マルチメディア通信と分散処理　106－28
コンピュータセキュリティ　16－28
（２００２．２．１５）

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

大谷 尚通, 桑田 喜隆, 小迫 明徳, 井上 潮†
†(株)NTTデータ 公共システム事業本部
〒105-0001 東京都港区虎ノ門 2-1-1 商船三井ビル
E-mail: {ootanihs, kuwatay, kosakoa, inoueu}@nttdata.co.jp

あらまし　不正アクセスによって引き起こされる被害を正確かつリアルタイムに求めるために，リソース依存モデルを用いた被害予測システムを提案する．この依存モデルは，システムや組織などが所有するソフトウェアやハードウェア，人員，業務といったリソースの情報をその依存関係と共に記述したものである．本システムは，不正アクセスよる予想損失額や被害を受けたリソースを推定して提示することによって，緊急対応フェーズにおけるシステム管理者の被害状況の把握や，対策の立案および実施に関する意思決定を支援する．

キーワード　被害評価, リスク・アセスメント, ネットワークセキュリティ, 意思決定支援, 不正アクセス, XML

Consideration of Network-Security Damage Estimation based on a Dependency Model

Hisamichi OHTANI, Yoshitaka KUWATA, Akinori KOSAKO, Ushio INOUE†
† Public Administration Systems Sector, NTT DATA CORPORATION
2-1-1, Toranomon, Minato-ku, Tokyo　105-0001, Japan

Abstract.　We propose the network-security damage estimation system with dependency model for understanding correctly damage caused by an illegal access at real-time. This dependency model has information of some resouces and these dependencies, and resouces are software, hardware, human and business process. This system can estimate damaged resouces and expectancy loss caused by an illegal access based on that model. As a result, the network administrator can understand situation of illegal access and make decision for planing and countermeasure on emergency response phase.

Keyword.　Damage Estimation, Risk Assessment, Network Security, Decision Support, Illegal Access, XML

1　はじめに

不正アクセスに対するセキュリティ・アセスメントは，主に不正アクセス発生前に実施しておく手続きである．そして，このアセスメント結果に基づいて不正アクセスの防止対策を施す．一方，不正アクセスにより被害が発生した場合，システム管理者には，被害の状況や影響範囲の正確な把握，迅速な対策の立案と的確な実施判断が求められる．このようなシステム管理者の状況把握，被害分析，意思決定を支援する緊急対策システムを筆者らは提案した[5].

本稿では，この緊急対策システムにおける被害分析方式として，不正アクセスによる被害のリアルタイムな推定手法およびプロトタイプシステムの実装について述べる．

2　不正アクセスに対するセキュリティ・アセスメント手法

セキュリティ・アセスメントやリスク管理は，ISO/IEC 17799(BS7799)[1], ISO/IEC TR 13335 (GMITS)[2]のような総合的なセキュリティマネ

ージメントのガイドラインに規定された一手法である．情報セキュリティにおけるリスク管理は，業務上の情報管理からコンピュータ・ウィルス，不正アクセスなど，広範囲を対象としているが，ここでは不正アクセスの脅威に対するリスク管理を中心に述べる．

2.1 セキュリティ・アセスメント

不正アクセスに対して事前に実施するセキュリティ・アセスメントには，以下のものがある．

a. システムやネットワークのセキュリティ状態，運用上のセキュリティポリシ，管理体制などを総合的に監査して，信頼性を計る．
b. 不正アクセスによるシステムやコンピュータ等の被害を事前に評価し，経営的な視点から対策や費用の投資判断を行う．
c. 脆弱性検査ツール(Vulnerability-Scanner)や手動にて模擬アタックを行い，システムやネットワークの弱点を検査する．

a，b は，業務的な側面からのアセスメントであるため，不正アクセスによるシステムの被害個所だけでなく，業務に及ぼす影響も把握することができる．つまり不正アクセスによる組織全体に対する影響や損害が評価できる．c は，個々のソフトウェア，コンピュータ上の具体的な問題点が明らかになるため，具体的な対策を施すことができる．

