# 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† 金岡 晃‡ 藤堂 伸勝‡ 岡本 栄司‡

†株式会社アイアイジェイテクノロジー
101-0051 東京都千代田区神田神保町 1-105 神保町三井ビルディング

masa@iij-tech.co.jp
‡筑波大学大学院システム情報工学研究科
305-8573 茨城県つくば市天王台 1-1-1

{kanaoka,okamoto}@risk.tsukuba.ac.jp toudou@cipher.risk.tsukuba.ac.jp

**あらまし** ネットワークシステムのアクセス制御構造と脆弱性の構成要素情報をモデル化し, システムに内在する脆弱性が攻撃された場合の被害規模の算出, 二次被害も含めた影響範囲の特定, さらにそれらの数値化を行った. 加えて RSS で自動配信される脆弱性情報を取り込み, システムへの影響を可視化するツールを作成した. その結果, 被攻撃対象となるシステムの攻撃に対する耐性を定量的に評価可能とした. また, 応用として CVSS との連携について検討を行った.

# Visualization and Measurement of Vulnerability Impact on Networked System

Masahiko KATO† Akira KANAOKA‡ Nobukatsu TOUDOU‡
Eiji OKAMOTO‡

†IIJ Technology Inc.
1-105 Kanda Jinbo-cho, Chiyodaku, Tokyo 101-0051, Japan

masa@iij-tech.co.jp
‡University of Tsukuba
1-1-1, Tennodai, Tsukuba, 305-8573, Ibaraki, Japan

{kanaoka,okamoto}@risk.tsukuba.ac.jp toudou@cipher.risk.tsukuba.ac.jp

**Abstract** We model an access control structure of networked system and vulnerable component information, and calculate a damage scale including 2nd damage when the weakness inside the system was attacked. Additionally, we make a visualize tool for system damage that automatically took RSS Feed of vulnerability information. Finally, an application to calculate CVSS environmental score was examined. As a result, it is shown that an quantitative evaluation of a tolerance to attack of the networked system is possible.

## 1 はじめに

インターネット上で不特定多数のユーザーにサービス提供を行うためのシステムは性能, コスト, 運用管理といった要求事項をバランスよく満たすことが求められる. その要求を実現するために単一の機器でシステムを構成することは稀であり, 安価なサーバやネットワーク機器を

複数台用いてネットワーク化したシステム (以下ネットワークシステム) が利用され, それぞれの機器を複雑に連携させることにより安全安心なサービス提供を行うのが一般的となっている.

近年インターネット利用者の爆発的な増加やセキュリティに対する要求の高度化により, ネットワークシステムの規模や複雑さは以前と比較にならない程に肥大化する一方, 現場では旧来行われているような技術者の経験を主とするセキュリティ設計, セキュリティ運用手法が利用されていることが多い. そのため設計時に考慮されていないセキュリティ上の問題が運用時に発覚したり, 脆弱性の影響判断を手作業で確認するといったことが頻繁に起こっているのが実情である. そのような状況において, 米国では影響判断の効率化, 自動化のために ISAP/SCAP [1] による脆弱性情報の標準化, 定量化が進んでおり, 一般に公開されている脆弱性情報はアプリケーション, バージョン, OS 種別といった構成要素情報が XML Schema で定義, 情報配信されている.

しかし, ネットワークシステムにおいて脆弱性の影響範囲を特定し対策の判断を行うためには脆弱性情報だけではなく, システム内にアプリケーションやプロダクトの構成要素がどう存在するか, それらがどうアクセス制御されネットワーク化されているか, 攻撃が対象に到達可能かどうか, といった情報が必要となる. 脆弱性情報がデータモデル化されているにもかかわらず, システム構成要素やネットワーク構造情報は, 構成要素をテキストや表形式にしてファイルやデータベースで管理し, ネットワーク構造は描画ツール等を使用して表記するという旧来のデータ記述手法が現場では未だ主流であり, 脆弱性情報の自動判断に生かせるネットワークシステムのデータモデルが存在しない. さらに, 攻撃による影響範囲の調査や重要度判断をシステムの運用管理者が人的に行うことにより, 判断が曖昧で定性的となり再現性のある評価や運用管理の自動化が困難なものとなっている.

