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

○加藤雅彦（株式会社アイアイジェイテクノロジー）
金岡晃（筑波大）
藤堂伸勝（筑波大）
岡本栄司（筑波大）

IIJ Technology

Agenda

- ◆本研究の目的と本論文の位置づけ
- ◆背景
- ◆既存研究とこれまでの成果
- ◆脆弱性影響度の定量化
- ◆脆弱性影響範囲の可視化
- ◆CVSSへの適用
- ◆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機能の異なる複数の機器を結合し、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で提案したネットワークシステム表現モデルと脆弱性情報を利用したネットワークシステムの脆弱性影響度判定

背景

背景～ネットワークシステム

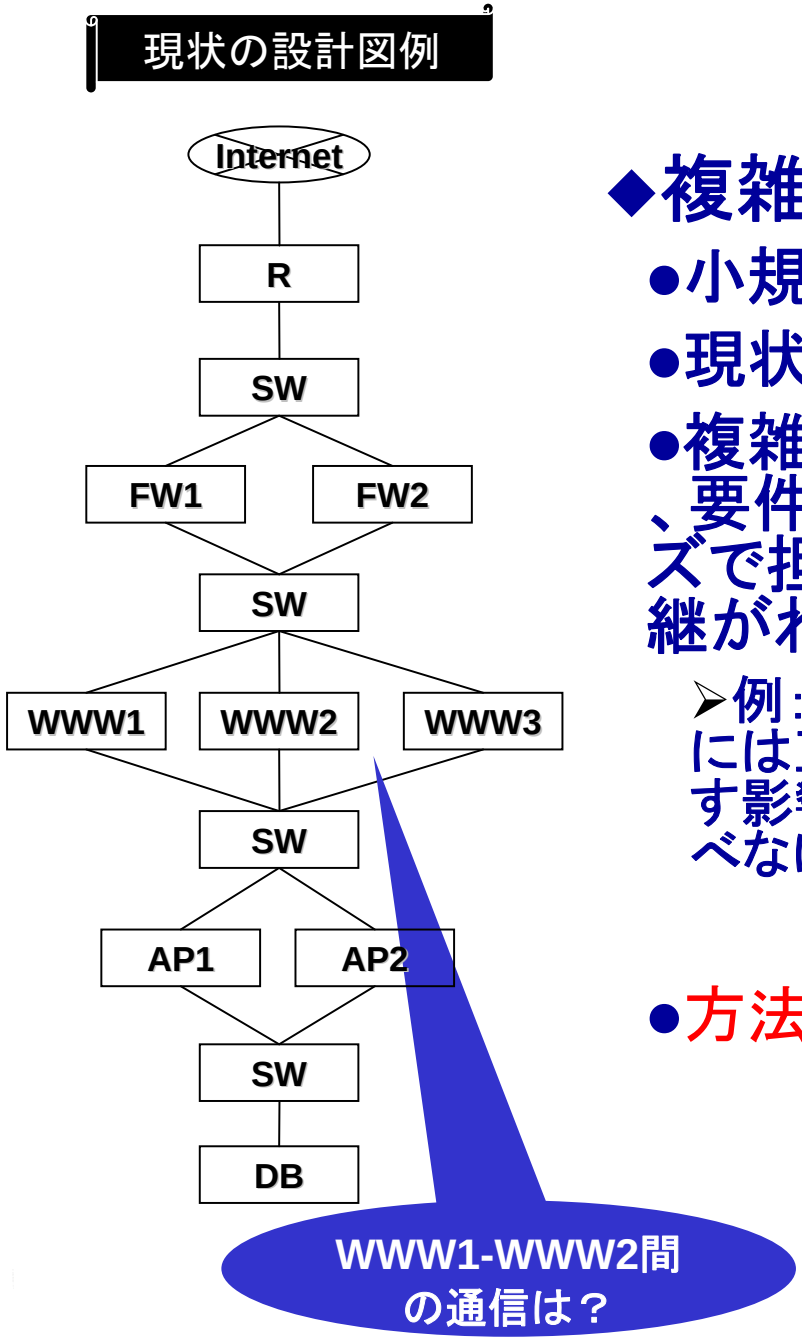
◆インターネットでサービス提供を行うシステムは一般的に単一機能の機器をネットワーク化し構成されている（巨大なコンピュータ1台、ではない）

◆サービス提供システムをネットワーク化するモチベーションとは・・・

- ●コスト（安くしたい）
- ●拡張性（将来の需要増に備えたい）
- ●処理の最適化（無駄なく資源を使いたい）
- ●アクセス制御（最小権限）
- ●耐障害性の向上（落ちないように）
- ●脆弱性対応の局所化（問題を最小限に）