2.2 リスク・アセスメント

セキュリティ・アセスメントにおいて，事前に起こりえる危険を想定して，それによって引き起こされる被害程度を金額を用いて表す手法がリスク・アセスメントである[3]．以下にこのリスク・アセスメントの求め方を説明する．

- **リソースの定義**
  リスク・アセスメントでは，資産価値をもつもの，すなわち資産(リソース)を明らかにしなければならない．リソースは，ハードウェアやデータのようにそれ自体に価値を持つものだけでなく，ソフトウェアやネットワーク，人，業務のように無形のものも含まれる．
- **Single Loss Expectancy (SLE)**
  ある脅威によってリソースの失われる割合(0〜100%)を影響度(EF：Exposure Factor)とする．あるシステムにおいて，脅威が少数のリソースにしか影響しないならば EF 値は小さく，すべてのリソースに対して壊滅的な影響を与えるならば EF 値は 100%に近い値となる．

  ある一つの脅威が発生した場合に，あるシステムや組織が失う価値が予想損失額(SLE：Single Loss Expectancy)である．この値は，そのシステムや組織の資産価値(AV：Asset Value)と EF より，以下の式で表される[4]．

$$SLE = AV \times EF \qquad (式\ 1)$$

2.3 セキュリティ対策案の検討

セキュリティ対策案の検討において，費用対効果の高い対策案を選択して実施するために，上記の SLE からセキュリティ対策費用の投資額の見極めをおこなう．

システムや組織全体に対するリスクの表現は，この SLE および，SLE をベースとした年間予想損失額(ALE：Annualized Loss Expectancy)による被害額の表現が一般的であり，専ら経営的な視点に基づく事前対策手法に使われている．

3 問題点

現在の Firewall や IDS 等の技術では，不正アクセスを 100%阻止することは出来ない．もし，攻撃者が不正アクセスに成功した場合，システム管理者はそれによる被害を最小限にとどめなければならない．そのためには，不正アクセス緊急時対応計画[6]における緊急対応フェーズ(図 1)をすばやく実施することが求められる．

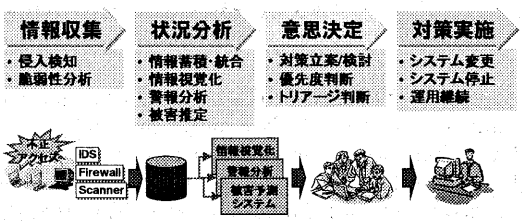

図 1：緊急対応フェーズ

筆者らが提案している図 1の緊急対応フェーズにおける対応ワークフローは以下の通りである．

1. IDS, Firewall による侵入検知
2. 警報のデータベース統合
3. 警報視覚化による状況把握
4. 注目すべき不正アクセス(EOI[1])の抽出
5. EOI の分析
6. 被害推定
   6.1. 被害範囲，程度の推定

[1] Event Of Interest

(不正アクセスが監視対象に与えた被害範囲や程度を推定する)

6.2. 対処による効果推定
(緊急対応や臨時的な復旧による回復効果を推測する)

7. 対策立案/検討
8. 対策実施

項目1から5までは，不正アクセス分析用統合データベースの構築，および情報視覚化を用いた状況把握・意思決定支援方式として提案され，連携した処理システムが実現されている[5]．しかし，項目6以降の処理方式はまだ実現されていない．

被害推定が実現できない理由は，以下の２つである．

- 大規模なシステムや業務は，多数のリソースから構成されており，ある不正アクセスの影響を受けるリソース，影響度(EF)を効率よく求めることが難しい．
- EOI による脅威は多数あり，脅威によって，影響するリソースとその EF が異なる．これらを一つ一つ洗い出すこと，予想損失額(SLE)を事前に求めておくことは困難である．

つまり，不正アクセスの影響を受けるリソースと EF を動的に検索し，被害を動的に推定できる方式および処理システムの実現が求められている．

4 リアルタイムな被害予測方式の提案

大規模なシステムや組織は，小さなリソースが無数に組み合わされて構成される．ある不正アクセスがリソースの一つ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．この影響が伝播する仕組みを用いることにより，不正アクセスから影響を受けるリソース，EF を動的に検索できる．このリソースが関係しあっている状態を記述したリソース依存モデルを作成し，ある一つの不正アクセスに対するリソースとリソースの資産価値(AV)，EF を動的に求める方式を提案する．

