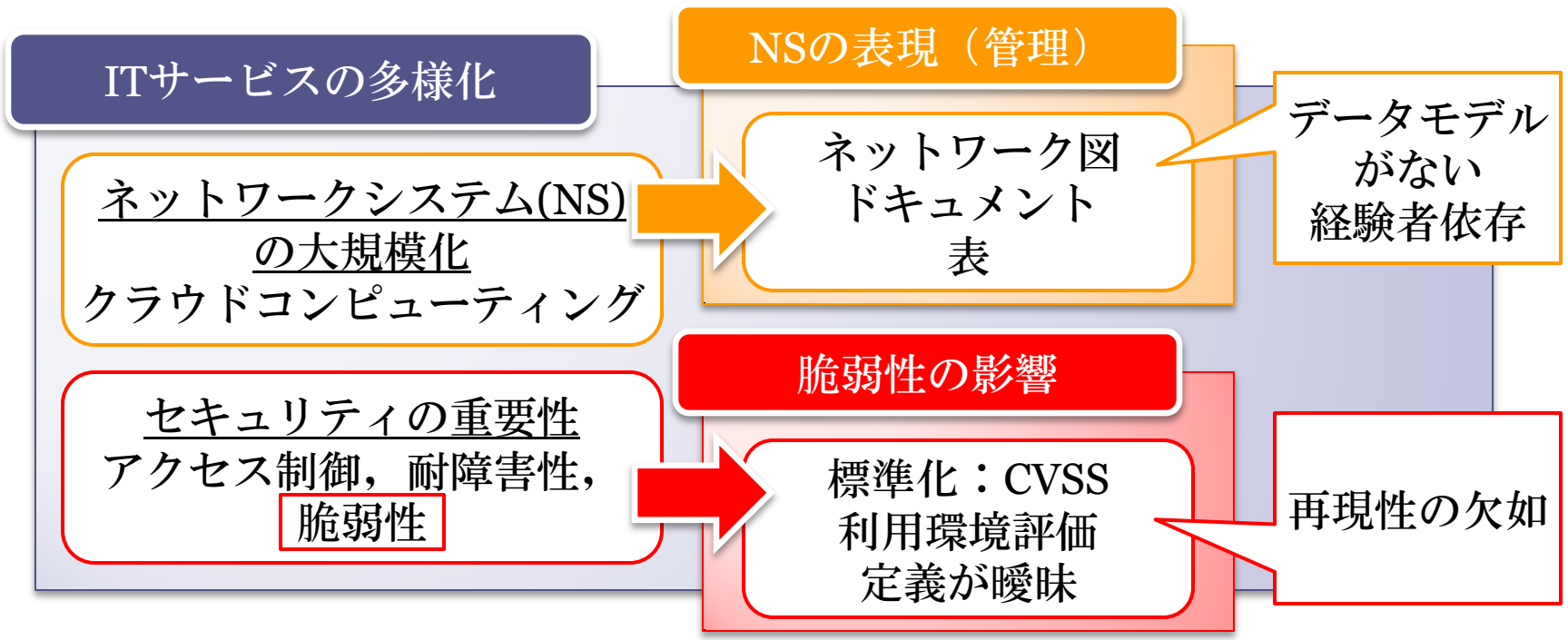
CVSSを用いたネットワークシステムの危険度測定手法の検討

○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. CVSS関連研究
4. NSQモデル
5. 提案手法
   - CVSSとNSQモデルの相互適用
6. まとめ