・・・等々様々な要件が存在

背景～ネットワークシステム



◆複雑な要件による最適化の困難性

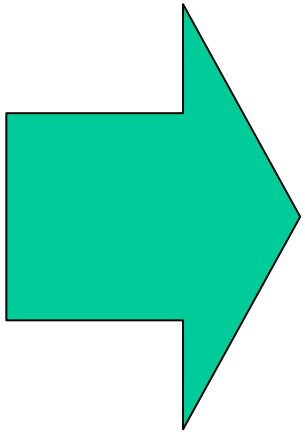
- ●小規模システムでさえ設計が複雑に
- ●現状は設計者のスキルや経験に依存
- ●複雑化、巨大化することにより関わる人が増え、要件定義、設計、開発、構築、運用の各フェーズで担当者が変わる。そこで完全に情報が引き継がれない
  - ➢例：アクセス制御は適切にされるべきだがドキュメントには正確に反映されておらず、脆弱性がシステムに及ぼす影響範囲を正確に知るためには実際の運用環境を調べなければいけない、等
- ●方法論や理論的アプローチが未開拓

背景～脆弱性情報

◆一方、システムは日々脅威にさらされている

◆脆弱性情報配信の現状

- ●毎日続々と公表される脆弱性情報
- ●広報手段としてWebやメールを利用
- ●内容は可読形式、つまり、人が読むことが前提
- ●一般的な情報であり、個別のネットワークシステムにどの程度影響するかは個々で判断せざるを得ない