さらに，このリソース依存モデルを用いて，不正アクセスによる SLE の算出，被害を受けたリソース推定などが行える被害予測システムを提案する．被害予測システムは，不正アクセス後の被害推定だけでなく，不正アクセスを想定した被害予測(リスク・アセスメント)や複数被害のトリアージの判断にも使うことができる．

5 リソース依存モデル

リソース依存モデルは，主従の関係を持つ複数のリソース情報から構成される．このリソース間の主従の関係を依存リンクと呼ぶ．

5.1 リソース

リソース依存モデルには，ハードウェアやデータのようにそれ自体に価値を持つものだけでなく，ソフトウェアやネットワーク，人，業務のように無形のものもリソースとして記述できる．

また各リソースの大きさは，ハードウェア 1 個や社員 1 人のようにそれ以上分割不可能な最小単位から，社員数十人からなる業務グループ単位など，リソース依存モデルの設計方針によって自由に決めることが可能である．

5.2 依存リンク

あるリソースが他のリソースを使用している場合や他のリソースの状態に依存する場合，この２つのリソース間には依存リンクが存在する．依存リンクは，依存元(子リソース)から依存先(親リソース)への有向グラフで表現される．例えば，リソース「メールクライアント(ソフトウェア)」は「Pop サーバ(ソフトウェア)」の状態に依存し，「Pop サーバ」は「メールスプール(データファイル)」を利用している場合の表現は図 2のようになる．

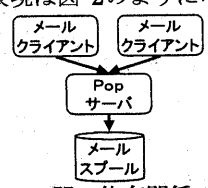

図 2：リソース間の依存関係の表現

図 3のように子リソース R_i は，2 つの属性値，資産価値 V_i とリソース状態値 S_i(S=0.0～1.0)を持つ．S_i=1.0 は R_i の機能が正常状態であることを示し，S_i<1.0 ならば何らかの異常があることを示す．S_i=0.0 ならば R_i の機能が完全に停止していることを示す．

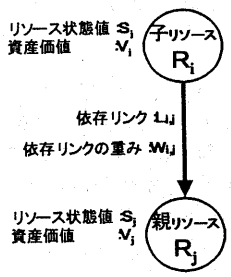

図 3：依存リンク表現

子リソース R_i は親リソース R_j への依存リンク $L_{i,j}$ が 1 つだけあり，その依存度(リンクの重み)を $W_{i,j}$ (W=0.0～1.0)とする．このとき，R_i の状態値 S_i は，次式より求められる．

$$S_i = S_j \times W_{i,j} \quad \text{(式 2)}$$

このときの R_i の予想損失額 SLE_i は，R_i の状態値 S_i と資産価値 V_i より，次式となる．

$$SLE_i = AV \times EF$$
$$= V_i \times (1-S_i)$$
$$= V_i \times (1-S_j \times W_{i,j}) \quad \text{(式 3)}$$

一つのリソースから複数のリソースに対して複数の依存リンクが存在する場合は，その複数の依存リンク間に成立条件が存在する．図 4の三層アーキテクチャによるクライアントサーバシステム(CSS：Client Server System)の例を用いて説明する．

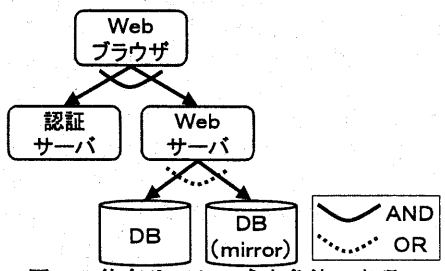

図 4：依存リンクの成立条件の表現

図 4は，一般的な三層 CSS に認証サーバと DB の多重化を施し，セキュリティ面と耐障害性を強化したシステムである．Web ブラウザは，Web サーバと認証サーバ両方のリソースを使用するため，両方への依存リンクをもつ．そして，Web ブラウザにとって Web サーバと認証サーバは，どちらも必要なリソースであるため，その依存リンクは成立条件 AND を持つ．また，Web サーバと DB，DB(mirror)の依存リンクは，DB のどちらか片方のリソースが使用可能なことが求められるため，成立条件 OR となる．

