2004－ＣＳＥＣ－26 (15)
2004／7／20

イベント依存モデルを用いた被害予測システムの実装

蓮井 亮二† 白石 善明†† 森井 昌克†

† 徳島大学工学部知能情報工学科 〒770-8506 徳島市南常三島町 2-1
†† 近畿大学理工学部情報学科 〒577-8502 東大阪市小若江 3-4-1
E-mail: †{hasui,morii}@is.tokushima-u.ac.jp, ††zenmei@info.kindai.ac.jp

あらまし ネットワークやシステムに対する不正アクセスを検知するシステムとしてIDS (不正侵入検知システム) がある．しかし，IDSは不正アクセスを検知するだけであり，事前に対処するものではない．そこで我々は，現在までに行われた不正アクセスから，その後に行われる不正アクセスを予想する方法としてイベント依存モデルを用いる方法を提案している．本稿ではイベント依存モデルを用いた被害予測システムを実装し，システムの有効性を示す．

キーワード 不正アクセス，被害予測，IDS(侵入検知システム)，依存モデル

Implementation of Damage Prediction System of Unlawful Access by Event Dependent Model

Ryoji HASUI†, Yoshiaki SHIRAISHI††, and Masakatu MORII†

† Department of Information Science and Intelligent System, The University of Tokushima
2-1 Minamijyousanjima, Tokushima-shi, 770-8506, Japan.
†† Department of Informatics, Kinki University
3-4-1, Kowakae, Higashi-Osaka, 557-8502, Japan.
E-mail: †{hasui,morii}@is.tokushima-u.ac.jp, ††zenmei@info.kindai.ac.jp

Abstract IDS(Intrusion Detection System) is well known as a system that detects unlawful computer access to network and systems. However, it is impossible to deal with IDS for unlawful computer access beforehand. We have proposed a method for predicting the unlawful computer access using the event dependent model. We implement damage prediction system of unlawful access using event dependent model. In this paper, we show effectiveness of the damage prediction system of unlawful access using event dependent model.

Key words unlawful computer access, damege prediction, IDS(Intrusion Detection System), dependent model

1. まえがき

外部ネットワークからの不正アクセスを防ぐ手段としてファイアウォールが広く普及している．しかしながらファイアウォールを経由しないまたは通過する不正アクセス手法が存在するため，IDS(侵入検知システム:Intrusion Detection System) を併せて導入するところが増えてきている．近年，IDSはセキュリティ分野で注目されており，IDSに関する研究や製品開発が活発に行われている．

IDSはシステムやネットワークの資源および活動を監視し，不正アクセスを検出する．システムあるいはネットワークが不正に使用された形跡を発見した場合，IDSはそれを管理者に通知する．監視対象サーバに直接インストールし，自ホストに流れてきたパケットやシステムの活動やログなどを検査対象とし，不正アクセスを検知するIDSをホストベースIDS(Host-based IDS) [1][2]と呼ぶ．ネットワーク上のトラフィックを監視し，既知の不正アクセスパターンに一致するパケットを検出したり，ユーザの普段のプロファイル情報と異なる動きやパケットを検出するIDSをネットワークベースIDS(Network-based IDS) [3]～[5]と呼ぶ．

IDSを利用して不正アクセスによる被害を防ぐためにはセキュリティに関する高度な専門知識が要求される．なぜならばIDSが発する多数のアラートの中から実施された不正アクセスを見つけ出し，さらにその対策を調べなければならないからである．またIDSが発するアラートはシステムまたはサービス間の不正アクセスに関する関連性を考慮していない点も，アラートから実施された不正アクセスを見つけ出すことが困難な要因となっている．このような問題点により，ローカルドメインのネットワーク管理者は正しくIDSを運用できていないことが多い．この問題点を解決する手段として，ローカルドメインに