ネットワークシステムの脆弱性対応には
人の介在が不可欠。
だがその複雑さゆえ、負担は大きい

背景

脆弱性の影響に関する
評価作業をできるだけ
自動化したい

既存研究と
これまでの成果

NSQモデル

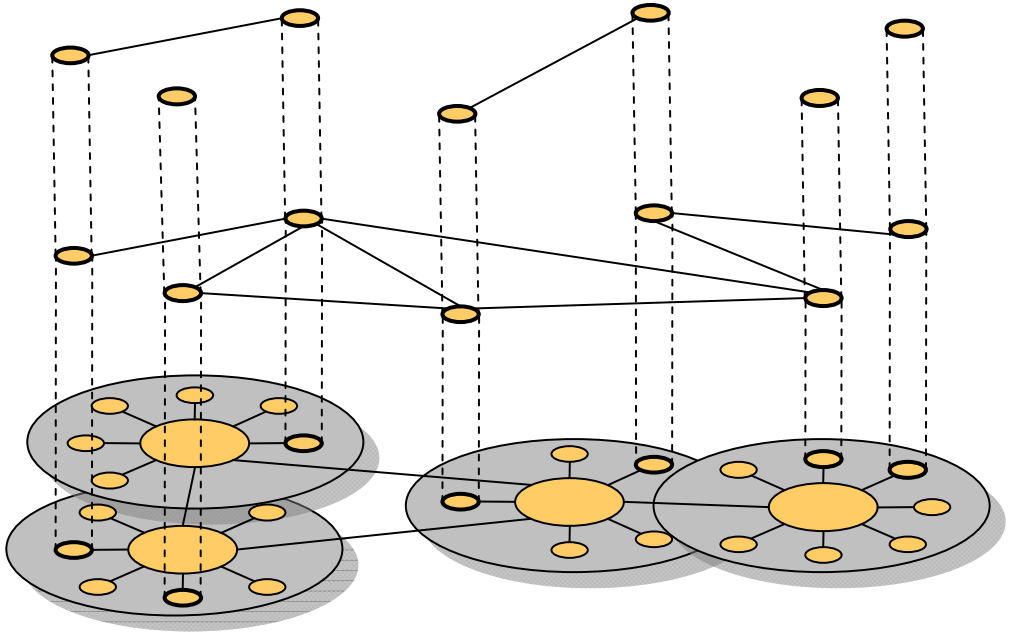
基本戦略

現状

物理的接続のみを反映した
ネットワーク表現

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

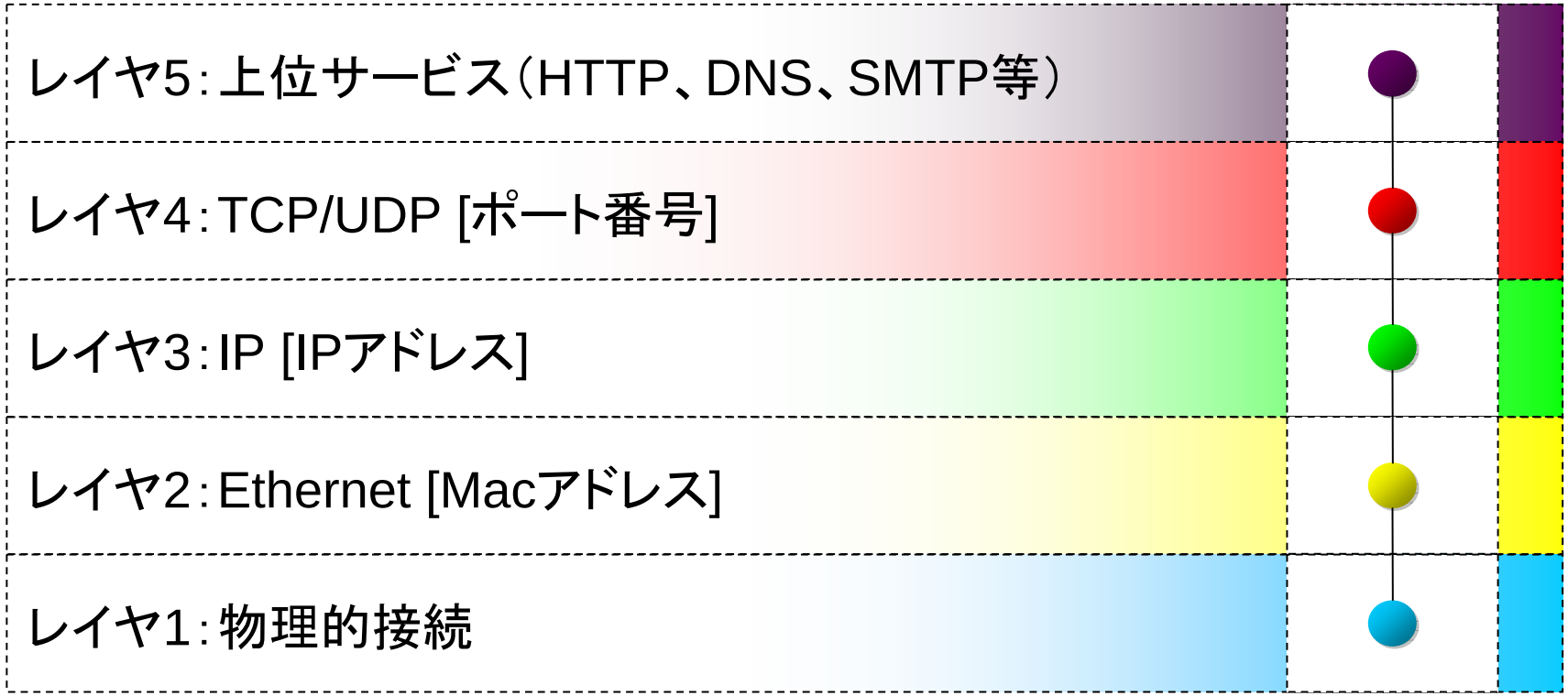


イメージ図

用語定義

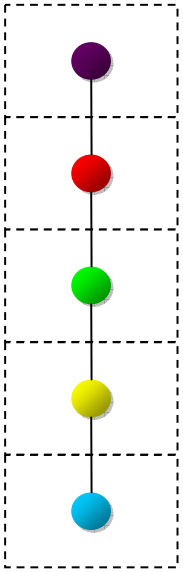
通信		情報の送受信
通信路		送信者（情報源）から受信者への情報伝達媒体であり、1つ以上のリンクにより構成される。
ノード		通信が行われる際の、送信者・受信者・中継者
レイヤ		同種情報が同種通信路で通信を行う際のノードとリンクの集まり
リンク		2つのノード間をつなぐもの
	レイヤ内リンク	同一レイヤにある2つのノードをつなぐリンク
	レイヤ間リンク	異なるレイヤにある2つのノードをつなぐリンク
モジュール		1つ以上のレイヤにまたがって機能を提供するもの
中継		当該レイヤの通信路を形成するにあたり、1つ下位のレイヤの通信路形成を決定する処理を行うこと