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各値の性質と現状

基本値（Base Score）

- 値は変化しない
- 第３者機関による提供が可能

現状値（Temporal Score）

- 値は時間により変化
- 運用が非常に困難
  - 35,000を超える脆弱性情報の定期的更新

環境値（Environmental Score）

- 値は利用環境により変化
  - 対応決定の指標
- 定義の曖昧さから利用が困難

CVSS各値の現状と性質

基本値（Base Score）

- 値は変化しない
- 第３者機関による提供が可能

現状値（Temporal Score）

- 値は時間により変化
- 運用が非常に困難
  - 35,000を超える脆弱性情報の定期的更新

環境値（Environmental Score）

- 値は利用環境により変化
  - 対応決定の指標
- 定義の曖昧さから利用が困難

CVSS関連研究（1）

- [FMFP06] S. Frei, M. May, U. Fiedler and B. Plattner, *"Large-Scale Vulnerability Analysis"*, 2006
  - 脆弱性のライフサイクルから危険度を評価
    - 攻撃手法確立～対策パッチ公開の期間＝高リスク
    - 脆弱性情報公開日との時間差を統計的に分析（数式近似）
- [WZX08] J. A. Wang, F. Zhang and M. Xia, *"Temporal metrics for Software Vulnerabilities"*, 2008
  - CVSS各値算出方法の変更
    - CVSS算出過程での感覚的な違和感を解消
- [SM08] K. Scarfone and P. Mell, *"Vulnerability Scoring for Security Configuration Settings"*, 2008
  - CCE（Common Configuration Enumeration）で識別された設定上のセキュリティ問題を評価
    - CVSS基本評価基準を応用

CVSS関連研究（2）

- [CSTH08] K. Clark, E. Singleton, S. Tyree and J. Hale, *"Strata-Gem: Risk Assessment Through Mission Modeling"*, 2008
  - あるミッションにおける個々の目的や資産、危機的状況を関連付けたツリーによるフォルトツリー分析
    - リスク算出のパラメータとしてCVSS基本値を利用
- [AAP07] M. D. Aime, A. Atzeni and P. C. Pomi, *"AMBRA – Automated Model-Based Risk Analysis"*, 2007
  - ベストプラクティスとCVSS基本値でNSのリスク分析を自動化
    - NS内のCVSS基本値の総和を３段階で評価
- [LH07] Y. P. Lai and P. L. Hsia, *"Using the vulnerability information of computer systems to improve the network security"*, 2007
  - アクセス制御とCVSS基本値を用いたセキュリティ定量化
    - 隔離前後におけるネットワーク内の脆弱性数とCVSS基本値の総和の差によりセキュリティ向上の割合を導出

調査結果のまとめと考察

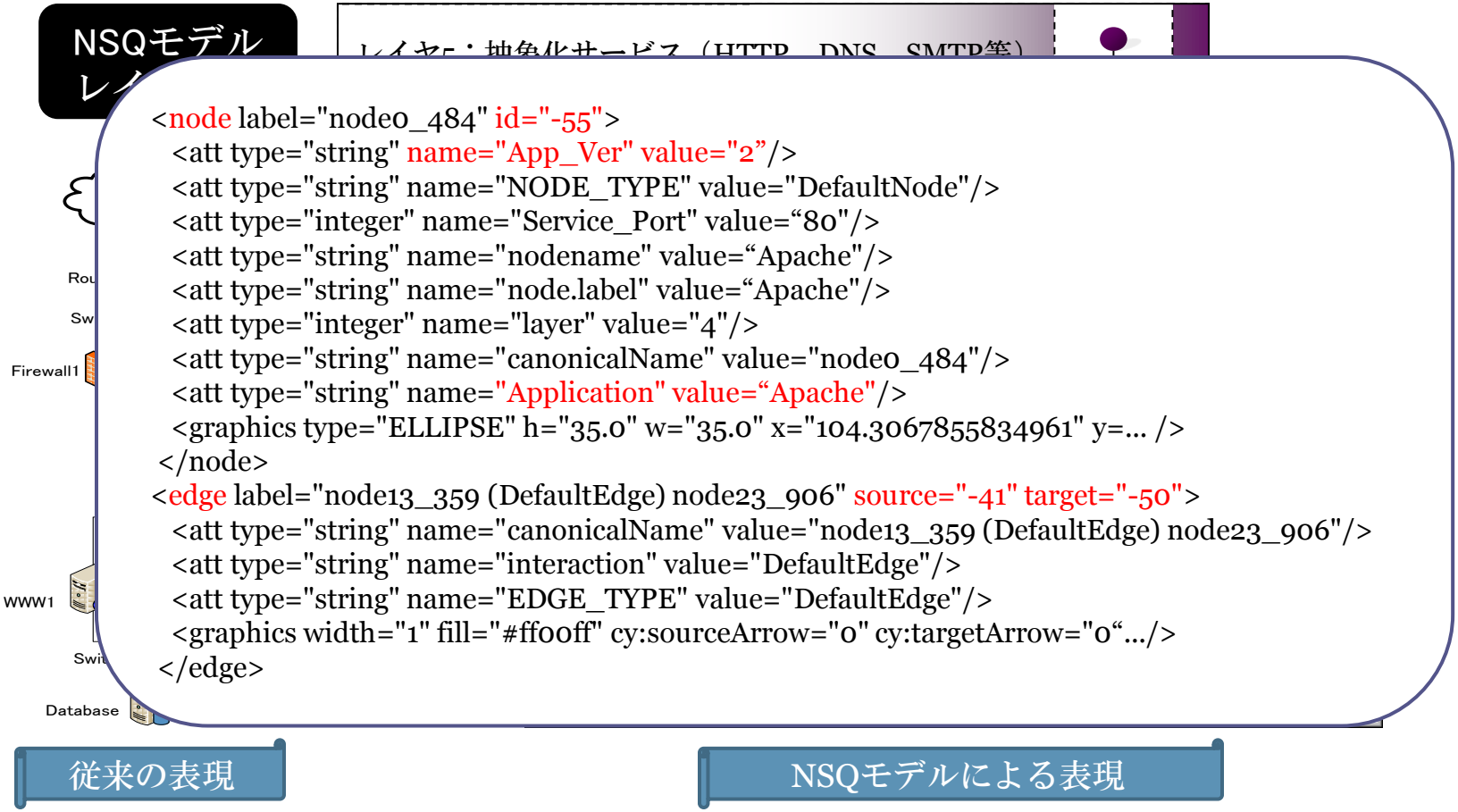
	FMFP06	WZX08	SM08	CSTH08	AAP07	LH07
基本値	×	○	○	○	○	○
現状値	△	○	×	×	×	×
環境値	×	○	×	△	△	△