以上の課題を解決するため本稿では, 2 章で既存研究の調査を行い, 3 章でアクセス制御情報と脆弱性にかかわるシステムの構成情報のデータモデル化と影響度の数値化, 4 章で影響範囲の可視化を行う. さらに 5 章で数値化の応用例を示す. 最後に 6 章で提案手法の有効性と課題について考察を行う.

# 2 既存研究

## 2.1 ネットワークシステムモデル

一般的にネットワークシステムは複数の機能を持つ機器群から構成されるが, これまでの研究によるコンピュータネットワークの解析はルータや Autonomous System (AS) などの同一機能を持つもの同士のつながりに関するネットワークの解析 [2] であり, 複数機能を有するネットワークシステムの解析ではない. ネットワークシステムの脆弱性判断を行うためには, アクセス制御情報, システム構成情報, 脆弱性情報といった複数の情報をまとめて扱う必要があり, 同一機能を前提としたネットワークモデルを直接適用することは困難である. そこで, 金岡らは複数機能を有するネットワークシステムの新たな表現モデル (以下 NSQ モデル) [3] [4] の提案を行った. NSQ モデルはネットワークシステムを通信層毎に分解し, それぞれの通信層に存在するネットワーク機能として認識可能な ID をノードとして表現する. また, 複数の通信層にまたがってノードを接続したものをモジュールと定義 ( 図 1 ) し, 一般的な機器はモジュールで表現する. さらにノードが同一レイヤー内でどのノードからアクセスされるか, 上位層のノードがどの下位層のノードに依存して存在しているかをノード間の接続として表すことで, ネットワークシステム内の識別可能なノードのアクセス制御と依存性が表現可能 ( 図 2 ) となっている. 本稿では NSQ モデルの定義を拡張し, ノード属性として構成情報を含んだ形でデータモデルを検討した.

## 2.2 脆弱性情報

脆弱性情報の提供は国内外含め複数の機関により行われているが, それぞれに提供方法やデー

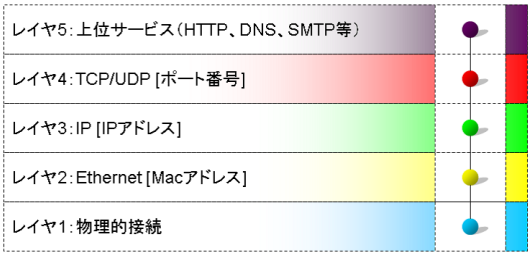


図 1: モジュール図

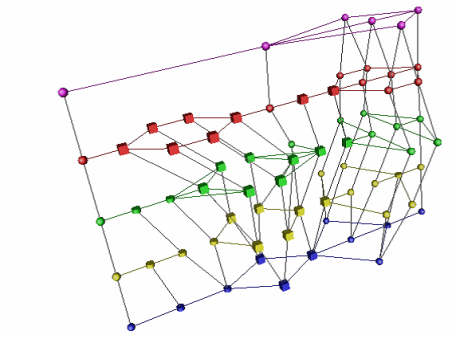

図 2: ネットワークシステムモデル例

タの内容が異なっている．今回, National Vulnerability Database (NVD) [5] , JVN iPedia [6] の 2 つの脆弱性情報提供サービスにより提供されるデータ利用について比較検討を行った．

- `NVD`
  脆弱性情報の XML Schema がある．脆弱性情報は XML ファイルで配布されるものの, インターフェースが通常の Web でありシステムが自動的にデータを利用するというよりは人による利用が主である．国産機器に関する脆弱性情報は少ない．

- `JVN iPedia`
  国産機器の脆弱性情報量が豊富である．RSS による脆弱性情報配信と, 自然言語形式で Web のインターフェースを利用しての情報入手がある．