レイヤ定義とノード



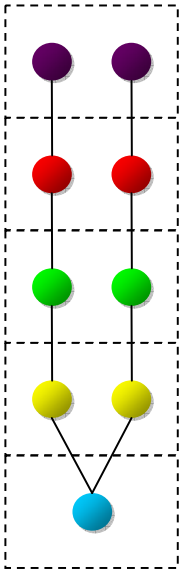
モジュール例

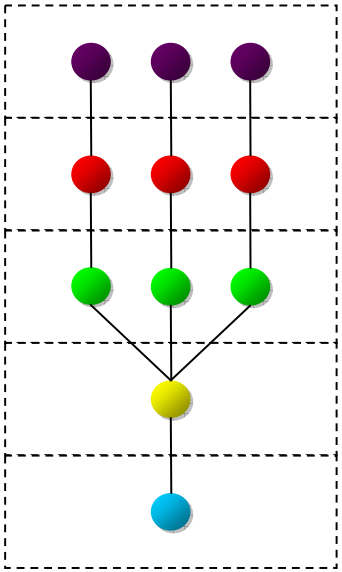
サーバ



単一のサービス
を提供するサーバ
（Webサーバなど）

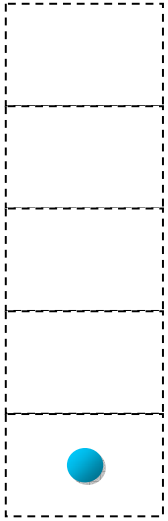
複数のサービスを
提供するサーバ
（Webサーバ
＋DBなど）



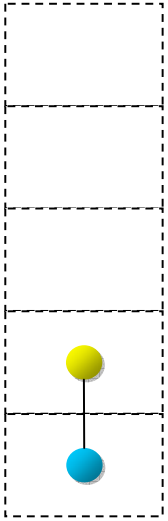


中継機器（機能）

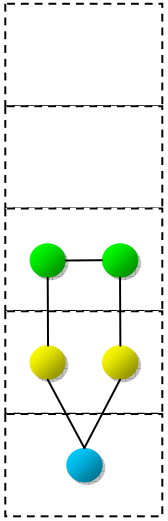
ハブ



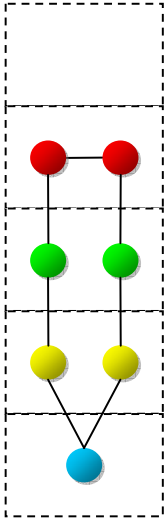
スイッチ



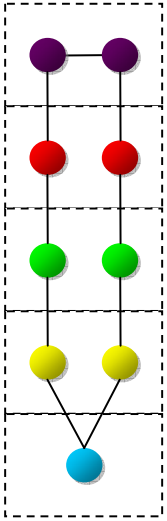
ルータ



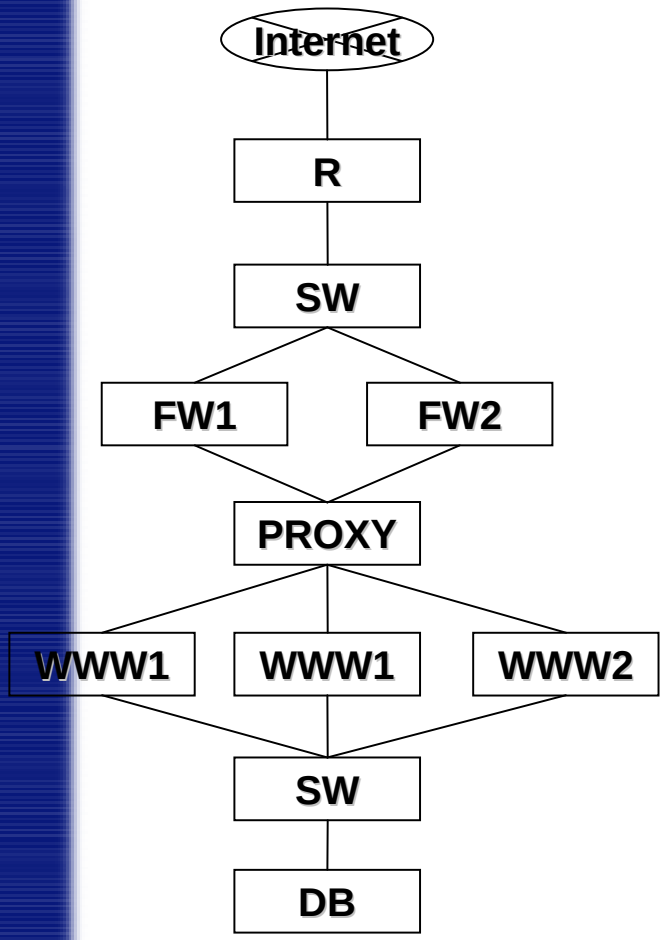
NAPT



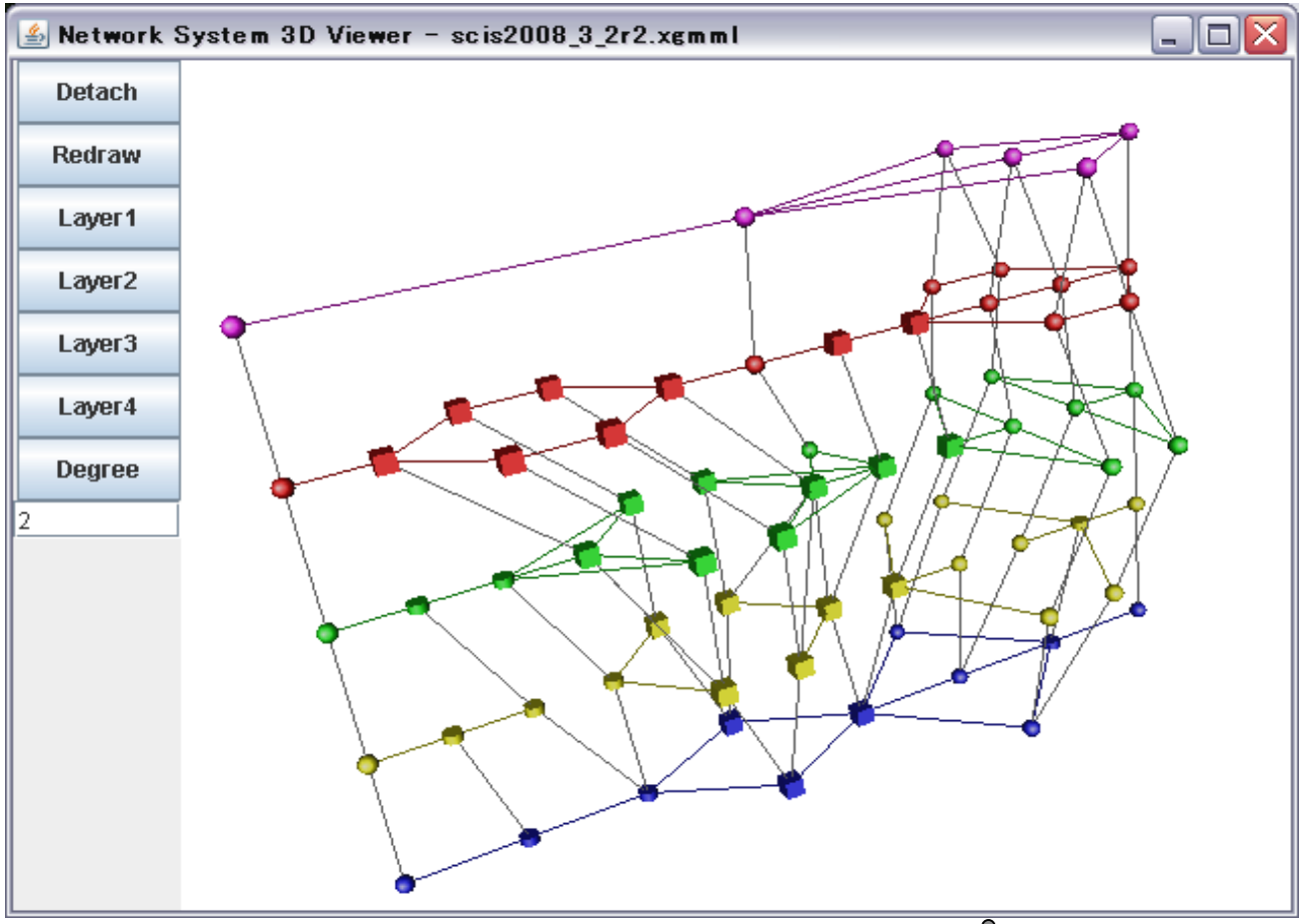
プロキシ



NSQモデルによるネットワーク表現例



従来の表現例



提案モデルによる表現例

既存研究（脆弱性情報関連）

◆脆弱性情報ソース

- ●NVD（NIST）
  - ➢National Vulnerability Database
  - ➢脆弱性情報データベース。XMLでの情報提供
- ●JVN（IPA）
  - ➢Japan Vulnerability Notes
  - ➢日本の脆弱性情報データベース。RSSに対応

◆脆弱性評価

- ●CVSS（FIRST）
  - ➢Common Vulnerability Scoring System
  - ➢脆弱性の評価手法
- ●KENGINE（JPCERT）
  - ➢脆弱性情報ハンドリングのためのエキスパートシステム

```
−<xs:schema elementFormDefault="qualified" attributeFormDefault="unqualified"
 targetNamespace="http://nvd.nist.gov/feeds/cve/1.2">
  −<xs:annotation>
    −<xs:documentation>
        This schema defines the structure of the National Vulnerability Database XML feed files version:
        1.2. The elements and attribute in this document are described by xs:annotation tags. This file is
        kept at http://nvd.nist.gov/schema/nvdcve.xsd. The NVD XML feeds are available at
        http://nvd.nist.gov/download.cfm. Release Notes: Version 1.2: * CVSS version 2 scores and
        vectors have been added. Please see http://nvd.nist.gov/cvss.cfm?vectorinfo and
        http://www.first.org/cvss/cvss-guide.html for more information on how to interpret this data.
      </xs:documentation>
    </xs:annotation>
  −<xs:element name="nvd">
    −<xs:annotation>
      −<xs:documentation>
          The root element of the NVD CVE feed. Multiple "entry" child elements describe specific NVD
          CVE entries.
        </xs:documentation>
      </xs:annotation>
    −<xs:complexType>
```