- [FMFP06]
  - 時間的な脆弱性の危険度を統計分析
- [WZX08]
  - CVSSそのものを変更
- [SM08]
  - CVSS基本評価基準を異なるタイプのセキュリティ問題へ応用
- [CSTH08], [AAP07], [LH07]
  - CVSS基本値の独自利用によるシステム／ネットワークのリスク分析
  - 環境値を利用していない

CVSS環境値に相当するものを
CVSS基本値を用いて独自に算出

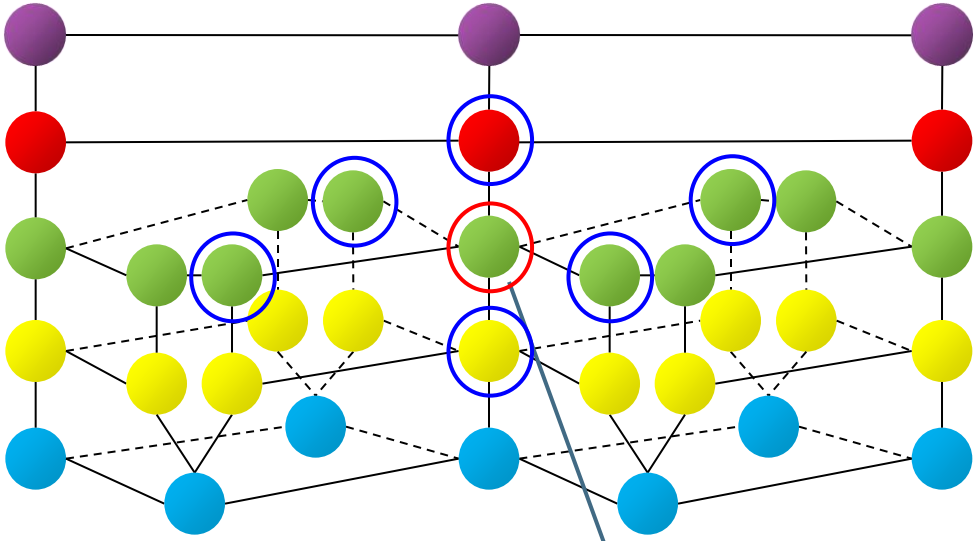
NSQモデル (Networked-system Security Quantification)

