不正アクセス被害予測のためのデータ作成支援ツールの検討*

大谷尚通　井上潮　桑田喜隆†
(株)NTTデータ 技術開発本部§

1 はじめに

大規模で複雑なシステムにおいて,不正アクセスによって引き起こされる被害を正確かつ迅速に見積もることは難しい．そこで筆者らはリソース依存モデルを用いた被害予測システム[1]を提案した．本システムは,不正アクセスを受けたシステムの状態をシミュレーションする事によって,副次的な影響を含む全体の被害状態を迅速に予測できる．本稿では,実システムを効率良くモデル化できるようにするための階層化手法と依存関係情報の収集及びモデル構築支援ツールについて述べる．

2 リソース依存モデル

リソースとは,システムを構成する計算機やネットワークインフラのような物理的なものだけでなく,ソフトウェアや人,業務のように無形のものも含む．あるリソースが他のリソースを使用したり,他のリソースの状態に影響を受けたりする場合,この間には依存関係があると言う．あるシステムに関するリソースと依存関係の情報を記述したものがリソース依存モデルである．リソース依存モデルは,依存関係を有向グラフで表現した図1を基本構造とする．不正アクセスが,ある一つのリソースに影響を与えた場合,その影響は関係するリソースへ次々と伝播していく．本システムは,この影響の伝播をシミュレートし,影響を受けたリソースの資産価値等から,損害や逸失利益等を算出する．なお,リソース依存モデルはXMLを用いて記述する．

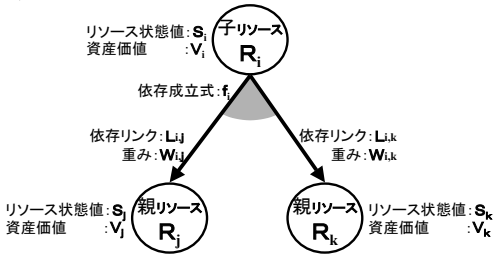

図１：依存関係のあるリソース間の表現

3 実システム適用時の課題と対策

大規模で複雑なシステムをモデル化する場合,以下の課題を解決する必要がある．

1. リソース依存モデルの設計
   数多くのリソースが複雑に組み合わされているため,依存リンク構造が複雑になり設計が容易でない．全リソースを忠実にモデル化しようとすると,作成コストが高くなる．
2. 依存関係情報の収集
   収集すべき情報量が多い．また,システム構成の変更に伴うモデルの修正にコストがかかる．
3. モデルの記述作業
   手作業によるモデルの正確な記述作業は困難である．

前記の三つの課題に対し,以下の解決方法をとる．

1. 三層モデルによる典型的なリソース依存モデルの提供
2. 依存関係情報の自動収集と自動生成
3. XMLで記述されたモデルの編集支援

以下,それぞれについて説明する．

4 リソース依存モデルの作成手法

4.1 典型的なリソース依存モデルおよび作成手法

被害予測を行うには,業務全体を一つのシステムとして捉えてモデル化する必要がある．そこで,まずシステム全体を業務,ワークフロー,組織,人員などの業務系,サーバ/クライアントソフト,DB等のアプリケーション系,通信,OS,ハードウェア等の基本システム系の三つに分類する(図2)．次にこの三つのそれぞれに適した方法を用いてリソース依存モデルを構築する．

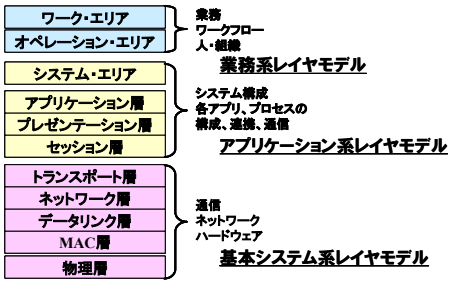

図２：被害予測の三層モデル

業務系レイヤは,業務や組織によってさまざまな形態が存在し,典型的なモデルに当てはめることが難しい．従って,このレイヤは,ヒアリング等によって業務体系やワークフローの情報を収集し,手作業によってモデル化する．

アプリケーション系レイヤは,クライアントサーバや三層アーキテクチャ等に基づいて構成されていることが多いため,いくつかの典型的なモデルに当ては

* Consideration of Data Collector and Editor for Network-Security Damage Estimation System.
† Hisamichi Ohtani, Ushio Inoue, and Yoshitaka Kuwata
§ Research and Development Headquaters, NTTDATA Corporation.