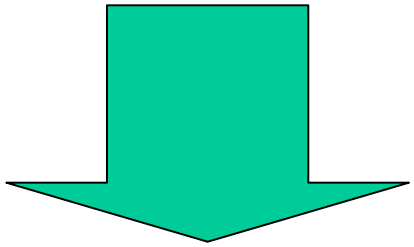
NVD Schema

脆弱性影響度の定量化

脆弱性影響度の定量化

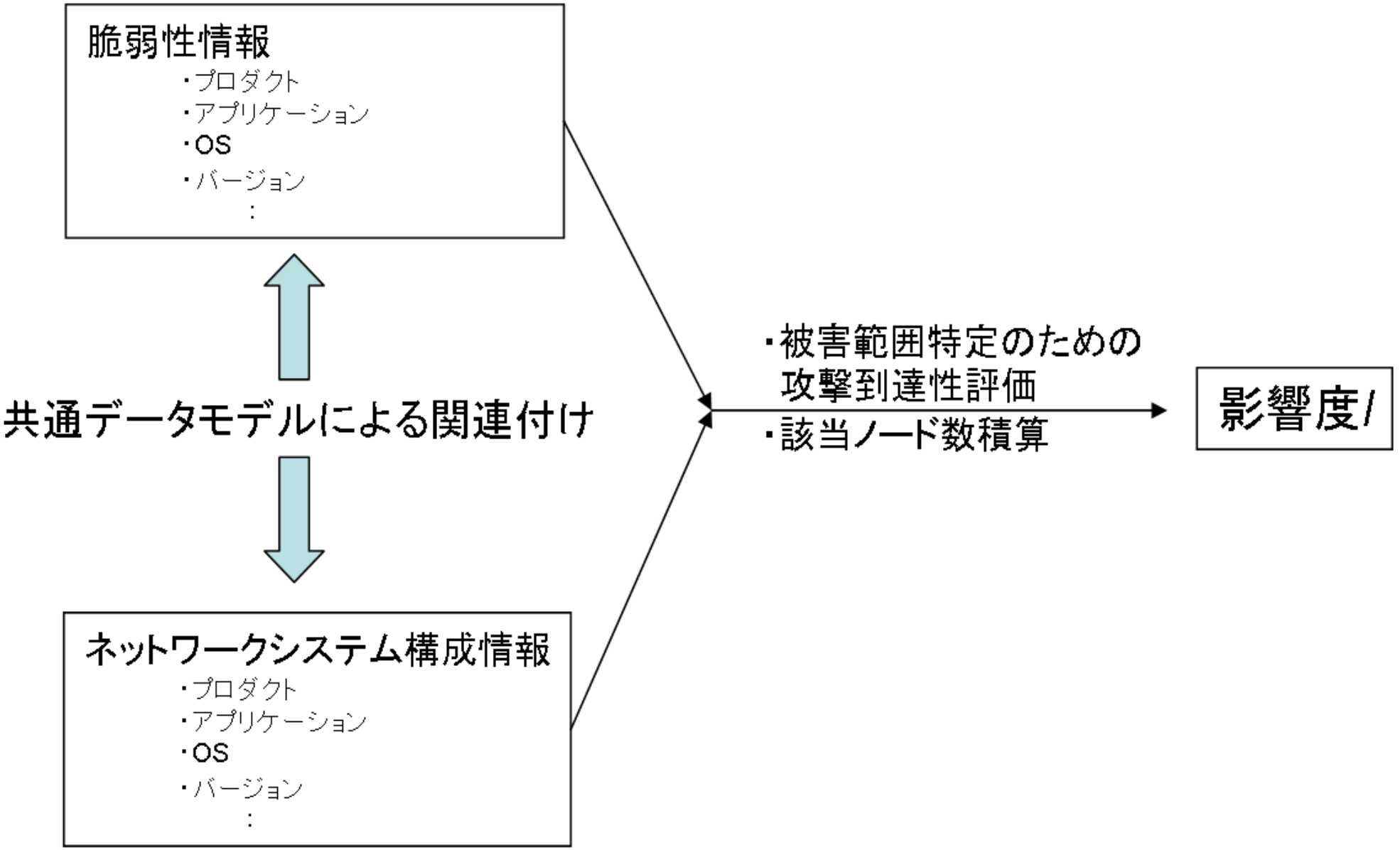
◆攻撃ベクトル表現は標準化されているが個別のネットワークシステムの構成情報は反映できない

◆一般的にネットワークシステム構成情報は脆弱性情報と比較できるデータ構造となっていない



脆弱性情報のデータモデルと
ネットワークシステムのデータモデルを
一致させる必要性

脆弱性影響度の定量化

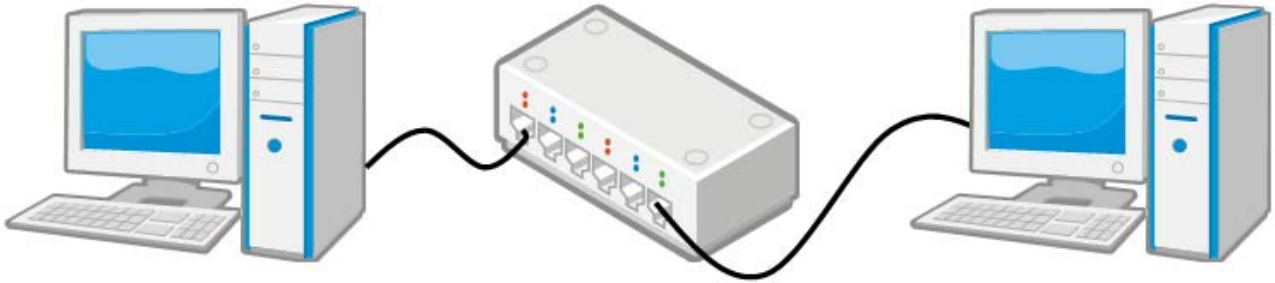


脆弱性影響度の定量化

◆表のようにNSQモデルと脆弱性情報を対応

Layer	NSQ	脆弱性情報
5	上位サービス	Application Data Flow
4	TCP / UDP	Application name / Version
3	IP Address	OS name / Version
2	Mac Address / VLAN ID	―
1	物理接続	Product name / Vendor name