（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モデルとCVSSの対応

（加藤ら，”ネットワークシステムにおける脆弱性影響度の定量化と可視化，” CSS2008 より）



加藤らによる提案手法

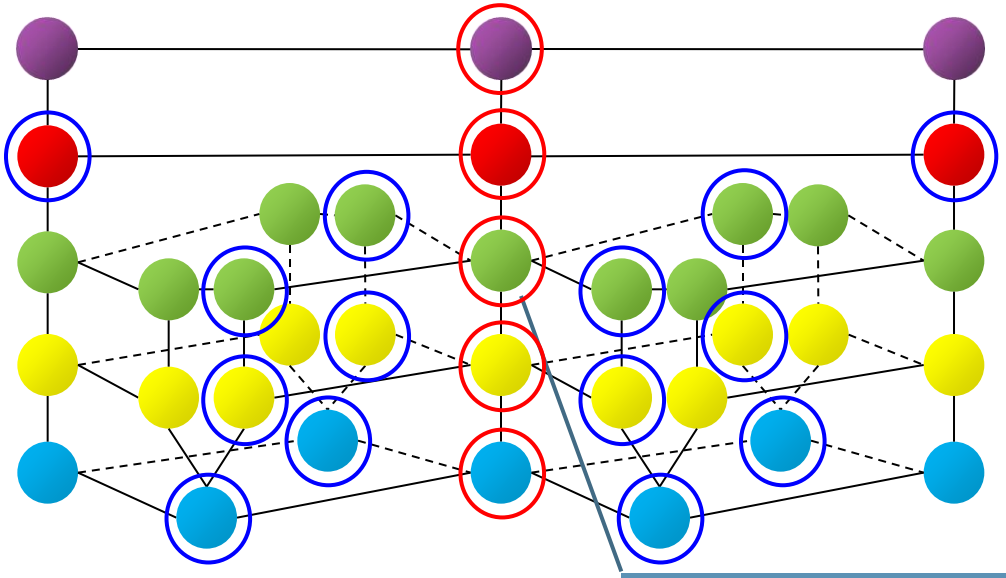
脆弱性の発見されたノード

- CVSS基本評価基準：C・I・Aへの影響の程度は？

部分的 ⇒ 脆弱性をもつノードに一次被害、その隣接ノードに二次被害

NSQモデルとCVSSの対応

（加藤ら，”ネットワークシステムにおける脆弱性影響度の定量化と可視化，” CSS2008 より）



加藤らによる提案手法

脆弱性の発見されたノード

- CVSS基本評価基準：C・I・Aへの影響の程度は？

部分的 ⇒ 脆弱性をもつノードに一次被害、その隣接ノードに二次被害

全面的 ⇒ 脆弱性を持つノードを含むモジュール全体に一次被害、
そのモジュールに隣接するノードに二次被害（レイヤ５を除く）

加藤らによる提案手法

- 課題
  - C・I・Aの差異を未考慮
    - 特に可用性(A)への影響範囲は要検討
- CDP（二次被害）の定義にギャップ
  - 加藤ら：対象が影響を受けた際の周囲への影響
  - CVSS：物理的機器への被害、生産基盤、身体などへ及ぼす二次的な被害