検討の結果, 脆弱性情報が XML でファイルとして入手でき加工がしやすいため, NVD による脆弱性情報を利用することとした．

### 2.3 脆弱性定量化

脆弱性による影響を数値化する代表的な手法として Common Vulnerability Scoreing System (CVSS) [7] があげられる．CVSS は基本評価基準, 現状評価基準, 環境評価基準の 3 つの値で構成されている．基本評価基準は脆弱性そのものの特性として攻撃経路情報, 認証の必要性, 攻撃の複雑さ, 機密性, 可用性, 完全性に対する影響を評価している．現状評価基準は脆弱性の対応状況による深刻度を, 環境評価基準は実際に攻撃を受けるシステムへの影響度を表している．これらの基準のうち基本評価基準は評価機関により定められるが, 環境評価基準はユーザの環境に応じてユーザが判断するため, 結果として値が定量的に定まらない一因となっている．CVSS の活用については, 小林らの論文 [8] でも検討されているが , 攻撃そのものの深刻度評価となっており, ネットワークシステムが実際にどれだけの影響を受けるかについては評価がなされていない．また, 別のアプローチとして JNSA の脆弱性定量化に向けての検討ワーキンググループによる, トリアージ値を使用した定量化手法 [9] も提案されている．脆弱性を手法, 原因, 対策といった複数の構成要素として分解し, 各要素の関連性と状態を定義し, それぞれに重み付けを行うことにより指標化, 数値化対策の可否判断が可能となっている．しかし, こちらも対策の判断に重点を置いた指標となっており, ネットワークシステムへの具体的な影響範囲特定等への適用は困難である．

## 3 脆弱性影響度の定量化

脆弱性の影響を評価するためには攻撃そのものの情報と攻撃を受けるネットワークシステムの情報が必要であり, ネットワークシステムの構成要素と脆弱性情報の構成要素が比較可能なデータモデルとなっていること ( 図 3 ) が望ましい．そこで, 本研究ではシステム構成情報モデルと脆弱性情報モデルを比較可能とすべく NSQ モデルを拡張し, 攻撃の到達性を考慮したうえでの攻撃対象ノード数を積算し全体ノード

数の何割にあたるかを計算することで定量化を行うこととした.

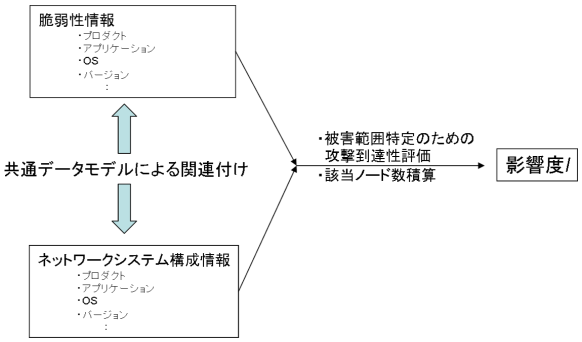


図 3: 脆弱性影響度定量化の概念

### 3.1 脆弱性情報とモデルの関連付け

NSQ モデル上で脆弱性情報を扱うため, 以下のようにシステム構成情報の各要素を通信層に分類して NSQ モデルのノードに対してモデル拡張を行った. (表 1)

表 1: 属性のマッピング

| Layer | attribute |
|---|---|
| 5 | Application Data flow |
| 4 | Application name / Version |
| 3 | OS name / Version |
| 2 | - |
| 1 | Product name / Vendor |

さらに, NVD が提供している脆弱性情報の XML Schema と拡張した NSQ モデルの構成情報を対応付けるために, NVD の脆弱性情報からアプリケーション情報を抽出した. 具体的には vuln_soft の prod,vers エレメント ( 図 4 ) を使用した. 図 5 では, ファイアウォールをはさんで 2 台のサーバが通信を行う場合のモデルへのマッピング例を示している.

### 3.2 攻撃到達性の評価

ファイアウォール等によりアクセス制御が行われている場合, 脆弱性が存在したとしても攻

```
−<vuln_soft>
 −<prod name="Outlook Express" vendor="Microsoft">
    <vers edition="sp2" num="5.5" />
    <vers edition="sp1" num="6.0" />
  </prod>
 −<prod name="Windows Mail" vendor="Microsoft">
    <vers num="" />
  </prod>
</vuln_soft>
```