設置した IDS の遠隔監視サービス [6] [7] や被害解析支援システム [8] などが存在する．ローカルドメインで何らかのインシデントが発生し IDS が不正アクセスを検知した場合，IDS の遠隔監視サービスではサービス提供者がアラートを受け取る．そしてローカルドメインの管理者に代わってアラートを分析し，インシデントに関する報告書を作成する．被害解析支援システムではそのシステムが IDS のアラートを受け取り，ローカルドメインの管理者に代わって被害の検出，原因の特定および対策の提示を行う．

遠隔監視サービス [6] [7] や被害解析支援システム [8] を用いることで，発生した不正アクセスに対して事後の対処を行うことはできる．しかしながらこれらのシステムを用いても不正アクセスを事前に防ぐことはできない．これは IDS が不正アクセスを検知するだけであり，不正アクセスに対して事前に対処するものではないことに起因している．そのため将来起こり得る不正アクセスの被害を予測し，迅速に対応することで被害を最小限度に抑えることが必要とされている．

不正アクセスによる被害を予測する研究にニューラルネットワークを用いた被害予測方式 [9] がある．この方式はニューラルネットワークを用いて被害を “実害なし”，“環境情報漏洩”，“性能低下”，“システムダウン”，“不正操作” の五つに大まかに分類し，現在までに起こった不正アクセスから予想されるシステムやネットワークの被害状況を予測するものである．今後実施される具体的な不正アクセスを予測するものではないため，不正アクセスを事前に対処することはできず，被害を最小限に抑えるという目標を達成することは困難である．

本稿では不正アクセスによって発生するイベントに着目し，現在までに行われた不正アクセスからその後に行われる具体的な不正アクセスを予測するためのイベント依存モデルを提案，実装し，その有効性を示す．本システムを利用することで，精度の高い被害予測ができ，ローカルドメインのネットワーク管理者は被害を最小限に抑えるための対策方法を容易に得ることができる．さらに本システムによって得られる対策を実施することで不正アクセスに対して事前予防 (プロアクティブな対応) が可能となる．

2. 被害予測システム

2.1 概　　要

本稿で提案するイベント依存モデルを用いた被害予測システムの目的は IDS が発するアラートから将来起こり得る不正アクセスを予測することである．

被害予測システムの流れを説明する．被害予測システムを設置したサイトで何らかのインシデントが発生した場合，サイト内に設置されている IDS は自動的に被害予測システムに接続し，アラートを被害予測システムに送る．被害予測システム側では受け取ったアラートをイベント依存モデルを用いて分析し，将来起こり得る不正アクセスを予測する．被害予測結果には予測される不正アクセスとその対策が示されている．

被害予測システムの最も簡単な使用環境は単一サイト内で使用することである．しかしながら被害予測システムを単一サイト内で用いる場合，IDS をサイト内に設置しなければならず，ネットワーク管理者にとって負担が大きい．なぜならば IDS の能力を最大限発揮するためにはシグネチャを常に最新のものに更新し続けなければならないからである．また IDS には固有の特徴があり，1 つの IDS を用いるだけでは全ての不正アクセスを検知することはできないことが知られている．この問題は複数の IDS を利用する事で解決できるが，複数の IDS を運用，管理することはネットワーク管理者の負担を増大させる．

上記 2 つの問題点を解決する方法として著者らが提案している Center Management Type Intrusion Detection System (以下センター集中管理型侵入検知システムと称する) [10] がある．本稿ではセンター集中管理型侵入検知システムの中で被害予測システムを用いて被害を予測することを考える．

図 1 はセンター集中管理型侵入検知システムを用いた被害予測システムの構成図である．センターは複数のサイトを監視する．監視しているサイトで何らかのインシデントが発生した場合，そのサイトは自動的にセンターに接続する．そしてパケットキャプチャエージェントが記録した通信データ (以下監査データと称する) をセンターに送る．センター側では数種類のネットワークベース IDS を設置しておき，そのネットワークベース IDS を利用して受け取った監査データを分析する．被害予測システムは数種類の IDS が出力したアラートから今後起こり得る不正アクセスを予測する．被害予測システムでは，各アラートの依存関係を調べることでイベント依存モデルを作成し，不正アクセスを予測することができる．そして不正アクセスを受けたサイトの管理者に予測される不正アクセスとその対策を通知する．