提案手法

ねらい

- 影響範囲の変化を検討
  - A（可用性）に関して検討
  - 通信の方向（上り／下り）を考慮

Aとは

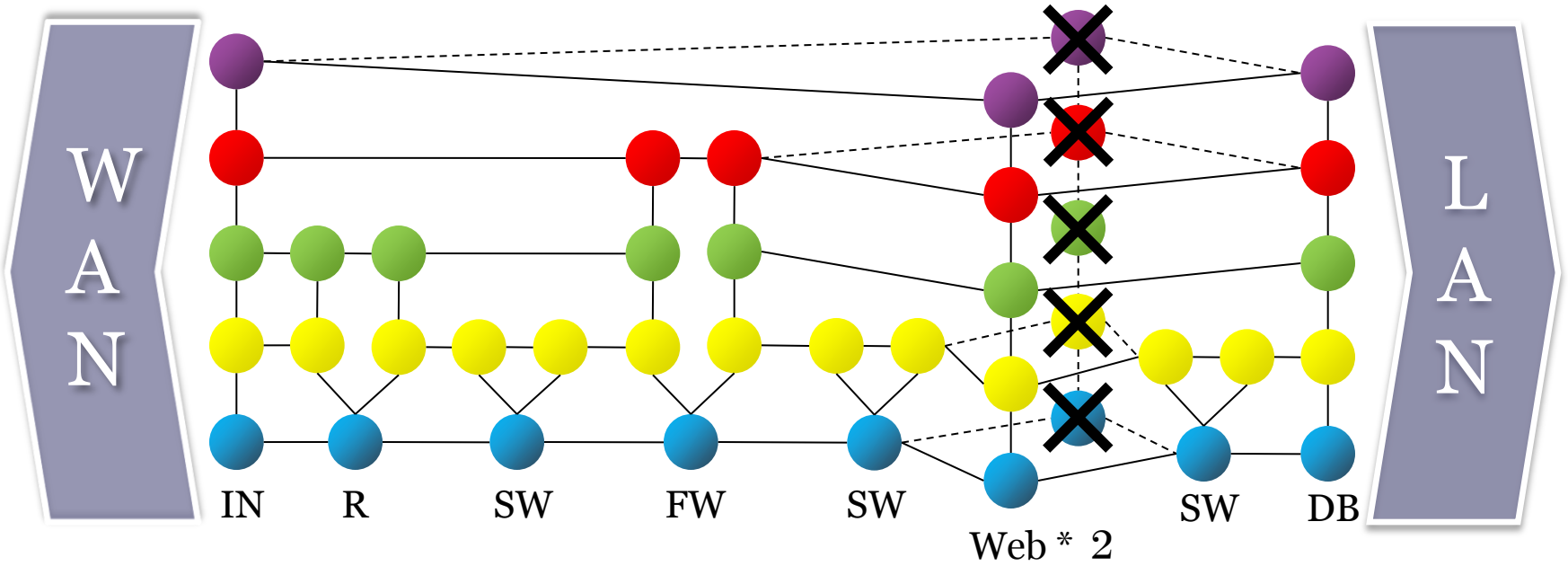
IPA（情報処理推進機構）：CVSS v2概説より

- 脆弱性を攻撃された際に、対象システム内の業務が遅延・停止する可能性を評価
  - 部分的：リソースを一部枯渇させることが可能
    業務の遅延や一時中断が可能
  - 全面的：リソースを完全に枯渇させることが可能
    システムを完全に停止させることが可能