図 5は成立条件付き依存リンクを持つ最小のリソース依存モデルである．これを用いて，依存リンク間の成立条件について説明する．子リソース R_i は，親リソース R_j への依存リンク $L_{i,j}$ と親リソース R_k への依存リンク $L_{i,k}$ をもち，$L_{i,j}$ と $L_{i,k}$ 間の成立条件式は f_i で表される．このときの R_i の状態値 S_i は，

$$S_i = f_i(S_j \cdot W_{i,j} , S_k \cdot W_{i,k}) \quad \text{(式 4)}$$

となる．

リソースの状態値は，正常／異常の 2 値表現ではなく，0.0～1.0 の中間値で表現したい．次の成立条件式 f_i の例を考えた．

[A] $f_i(x) = \min(x)$：図 4の成立条件"AND"に対応．依存リンクをもつリソース R_x のうち，最も小さい x を選択する．よって，図 5において，R_i の状態値 S_i は以下の式で表される．

$$S_i = \min(S_j \times W_{i,j}, S_k \times W_{i,k}, \cdots) \quad \text{(式 5)}$$

[B] $f_i(x) = \max(x)$：成立条件"OR"に対応．依存関係をもつリソースのうち最も大きい x を選択する．よって(式 6)で表される．

$$S_i = \max(S_j \times W_{i,j}, S_k \times W_{i,k}, \cdots) \quad \text{(式 6)}$$

[C] $f_i(x) = \text{plus}(x)$：リソース R の状態が，依存する全ての親リソース R_x の状態に関係するような依存モデルの成立条件．例えば，ある業務を社員３人で分担する場合．依存関係をもつ親リソースの状態値の総和を取る．

$$S_i = (S_j \times W_{i,j} + S_k \times W_{i,k} + \cdots) \quad \text{(式 7)}$$

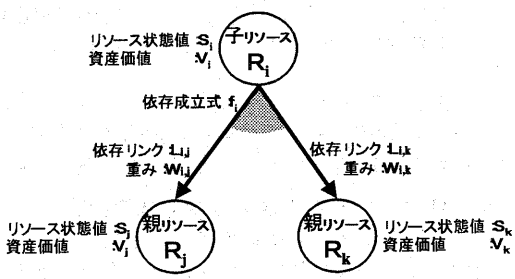

図 5：依存リンク成立条件の表現

5.3 被害影響範囲の導出アルゴリズム

依存モデルに対して不正アクセスによる直接の影響状態を指定し，依存リンクに沿ってその影響を伝播させることによって，影響を受ける全リソースを導出することができる．ただし，依存リンクの再帰的な状態はないものとする．図 6は，ハードウェア(コンピュータ)からソフトウェア(クライアント／サーバ)，人，業務から構成されるリソース依存モデルにおいて，リソース「コンピュータ 2」に対する脅威が発生した場合の影響範囲のイメージを表す．

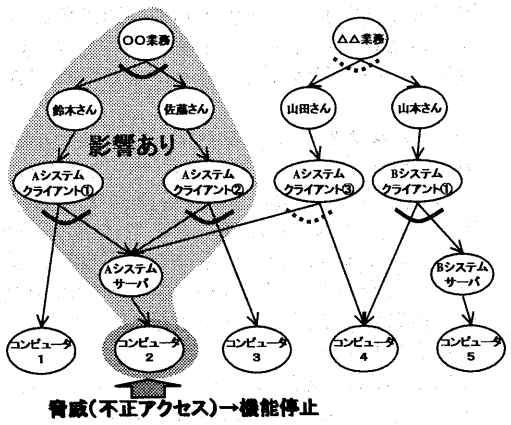

図 6：ある脅威による全影響の表現

図 5のリソース依存モデルの各要素に値を設定した例(図 7)を用いて，被害影響の導出アルゴリズムを説明する．

- 初期状態

  リソース R_k に対して不正アクセスが行われ，R_k の状態値 S_k=0.6 になった．リソース R_j は R_k と依存がなく独立しているため，不正アクセスの影響を受けず，R_j の状態値 S_j=1 となる．