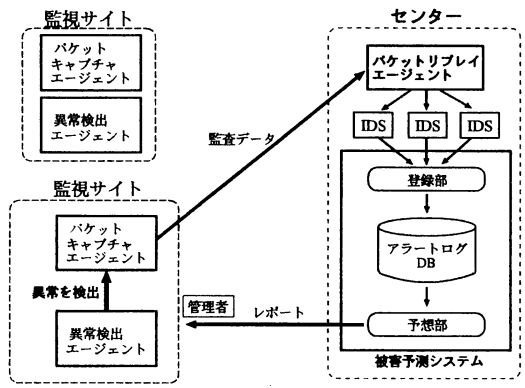

図 1　センター集中管理型方式を用いた被害予測システム

2.2 構　　成

図 2 は被害予測システムの構成と処理の流れを示している．被害予測システムは登録部，アラートログ DB，予測部から構成される．

[異常検出エージェント]

異常検出エージェントは監視しているホストの状態やファイアウォールのログから異常を検出する．異常検出時にはパケットキャプチャエージェントに監査データをセンターへ送信することを指示する．異常検出エージェントが検出する異常として攻撃者からの偵察行為やファイルの改ざんなどが想定される．異常検出エージェントには既存のホストベース IDS を用いる．

[パケットキャプチャエージェント]

パケットキャプチャエージェントの役割は監視対象を出入りする全ての通信を記録することである．そのためパケットキャプチャエージェントは監視サイトの出入口であるゲートウェイ

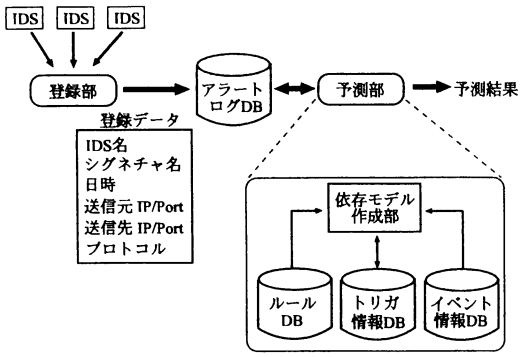

図 2　被害予測システムの構成と処理の流れ

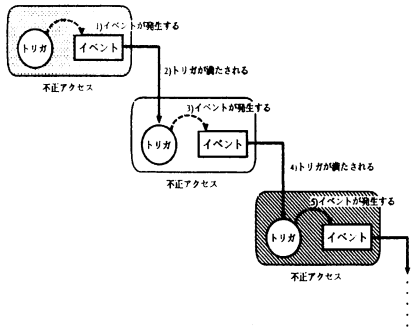

図 3　不正アクセスの連続性

付近に設置される．被害予測時に攻撃者が監視サイトから得た情報を解析に利用するために，監視サイトから出ていく通信も記録する．

パケットキャプチャエージェントは異常検出エージェントからインシデント分析開始の指示を受けた場合，監査データをパケットリプレイエージェントに送信する．その際記録している全てのデータを送信するのではなく，インシデントが検知された時刻付近の監査データのみを送信する．

[パケットリプレイエージェント]

パケットリプレイエージェントの役割は受け取った監査データをセンターのシュミレーションネットワークに再発生させることである．再発生した監査データは数種類のネットワーク IDS で分析される．複数の IDS を用いて分析することで検知率の向上が望める．

[アラートログ DB]

アラートログ DB の役割は不正アクセスが発生した際に過去にさかのぼって被害予測を行うことができるように，アラートに関する情報を保存することである．これにより，偵察行為と偵察行為後に実施される不正アクセスに十分な時間が空いても被害予測が可能となる．

