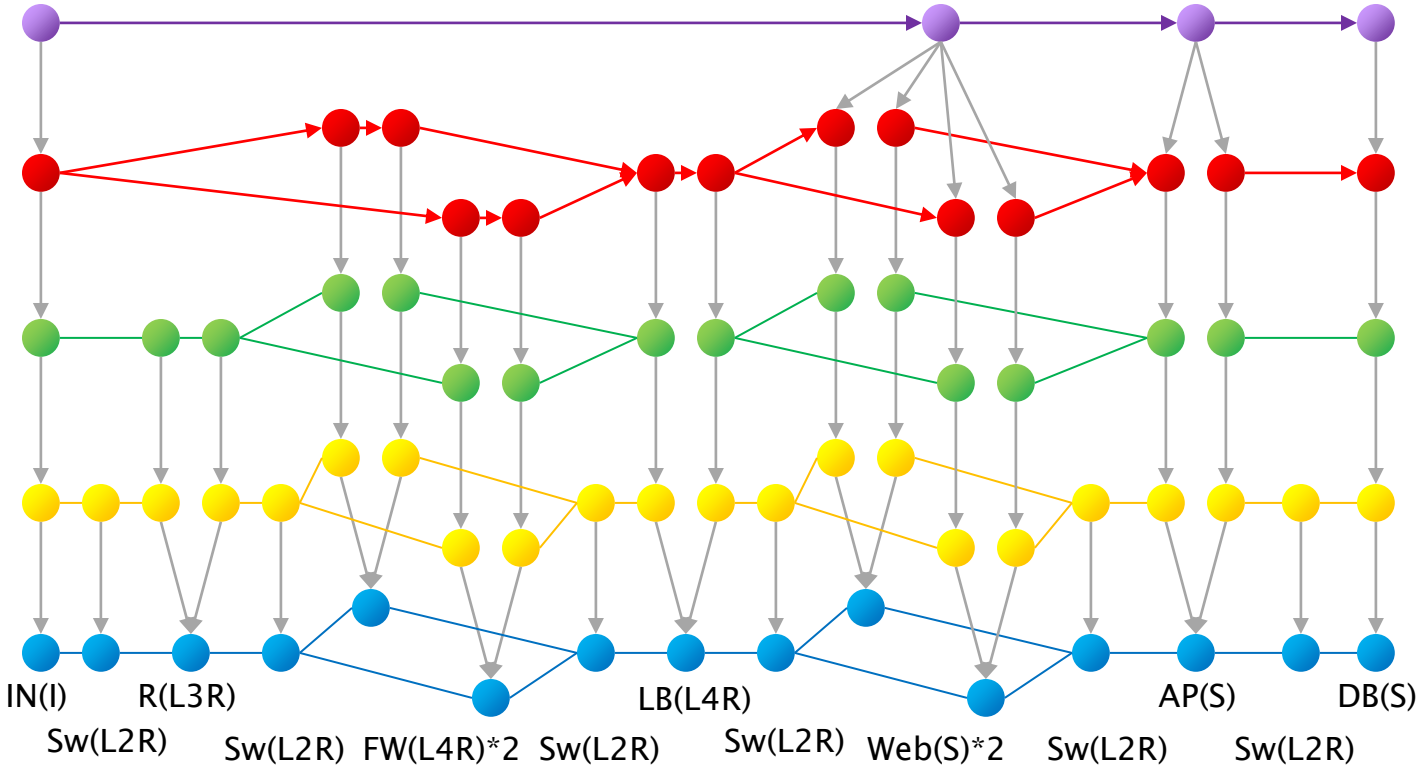
•3つのサーバをスイッチ(L2R)で中継して直列に接続

ケースY



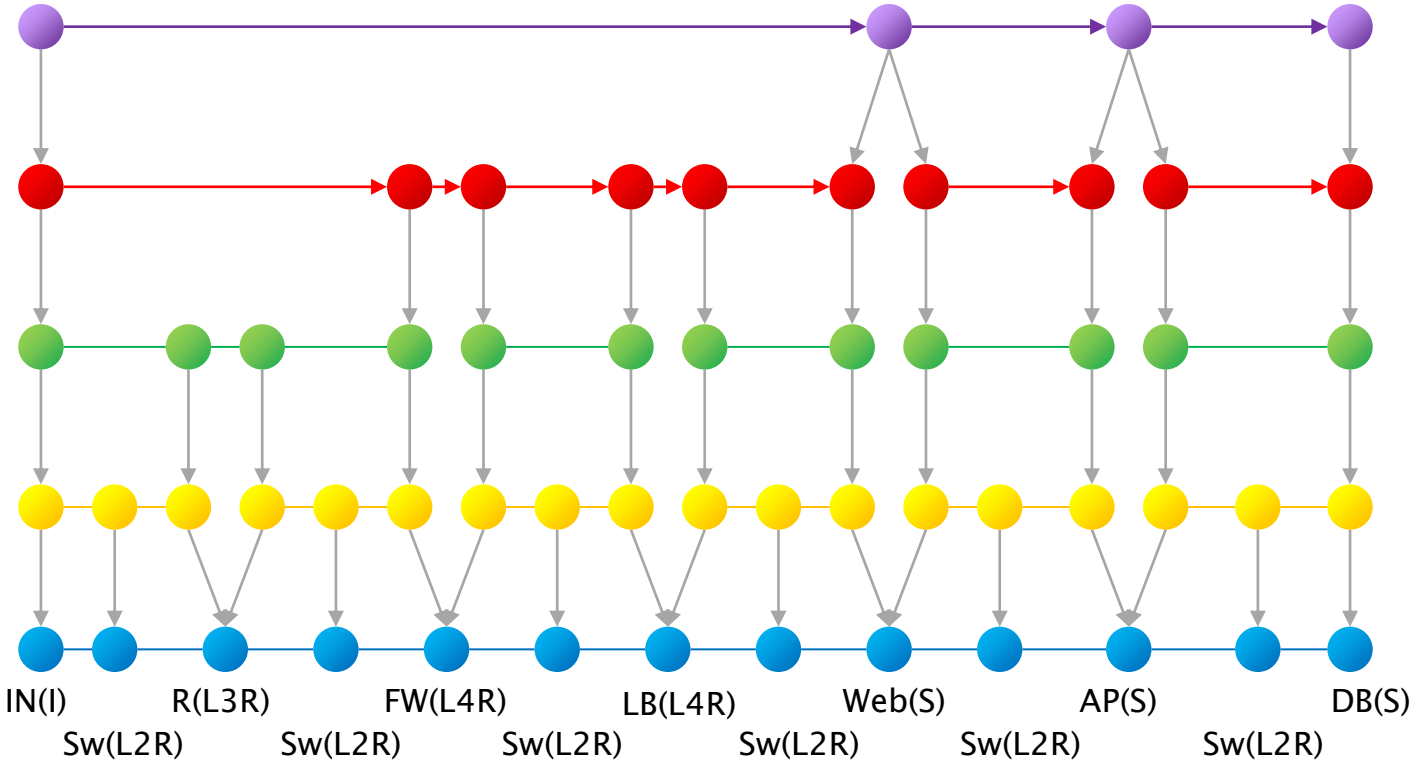
•ケースXの中継機器をルータ(L3R)に変更

ケースZ



- ルータ→ファイアウォール→ロードバランサ→サーバ群
- ファイアウォール，Webサーバを冗長化
- 上記モジュール間はスイッチで中継
- 最も一般的な構成

ケースZ’



- ケースZの冗長性を排除

結果

nA: 可用性影響なし(C:P, I:C, I:P)
ノード数割合

A: 可用性影響あり(C:C, A:C, A:P)
ノード数割合

- *nA*平均
  - 構成毎の変化見られず
  - ケースZ→Z'で若干減少
    - L5ノードへの影響
- *A*平均
  - 全体平均
    - ケースX→Yの増加
      - ✓ さらされ易さ増加
    - ケースZ, Z'間の差
      - ✓ 冗長化の効果
  - モジュールタイプ別平均
    - ✓ 中継機器 ＞ サーバ

	ケースX	ケースY	ケースZ	ケースZ'
全体平均				
nA	32.4%	32.6%	30.1%	28.4%
A	62.5%	83.7%	73.4%	81.5%
レイヤ別*nA*平均				
L3	37.6%	36.0%	32.2%	31.0%
L4	33.9%	33.7%	30.5%	29.0%
モジュールタイプ別*A*平均				
S	77.2%	87.6%	75.4%	83.5%
L3R	N/A	90.6%	85.6%	98.1%
L4R	N/A	N/A	78.7%	88.9%

まとめと今後

- まとめ
  - CVSSの機密性・完全性評価の実態調査
  - モデル上の機密性・完全性の脆弱性影響範囲を定義
  - 影響範囲測定
    - 冗長化効果および中継機器における可用性影響の大きさを確認
    - 機密性・完全性影響の評価困難　⇒　他の評価尺度
- 今後
  - 実ネットワークトポロジの評価
  - 仮想環境に対応した影響範囲特定手法の検討