脆弱性影響度の定量化

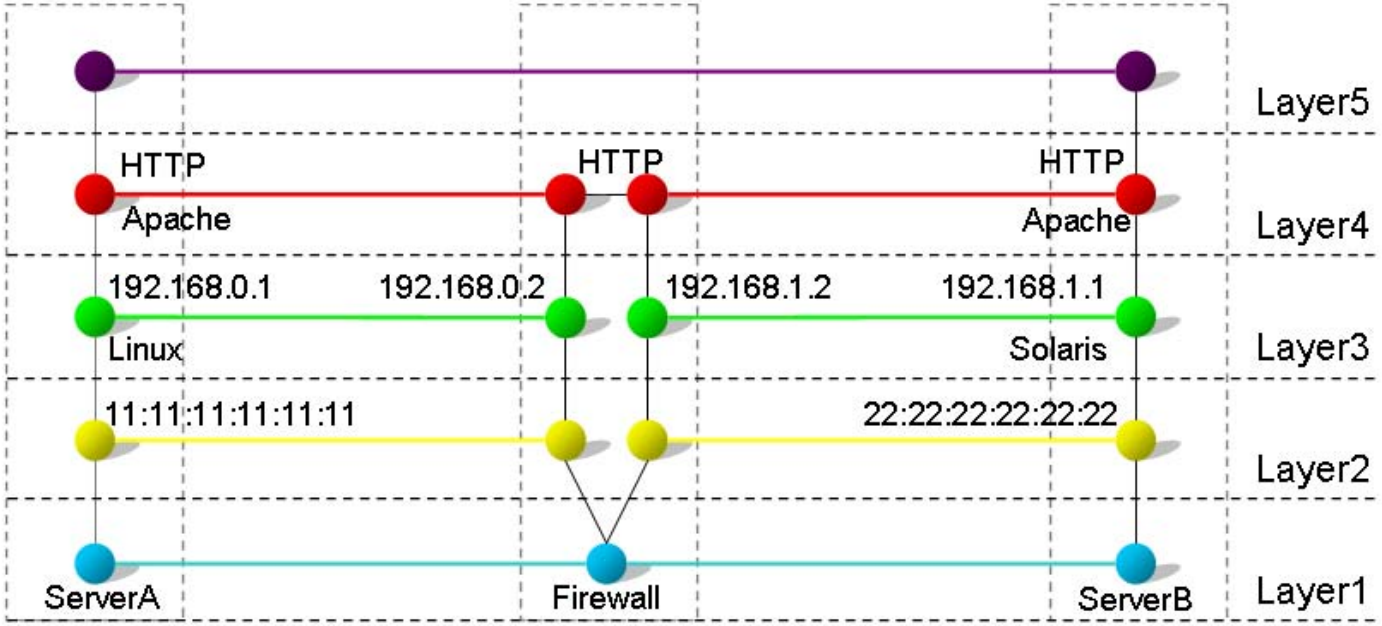


ServerA — Firewall — ServerB

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

IP:192.68.0.2　IP:192.168.1.2

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



脆弱性影響度の定量化

◆定量化のコンセプト

- ●システムの全ノード数(Ds)に対しての被攻撃ノード数の割合を指標として定量化

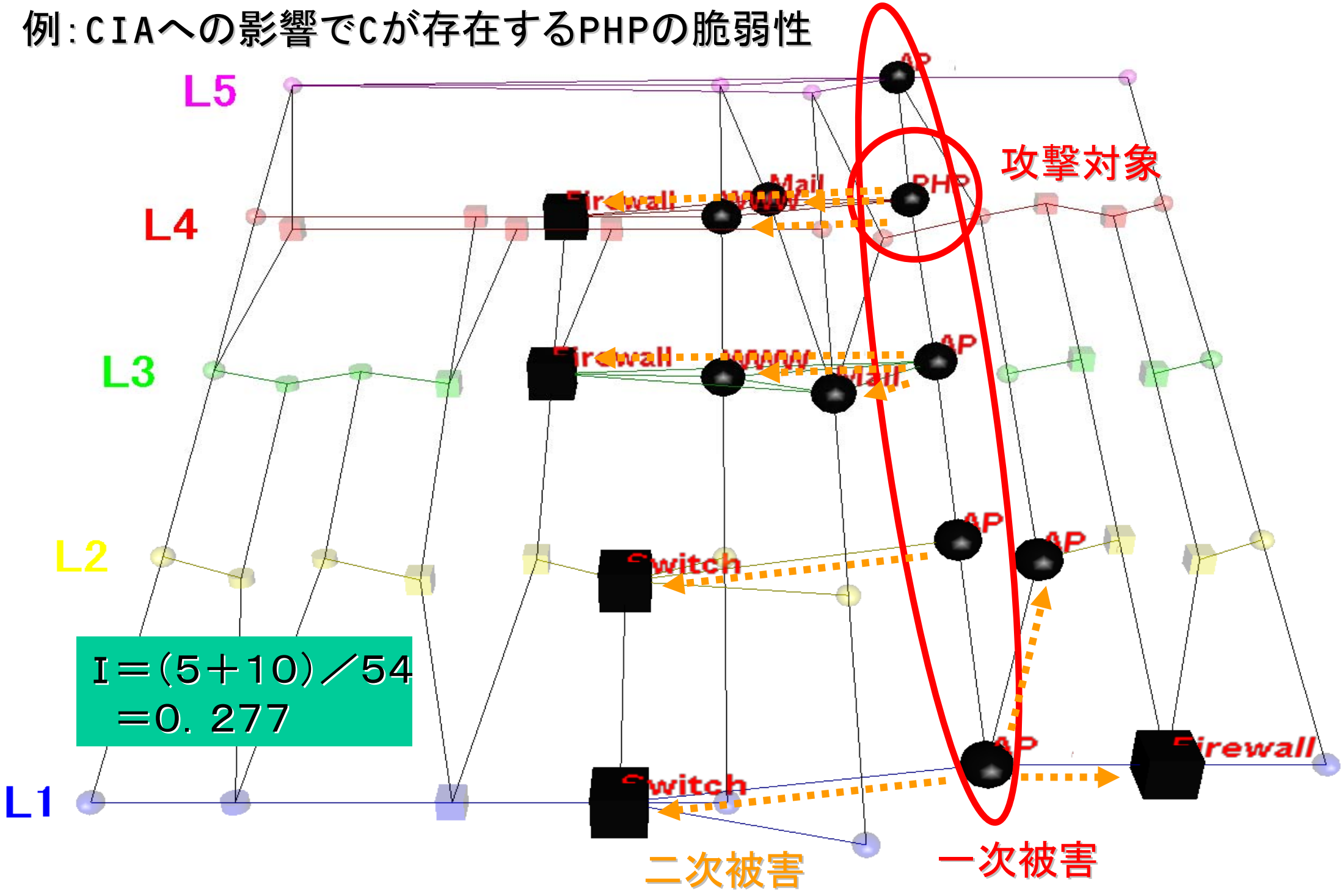
◆被攻撃ノード数の定義

- ●一次被害ノード(Dn)と二次被害ノード(Dm)に分類
  - ➢一次被害ノード
    - •攻撃元からのアクセスパスが存在し、直接攻撃される可能性があるノード(群)。攻撃ベクトルCIAにC(complete)が存在する場合はモジュール全体が一次被害対象とする。
  - ➢二次被害ノード
    - •一次被害ノードに隣接するノード

◆影響度

$$I = \frac{Dn+Dm}{Ds}$$

例：CIAへの影響でCが存在するPHPの脆弱性



I＝(5＋10)／54
＝0．277

脆弱性影響範囲の可視化

デモをご覧ください

CVSSへの適用

CVSS

◆CVSSのパラメータ

- ●Base Metrics
  - ➢脆弱性そのものの特性を評価
- ●Temporal Metrics
  - ➢脆弱性の現在の深刻度を評価
- ●Environmental Metrics