図 4: NVD の XML 例

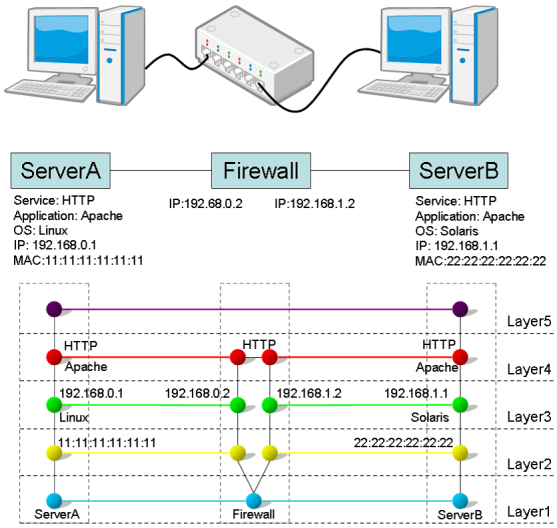


図 5: マッピング例

撃が該当機器まで到達せず, 脆弱性の影響を受けない可能性がある. そのため, 単純に脆弱性のあるアプリケーションがネットワークシステム内部に存在するというだけでは影響を判断できず, 通信の到達性を評価する必要がある. パス探索等により通信経路を調べる手法では経路探索の計算コストが高く規模の大きなシステムでは適用が難しいが, NSQ モデルでは各通信層でアクセス可能なノードが接続されるため, 到達性に関しては攻撃の起点と攻撃対象が接続されているかどうかで判断が可能である. よって, そのモデル特性をそのまま到達性の確認要件とした. なお, 本稿では攻撃の起点をインターネットとしたが, ネットワークシステム内部を攻撃の起点とすることも可能である.

### 3.3 被害範囲と影響度の定義

ネットワークシステムが何らかの攻撃を受けた場合, 攻撃の対象となったノードが直接的な

被害を受ける以外に, ネットワークシステム内部の近隣ノードに二次被害が発生する可能性がある. 機密性, 完全性に関する攻撃の二次被害と可用性に関する攻撃の二次被害とでは被害範囲が異なることが考えられるが, 本稿では以下のように被害対象範囲を定義することとした. 可用性の考慮に関しては考察で述べる.

- 一次被害対象
  脆弱性情報の基本評価基準で全面的な脅威が一つ以上含まれる場合, 攻撃を受けるノードを含む機器全体が一次被害を受けるとする. つまり, 攻撃対象ノードが含まれるモジュール全体が被害対象となる. 基本評価基準に全面的な脅威が存在しない場合は, 攻撃対象となったノードのみを一次被害の対象とする.

- 二次被害対象
  二次被害対象は一次被害で対象となったノードに隣接しているノードすべてとする. 不正侵入等によりノードの制御が攻撃者によって奪われた場合, 二次被害がどのような攻撃方法で発生するか不明である. よって, 一次被害を起こした攻撃の種類とは関係なく隣接ノードすべてに危険性があると想定した. 二次被害対象は以下の方法で算定を行う.

一次被害対象ノード数を Dn, 二次被害対象ノード数を Dm, インターネットを除くすべてのノード数を Ds, 被害対象となるノード数の全体ノード数に占める割合を影響度 (I) とし, 以下のとおり定義した. 1 に近いほど攻撃による影響が大きい.

$$\text{影響度}\ (I) \quad = \quad \frac{Dn + Dm}{Ds} \qquad (1)$$

例として 図 6 のネットワークシステムで AP 上にある PHP の脆弱性に対する攻撃が発生した場合を想定し, 影響度計算を行ったところ以下のような結果となった.

$$\frac{1 + 14}{48} \quad = \quad 0.3125 \qquad (2)$$

これにより, 実際に攻撃対象は 1 ノードであるにもかかわらず, 二次被害はシステムの 30%以上に及ぶ可能性が数値から判断でき, 対策指標として利用可能であることを伺わせる結果となっている.

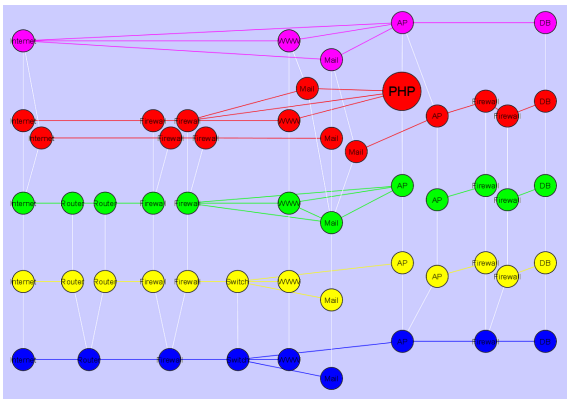


図 6: モデル例

## 4 脆弱性影響範囲の可視化

さらに拡張した NSQ モデルを使い, 影響範囲が見てわかるよう可視化ツールを作成した. 実際の運用環境では新たな脆弱性が公開された場合にシステムへの影響を確認するという作業が行われるため, ツールの動作もそれに習ったものとした. 具体的には, NVD の RSS Feed を取得し, 着目する脆弱性情報を選択することで, 攻撃対象ノードを自動検索する. その結果として, 一次被害対象, 二次被害対象を強調表示することで被害をわかりやすくするというものである.