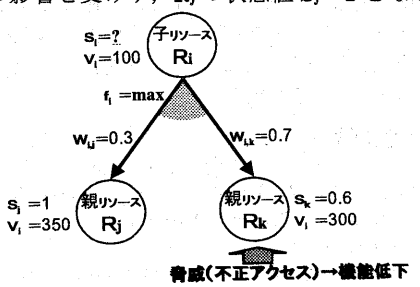

図 7：リソース R_k に対する脅威発生状態

- 計算 1

  リソース依存モデルに対して，状態値 S が定まっていないリソースに対して，依存成立式を用いて S の値を求める計算を繰り返す．図 7の子リソース R_i は，親リソース R_k，R_j と依存リンクがあるため，リソース R_i の状態値 S_i は，依存成立式 f_i より以下のように計算する．

$$\begin{aligned} S_i &= f_i(R_k, R_j) \\ &= \max\{ S_j \times W_{i,j}, S_k \times W_{i,k} \} \\ &= \max\{ 1 \times 0.3, 0.6 \times 0.7 \} \\ &= \max\{ 0.3, 0.42 \} \\ &= 0.42 \end{aligned} \qquad \text{(式 8)}$$

よって S_i=0.42，S_k=0.6，S_j=1 となる．不正アクセスによるリソース R_k の稼動状態悪化により，リソース R_i の稼動状態も大きく悪化していることが明らかになった．

- 計算 2

  計算 1 の結果より，この不正アクセスによるリソース R_i の EF_i は，$EF_i=1-S_i=0.58$ となる．よって，リソース R_i の被害値 SLE_i は，次式となる．

$$\begin{aligned} SLE_i &= V_i \times (1 - S_i) \\ &= 100 \times (1 - 0.42) \\ &= 58 \end{aligned} \qquad \text{(式 9)}$$

  この計算例では，資産価値 V_i の価値単位は千円／時と表現する．

- 計算 3

  よって，不正アクセスによるこの依存モデル全体の予想損失額 SLE は，各リソースの SLE の合計である．よって，3 つのリソースの予想損失額 SLE_j=0, SLE_k=58, SLE_i=120 より，

$$\sum_{n=i}^{k} SLE_n = 178 \qquad \text{(式 10)}$$

  となる．

よって，R_k に対する不正アクセスにより，このリソース依存モデルが受ける被害は，178,000 円/時と判明する．

6 リソース依存モデルを用いた被害予測システム(プロトタイプ)の実装

6.1 リソース依存モデルの実装

5で述べた方式に基づいてリソース依存モデルを表現するための記述フォーマットを設計した．リソース依存モデルの情報は，関連システムや組織間で収集や交換することを想定し，XML を用いることとした．この収集の仕組みを利用することによって，大規模なシステムや組織のリソース依存モデルを記述する場合，まずシステム管理者が，自分の管理するサブドメイン/セグメント範囲のリソース依存モデルを記述し，それらのリソース依存モデルを収集・結合することによって，大規模なリソース依存モデルが作成できる．

またこのフォーマットには，リソースおよび依存情報を記述するだけでなく，これを視覚化するための情報も記述する．

6.2 被害予測システムの実装

XML を用いて記述されたリソース依存モデルを読み込み，脅威による影響箇所を指定することによって，被害状況の予測／推定結果を出力する被害予測システム(プロトタイプ)を作成した．本シ