手法概要

- 部分的／全面的の差により影響範囲は変化しない
- 上流(WAN側)の影響は下流(LAN側)まで影響
- 周囲システムの影響をTD(対象システム範囲)に含める

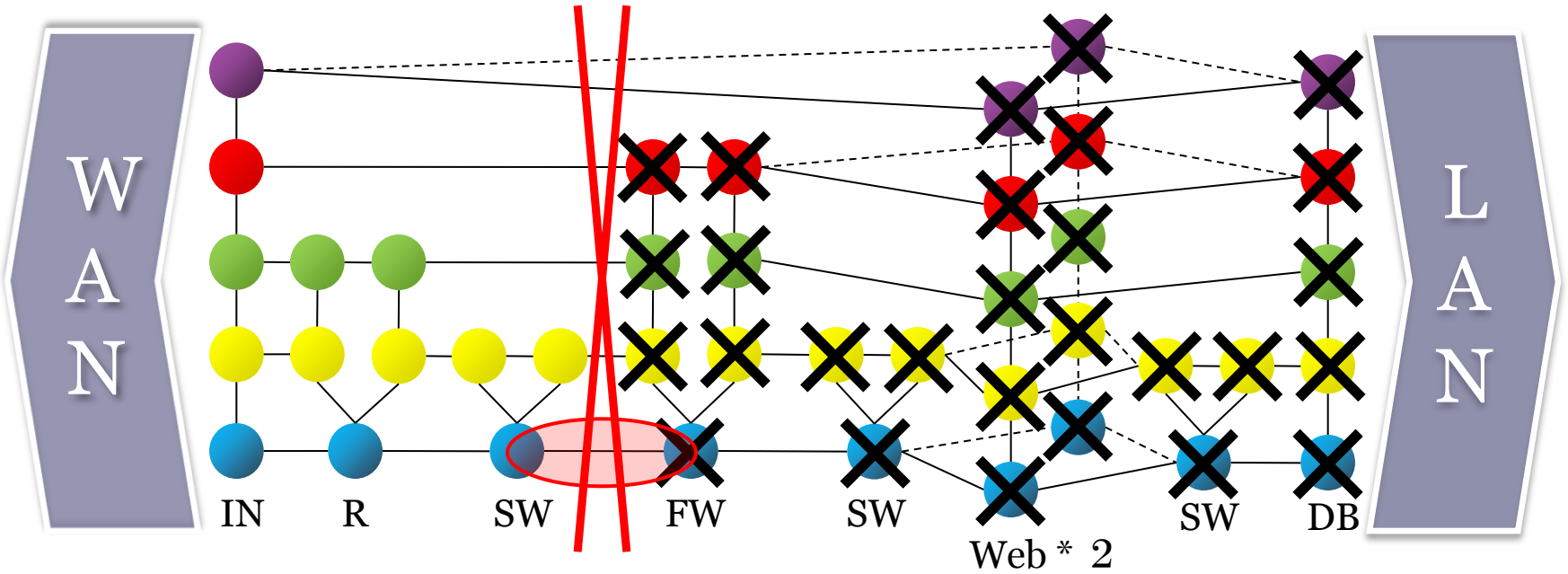
手法適用例（被害小）



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　影響拡大なし

手法適用例（被害大）



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

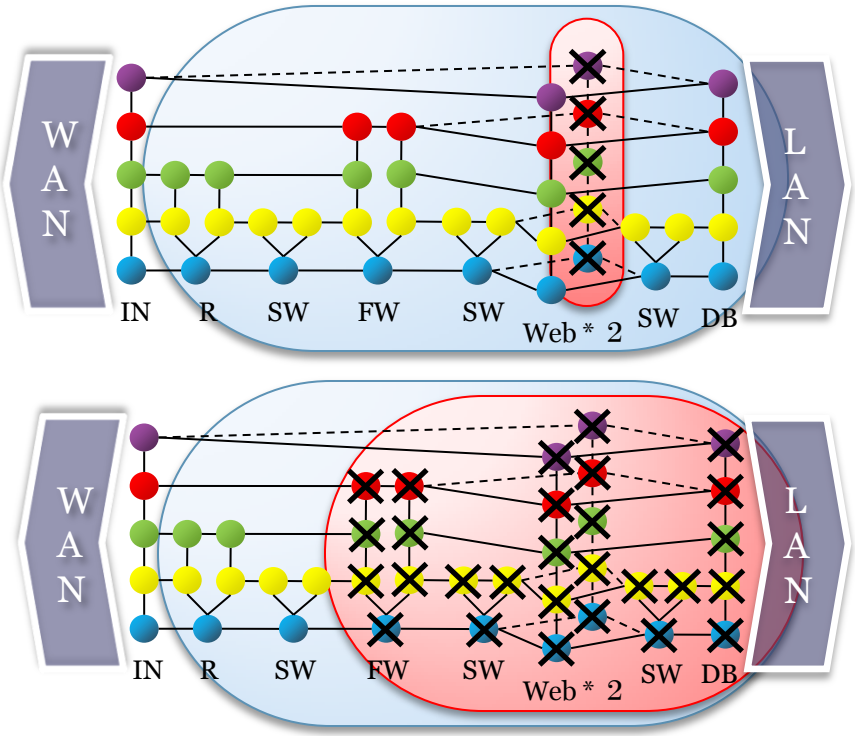
下流（LAN側）の
全モジュールに影響

CVSS環境値算出例

仮定

N＝(全体ノード数)－(INモジュールノード数)＝36
N_A＝(可用性影響ノード数)
脆弱性のCVSS基本値＝5.0

- 被害小のケース
  - N_A＝5
  - 影響度(I)＝N_A/N＝5/36＝0.14
  - TD＝小規模＝0.25
  - CVSS環境値＝5.0 × 0.25＝1.25
- 被害大のケース
  - N_A＝28
  - 影響度(I)＝N_A/N＝28/36＝0.78
  - TD＝大規模＝1.00
  - CVSS環境値＝5.0 × 1.00＝5.00



まとめ

既存のCVSSを用いたリスク分析

- CVSS基本値を利用した独自の環境評価手法
- NSQモデルを用いた定量的なCVSS環境評価パラメータ設定（加藤ら）
  - 影響タイプ（C・I・A）の差異の未考慮
  - CDP（二次被害）定義のギャップ

手法提案（加藤らの手法を検討）

- 影響タイプ毎に影響範囲を切り分け
  - A（可用性への影響）に着目
- 脆弱性を持つノードの位置による影響範囲の差異を明示
  - 再現性の確保

今後

- 他の影響タイプ（C・I）についての検討
- 様々な構成のNSに対するシミュレーション