アラートログ DB に記録するデータ項目を表 1 に示す．アラートログ DB には，IDS 名，シグネチャ名，日時，攻撃元情報，攻撃先情報，プロトコルが記録される．IDS 名とシグネチャ名は検知された攻撃を特定するために必要である．日付，時刻は出力されたアラートの順序関係を把握するときに必要となる．送信元 IP/Port，送信先 IP/Port は攻撃元と攻撃先を特定するために必要である．また，その他の情報としてプロトコルの種類も必要である．これらの項目は IDS が出力する全てのシグネチャに含まれる内容である．

[登録部]

登録部の役割は各種 IDS から受け取った書式の異なるアラートから被害予測に用いる情報を抜き出し，統一されたフォーマットをもつアラートログ DB に格納することである．センター側では数種類のネットワークベース IDS を利用する．IDS が出力するアラートの形式は IDS ごとに異なる．そこで，“アラートログ DB ” で述べた全てのシグネチャに含まれ，かつ被害予測に役立つ情報をアラートから抜き出し，アラートログ DB に登録する．

[予測部]

予測部の役割はアラートログ DB に保存されている情報から被害を予測することである．その際 **3** 章で述べるイベント依存モデルを用いて被害を予測する．

3. イベント依存モデル

3.1 概　　念

集中的かつ連続的に不正アクセスが成功することは稀である．ある種の不正アクセスを検知しさらに防御したとしても，何らかの脆弱性は残っており，ある程度期間が経った後でその脆弱性を利用して不正アクセスに成功される危険性は依然として残ってしまう．

このような将来起こり得る不正アクセスを予測する方法として，ある不正アクセスが起こった時にその後どのような不正アクセスが実施されるかという不正アクセスの傾向を全て DB 化することが考えられる．しかし不正アクセスの手法は攻撃対象にインストールされている OS やソフトウェアの違いによって，様々な方法が存在する．また不正アクセス手法は日々進化しており，OS やソフトウェアの新たなバージョンで脆弱性が発見されると，その脆弱性を利用した新たな不正アクセスが増えることになる．そのため不正アクセスの傾向をあらかじめ DB 化するだけでは上で述べた不正アクセスの多様性に対応することが困難である．

そこで本研究では図 3 に示すような，ある不正アクセスによって発生したイベントがさらなる不正アクセスのトリガとなり，新たにイベントが発生するような不正アクセスの連続性に注目する．ここでイベントとは不正アクセスによって起こる攻撃者の状態の変化である．本研究においては IDS のアラートなどの不正アクセスの痕跡から得られるイベント情報から依存関係を調べる．イベント依存モデルとは不正アクセスによって発生するイベントをもとに各不正アクセスの依存関係を表したものである．イベントの依存関係を知ることにより，ある不正アクセスが実施された場合，多数存在する不正アクセス手法の中から次に実施される不正アクセスを絞り込むことができる．したがって今後実施される不正アクセスを予測し，被害を予測することが可能となる．

3.2 トリガとイベントの定義

攻撃者が不正アクセスを実施する際に，不正アクセスを成功させるための条件をトリガと呼ぶ．そして攻撃者が不正アクセスに成功した事によって起こる状況の変化をイベントと呼ぶ．

トリガには攻撃者が満たすべき条件と攻撃対象の環境が満たすべき条件の 2 つがある．攻撃者が満たすべき条件とは攻撃者

表 1　アラートログ DB の形式

IDS 名	シグネチャ名	日時						送信元情報		送信先情報		プロトコル
		年	月	日	時	分	秒	IP	Port	IP	Port	
Snort	SCAN namap TCP	2004	6	1	00	02	00	100.0.0.1	1800	192.168.67.131	23	TCP
Snort	SCAN fingerprint attempt	2004	6	1	00	03	00	100.0.0.1	1801	192.168.67.131	23	TCP
Snort	TELNET Bad Login	2004	6	1	00	03	30	100.0.0.1	2000	192.168.67.131	23	TCP
Snort	TELNET Bad Login	2004	6	1	00	03	40	100.0.0.1	3000	192.168.67.131	23	TCP
Snort	DOS Jolt attack	2004	6	1	00	04	10	100.0.0.1	4000	192.168.67.131	100	TCP
・	・	・						・		・		・
・	・	・						・		・		・
・	・	・						・		・		・