  - ➢製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価

◆Environmental Metrics

- ●Target Distribution
  - ➢利用環境の中で、脆弱性を攻撃される可能性のある対象システムを利用している範囲を評価
- ●Collateral Damage Potential
  - ➢対象システムが脆弱性を攻撃された場合の物理的な機器への被害や、生活基盤、身体などへ及ぼす二次的な被害の可能性を評価

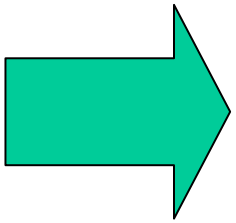
CVSSへの適用

◆CVSSのTD（Target Destribution）

- 一次被害と同様とする

◆CVSSのCDP（Collateral Damage Potential）

- 二次被害と同様とする



Environmental Score
への適用

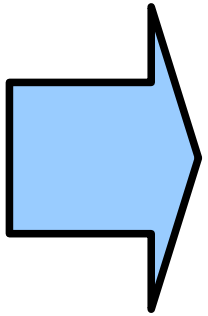
まとめ

まとめ

◆NSQモデルを利用した脆弱性情報のデータモデル化を行った

◆データモデルを利用した脆弱性影響度の算出と影響範囲の可視化を行った

◆CVSSのEnvironmental Scoreへの応用を試みた



ネットワークシステムのアクセス制御構造と構成情報をデータモデル化することにより、脆弱性評価を人手を介することなく自動処理することが可能であることが確認できた

今後の予定

- ◆実稼動中のシステムへの適用
- ◆可用性の影響範囲についての検討
- ◆システム設計ツールとしての評価

ご清聴ありがとうございました