めることができる．従って,情報収集の自動化とモデル作成の手順化を行なう．

基本システム系レイヤは,計算機本体やネットワークセグメント等,個々の独立した要素から構成される．各リソースは独立性が高く,記述すべき依存関係は少ない．従って,複雑なリソース依存モデルは必要無く,リソース情報の自動収集もしくは他システムからの転用によってモデルを作成する．

4.2 依存関係情報の自動収集と自動生成

最近普及しているWebアプリケーションは,クライアント管理が不要なため,クライアントの特定が難しい．その他のアプリケーションにおいても,それらの間に成り立っている依存関係の抽出とモデル化にコストがかかる．そこで,アプリケーション系レイヤにおいては,依存関係情報を自動的に収集する方法を用いる．アプリ間の通信を傍受し,分析して,リソース依存関係の情報の記述フォーマット(XML)にあわせて出力するツールを開発した．このツールは,ネットワーク上を通過するパケットをキャプチャし,TCPパケットの場合はさらにプロトコルエンジンを用いてセッションを解析し,各アプリ間の通信記録から,その間の依存関係の情報を生成する．(図3)

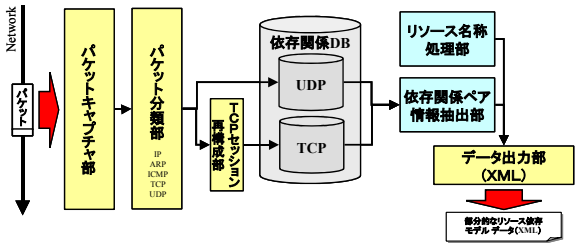

図 3：自動収集ツール構成図

4.3 リソース依存モデル編集支援エディタ

業務系レイヤのモデル作成は,手作業中心である．また,アプリケーション系レイヤの自動的に収集・出力された情報も目的に応じて手動により修正する必要がある．最終的には,基本システム系レイヤの情報も含め,各レイヤの情報を手動でまとめて,全体のリソース依存モデルを完成させなければならない．リソース依存モデルはXMLで記述されるため,テキストエディタを用いた編集も可能である．しかし,モデルの規模が大きくなれば、作業コストが上昇し,作業効率も悪化する。そこでリソース依存モデル専用の編集支援エディタを開発した．

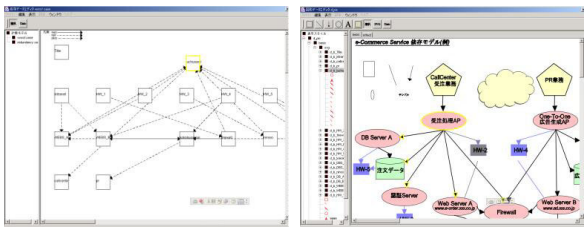

図 4:支援エディタ画面(依存関係エディタと図形エディタ)

リソース依存モデルを記述したXMLデータは,依存関係を記述する部分と,それを表現するための図形をSVG(Scalable Vector Graphics)を用いて記述する部分との性質の異なる二種類のデータから構成される．従って,グラフィカルな編集機能を備えた二つのキャンパスウィンドウ(図4)とその二種類のデータの間を関連付ける処理パネルを中心として構成される．(図5)

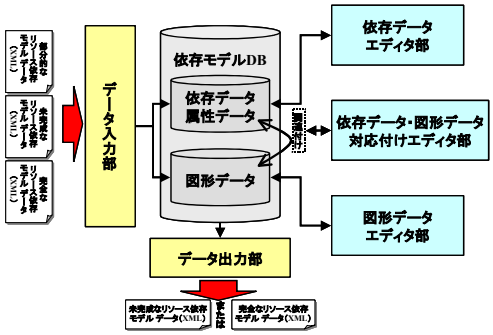

図 5：支援エディタ構成図

5 関連動向

不正アクセスによる業務停止時の逸失利益や浪費された人件費だけでなく,対策・復旧作業の人件費,損害賠償に要した費用,イメージダウンによる損害額等を含めたインシデント全体の被害額を求めるための被害額算出モデル[2]も提案されている．本システムによる逸失利益や浪費コストの予測算出と上記モデルを用いた広範囲な被害額算出により,対策投資額の見積もりや投資効果などを測定し,コストという明確な指標を用いた効率的な情報セキュリティマネジメントを実現することが可能になる．

6 まとめ

本稿では,リソース依存モデルを用いた被害予測システムの実用化に向けたモデル化手法の検討および構築支援ツールの開発について述べた．このように,被害予測対象のシステムを三つの構成要素に分類し,それぞれ適切な方式によってモデル化する手法をもとにして,依存関係情報の自動収集ツールとリソース依存モデル編集支援エディタによる構築支援を組み合わせた,効率的なモデル作成手法を実現した．

今後は,より多くの実システムをモデル化して実証実験を実施し,本被害予測システムおよびモデル化手法の有効性を確認したい．

参考文献

[1] 大谷尚通,桑田喜隆,小迫明徳,井上潮,“依存モデルを用いたセキュリティ・アセスメントのための被害予測システムの検討”,第16回コンピュータセキュリティ研究会,2002.

[2] 日本ネットワークセキュリティ協会,“情報セキュリティインシデントに係る調査”,IPA 平成13年度調査・研究報告書,2002.