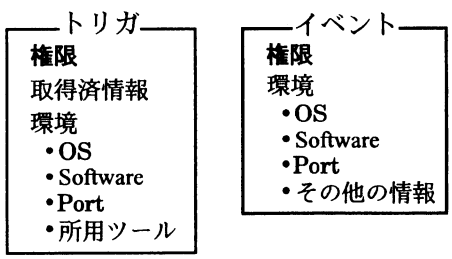

図 4　トリガとイベントの定義

が不正な操作を実行できるだけの権限を攻撃対象で有していることや，アカウント情報などの不正な操作を実行するために必要な情報を事前に知っていることである．攻撃対象の環境が満たすべき条件とは，不正な操作を可能にする OS やソフトウェアが攻撃対象にインストールされていることや不正な操作で利用可能なサービスが提供されていることである．また不正アクセスは一般的にツールを用いて実施される．そこで不正アクセスで使用されるツールがインストールされていることも攻撃対象の環境が満たすべき条件とする．以上より，不正アクセスが実施されるトリガは権限，取得済情報，環境 (OS，ソフトウェア，Port，所用ツール) の組で表すことができる．

不正アクセスが実施された場合，攻撃者にとって何らかのイベントが発生する．イベントとしては不正アクセスによって攻撃者が権限を取得する，または攻撃者の権限が昇格するといったことが挙げられる．またその他のイベントとして攻撃対象の環境 (OS，ソフトウェア，Port) に関する情報を得ることやそれ以外の情報を得ることが挙げられる．以上より，不正アクセスの実施により発生するイベントは権限，情報の取得 (OS，ソフトウェア，Port，その他の情報) の組で表すことができる．

以上を整理するとトリガとイベントはそれぞれ図 4 のように表すことができる．

3.3　イベント依存モデルのルール

不正アクセスが起こった際にはイベントが発生する．そのイベントが別の不正アクセスを引き起こすトリガとなっている場合，両不正アクセス間には依存関係があると言える．本節では依存関係があるかどうかを判断する基準となるルールについて説明する．

あるアラートを A_i とし，そのアラート A_i から作られるトリガを T_i，イベントを E_i と表す．このときアラートが n 種類存在する場合，トリガ情報 DB は $T = \{x|T_i, i = 1, 2, \cdots, n\}$，イベント情報 DB は $E = \{x|E_i, i = 1, 2, \cdots, n\}$ と表すことができる．

トリガとイベントの各要素は権限：$auth$，OS：os，ソフトウェア：$soft$，Port：$port$，所用ツール：$tool$，取得済情報：$info$，その他：$other$ とする．このとき，あるアラート A_i のトリガ情報は $T_i = \{T_{i.auth}, T_{i.os}, T_{i.soft}, T_{i.port}, T_{i.tool}, T_{i.info}\}$ と表すことができる．またあるアラート A_i のイベント情報は $E_i = \{E_{i.auth}, E_{i.os}, E_{i.soft}, E_{i.port}, E_{i.other}\}$ と表すことができる．

アラート A_i のイベント E_i とアラート A_j のトリガ T_j が次の関係を満たすとき，アラート A_i と A_j は依存関係があると定義する．

$$E_i \supseteq T_j \tag{1}$$

式 (1) の関係を満たすとき，A_i を依存元，A_j を依存先と定義する．依存元と依存先は必ずしも一対一対応であるとは限らない．一つのアラートから他の複数のアラートに対して依存関係が成り立つ場合もある．