ステムは，Java2 Standard Edition をベースとして，XML の処理部に Xerces ver.1.4.3 を用いて構築した．

6.3 被害予測システムの動作例

インターネット接続点を持つ一般的なネットワークを想定したリソース依存モデルを用いた場合の動作例を以下に示す．

- 不正アクセスの指定

  被害予測システムにリソース依存モデルを入力し，IDS 等の検知結果をもとに不正アクセスによって直接被害を受けたリソースに異常な状態値を設定する．

- 影響分析結果の表示

  リソース依存モデルと被害箇所の設定より，被害の影響を計算し，その結果を視覚的に表示する(図 8，図 9)．図 8の左側のウィンドウは，被害リソースを依存リンクの構造を用いて表現しており，右側は，リソース依存モデル全体に対する SLE とその影響受けたリソースの一覧情報を表示している．依存リンクの構造の表現は，被害拡大の様子を把握できる．

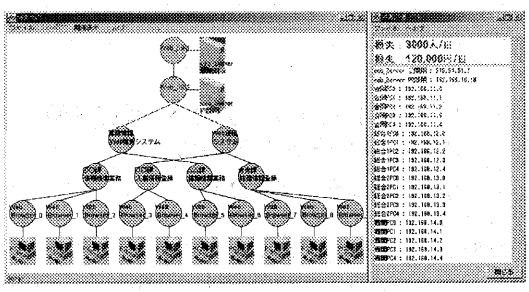

図 8：影響分析結果の依存リンク表示

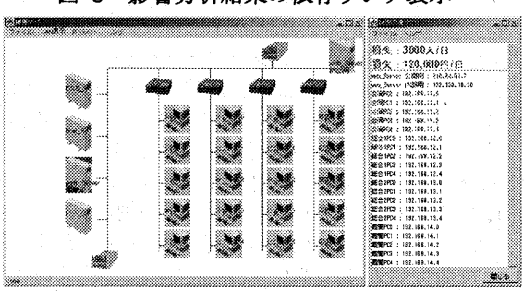

図 9：影響分析結果の LAN 表示

図 9の左側は，ネットワーク(LAN)構造を用いて，このネットワーク上の全リソースと被害リソースを表示した場合である．被害を受けてないリソース(S=1)の図形はそのままで，被害を受けたリソース(S≠1)の図形は色を付けて強調表示している．ネットワーク構造の表現は，被害個所の物理的な位置が把握できる．

システム管理者は，この被害個所や全体的な SLE，個々のリソースの被害状況の情報から，対策実施個所の選定，実施の判断が迅速に行える．システムの設定値を変えて被害予測を行うことにより，いくつもの脅威が同時に発生した場合のトリアージ(対処優先度)の判断や，複数の対応策から最善策を判断することも可能である．

また，実際に発生した被害の影響を“推定”するだけでなく，事前に脅威に対するシステムの影響度を“予測”するリスク・アセスメントの手段として利用することも可能である．

7 まとめ

本研究では，セキュリティ・アセスメントのためのリソース依存モデルと，それを用いた不正アクセスに対する被害評価方式を提案した．また，リソース依存モデルの XML-DTD の設計および被害予測システムのプロトタイプを構築し，被害把握や対策検討に利用できることを確認した．今後は，不正アクセス検出から状況把握，警報分析，被害推定まで視覚的に支援する連携システムを実現していく予定である．

参考文献

[1] British Standard, BS Tech Cttee BSFD/12, Info. Sec. Mgmt, "BS 7799 :1995 Code of Practice for Information Security Management", British StandardsInstitution, 1995.

[2] ISO/IEC TR 13335 "Information technology -- Guidelines for the management of IT Security", http://www.iso.ch/.

[3] Micki Krause, Harold F. Tipton, "Handbook of Information Security Management", Auerbach Publications.

[4] Stephen Northcutt, "Network Intrusion De-tection. An Analyst's Handbook", New Riders Publishing, 2001.

[5] 大谷尚通，桑田喜隆，小迫明徳，井上潮，岩田恵一，“広域不正アクセスに対する侵入検出・状況把握システムに関する検討”，第 63 回全国大会，pp. 499-500 2001.

[6] 田口 篤，楠 正宏，“対サイバーテロ・コンティンジェンシープランの立案の研究”，重要インフラセキュリティ対策事業 関連論文集，pp. 107-116 情報処理振興事業協会，2001.