図 7 は図 6 のモデルで PHP が攻撃された場合の影響範囲について可視化を行ったものである. 大きく表示されているノードが二次被害も含めての影響範囲であり, これにより影響の大きさが視覚的に理解できることがわかる.

## 5 CVSS への適用

最後に, 影響度を CVSS の環境評価基準に適用可能かどうか検証を行った. CVSS の定義と照らし合わせ, 一次被害対象を Target Distribution (TD) , 二次被害対象を Collateral Damage Potential (CDP) として関連付けを行った. CDP は 4 段階に分類されているが数値の基準

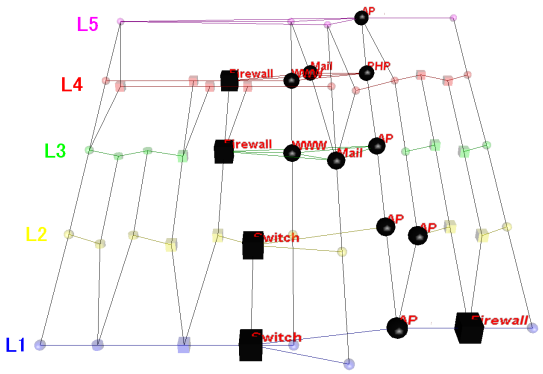


図 7: 影響範囲の可視化

が明示されていないため, 今回は表 2 のように値を対応させることとした.

表 2: 環境評価基準とのマッピング

| 影響度 (I) | TD | CDP |
|---|---|---|
| $I = 0$ | なし | なし |
| $0 < I < 0.25$ | 小規模 | 軽微 |
| $0.25 \leq I < 0.5$ | 中規模 | 中程度 |
| $0.5 \leq I < 0.75$ | 中規模 | 重大 |
| $I > 0.75$ | 大規模 | 壊滅的 |

以上の定義を使用し, 図 6 において CVSS の計算を行ったところ, 環境評価基準は以下の結果となり, NSQ モデルの拡張による影響度計算が CVSS の環境評価基準算出の一手段として活用可能であることがわかった.

TD=2.08 (%)
CDP=31.25 (%)
環境評価基準値= 2.1

## 6 考察

本研究では, NSQ モデルの定義を拡張することでアクセス制御されたネットワークシステムに対しての攻撃による影響範囲の特定と影響度の定量化が可能であることがわかった. また, 可視化を行うことによりシステムへの影響が見てわかりやすく表現できることが確認できた. さらに CVSS での環境評価基準値の計算に応用可能であることも示した。一方, 攻撃を受けた場合の影響範囲に関する定義は検討の余地を残しており, 特に可用性を考慮した場合の影響範囲は検討が必須であると考えられる. 今後は実際に稼動している環境からモデルを抽出しての評価, 定量指標を用いた対策判断の自動化, 可用性を考慮した場合の影響範囲の特定等に関して検討を行う.

## 参考文献

[1] ISAP/SCAP
http://nvd.nist.gov/scap.cfm

[2] L.Li, D.Alderson, W.Willinger, J.Doyle, "A First-Principles Approach to Understanding the Internet's Router-level Topology", SIGCOMM'04, 2004

[3] 金岡晃, 藤堂伸勝, 加藤雅彦, 岡本栄司, "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, 2008

[4] 金岡晃, 藤堂伸勝, 加藤雅彦, 岡本栄司, "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", 第 5 回情報通信システムセキュリティ時限研究会, 2008

[5] National Vulnerability Database
http://nvd.nist.gov/

[6] JVN iPedia
http://jvndb.jvn.jp/

[7] Common Vulnerability Scoring System
http://www.first.org/cvss/

[8] 小林克己, 寺田真敏, 山岸正, 小林偉昭, "CVSS を用いた脆弱性評価の検討", CSS2006, 2006

[9] 脆弱性定量化に向けての検討報告書
http://www.jnsa.org/result/2006/tech/vulnera/