式 (1) を満たしているかどうかの判断は，トリガ，イベントの各要素である “権限”，“OS”，“ソフトウェア”，“Port”，“その他” に対するルールを全て満たしているかどうかで判断する．

そのルールを以下に説明する．権限に関して，管理者権限は一般ユーザ権限よりも多くの実行権が与えられていることから，管理者権限は一般ユーザ権限を包含すると言える．そのため管理者権限を取得した場合，一般ユーザ権限で実行できることは全て実行できる．そこで権限に関して包含関係を考慮するルールを用い，依存関係を判断する．

例えばイベント $E_{i.auth}$ が “Administrator(管理者権限)” であり，トリガ $T_{j.auth}$ が “一般ユーザ権限” であったとする．この場合，Administrator 権限は一般ユーザ権限を包含するので，権限に関するルールである $E_{i.auth} \supseteq T_{j.auth}$ を満たす．よって両アラートは権限について依存関係があると言える．

これは OS やソフトウェアのバージョンに関しても言えることであり，OS やソフトウェアやその他に関しても同様の包含ルールを適応する．したがって依存関係を判断するルールは式 (2)〜(6) のようになる．

$$E_{i.auth} \supseteq T_{j.auth} \tag{2}$$

$$E_{i.os} \supseteq T_{j.os} \tag{3}$$

$$E_{i.soft} \supseteq T_{j.soft} \tag{4}$$

$$E_{i.port} = T_{j.port} \tag{5}$$

$$E_{i.other} \supseteq T_{j.tool} + T_{j.info} \tag{6}$$

上記の式 (2)〜(6) を全て満たした場合，式 (1) を満たしているとする．

また不正侵入者は過去に得た情報を利用して不正アクセスを行うことがある．この過去に得た情報とは計算機の稼働状況や

ツールとなるファイルの存在などを指しており，イベント情報の中ではその他の情報 $E_{i.other}$ としてまとめている．次に起こる不正アクセスの依存関係を調べる際には，過去に得られた情報 $E_{i.other}$ を引き継いで判断する必要がある．式 (1) を満たして依存関係が認められた際には，アラート A_j から作られる E_j の情報 $E_{j.other}$ にそれまで起こったイベントの情報 $E_{i.other}$ を加えた $E'_{j.other}$ を次のイベント $E_{j.other}$ とする．

4. 被害の予測方法

不正アクセスが検出された際に IDS が出力するアラートを被害予測システムの入力とし，**3.3** 節で述べたルールに基づいてイベント依存モデルを作成することで，今後実施される不正アクセスを予測する．

イベント依存モデルを作成する手順を次に示す．

Step1) 依存元の指定

入力されたアラートから依存元となるアラートを一つ選ぶ．

Step2) イベント情報の取得

Step1 で依存元に指定したアラートのイベント情報を取得する．

Step3) 依存先候補を取得

依存元を除いたアラートの中からトリガ情報が依存元のイベント情報と依存関係にあるアラートを取得する．

Step4) 依存先の決定

依存先候補のアラートの中から一つ選択し，次の依存元とする．

Step1 で依存元となるアラートを指定して，Step2 ～ Step4 の処理を繰り返すことで，依存元から依存関係によって繋がっているアラートを辿り，ある程度先に繋がっているアラートまで調べる．そして Step1 で指定する依存元を別のアラートに変更して，上記の処理を繰り返すことで，入力された全てのアラートに対して依存関係を調べる．イベント依存モデルの構成を図 5 に示す．複数のアラートを入力とすることによって，Step2 ～ Step4 の処理を繰り返し調べた依存関係の結果に重複箇所が表れることがある．これにより，実施される可能性が高い不正アクセスを予測することができる．

攻撃者が不正アクセスを実施したとき，攻撃者が攻撃対象から得た情報全てが IDS が出力するアラートに記述されているとは限らない．例えば，攻撃者がポートスキャンを実施した場合，攻撃者は攻撃対象でサービスを提供しているポート番号に関する情報を得る．これに対しポートスキャンの痕跡を示すアラートから攻撃対象でサービスを提供しているポート番号を得ることはできない．そこで被害予測の精度向上のために攻撃者が攻撃対象から得た情報の中で，IDS から出力されるアラートには含まれない情報を被害予測システム側で調べ，被害予測に用いる．**2.2** 節でパケットキャプチャエージェントが監視サイトのゲートウェイを出入りする全ての通信を記録することを述べた．通信内容を調べることで攻撃者が監視サイトから得た情報を被害予測システム側でも知ることができる．攻撃者が攻撃対象から得た情報を被害予測で用いることができるため，攻撃者が今後実施する不正アクセスと被害予測システムが予測する不正アクセスの方向性が一致する．したがって，攻撃者が得た情報を被害予測に用いることで，予測結果に明らかに実施されない不正アクセス名が含まれることを防げる．そして，今後実施される可能性の無い不正アクセスが予測結果から省かれることで，ネットワーク管理者は予測結果を元にした対策が取りやすくなる．

なお，攻撃者が攻撃対象から得た OS や ソフトウェア の種類やバージョンに関する情報や攻撃対象でサービスを提供している Port に関する情報を監査データから被害予測システム側で調べる．

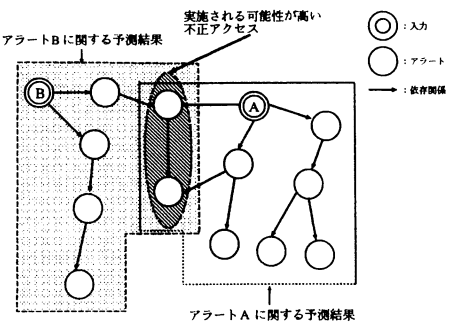

図 5 イベント依存モデルの構成

5. 実装実験

5.1 実験設定

被害予測システムの予測部を実装し実験した．IDS として Snort2.1.3 を用いた．また，実験データは，平成 11 年度～平成 13 年度にかけて，警察庁，通信放送機構 (TAO)，中央大学，徳島大学が共同で行った警察プロジェクト (不正アクセス検知プロジェクト) で取得した不正アクセス実証実験データを使用した．予測部のトリガ情報 DB とイベント情報 DB，ルール DB は，Snort Rules Database [11] を元に人手により作成した．実験においては出力されたアラートの中で致命的でないアラートからその後実施された不正アクセスを予測できるかを確認した．

5.2 被害予測結果

被害予測システムの出力結果を図 6 に示す．被害予測システムへの入力は “WEB-IIS iissamples access” である．これは，WEB サーバの一つである IIS に含まれる脆弱なサンプルファイルに関する情報収集行為を示すアラートである．この不正アクセスは，脆弱なサンプルファイルに関する情報を収集するだけであるので致命的な不正アクセスではない．図 6 の予測結果から，将来起こり得る不正アクセスとして “WEB IIS msadcs.dll access” や “WEB-IIS .htrTransfer-Encoding : chunked” などの不正アクセスを予測できていることが分かる．攻撃者が “WEB IIS msadcs.dll access” や “WEB-IIS .htrTransfer-Encoding : chunked” の不正アクセスに成功すると Administrator(管理者) 権限を取得されるため，これらは危険な不正アクセスである．

被害予測システムの出力結果には各不正アクセス毎に成立するためのトリガを示す項目があり，ネットワーク管理者は被害条件 (トリガ表示) ボタンを押すことで，不正アクセスが成立するための条件を知ることができる．さらにネットワーク管理者はトリガ情報を見ることで，事前に不正アクセスへ対処することができる．“WEB IIS msadcs.dll access” のトリガ情報を図 7 に示す．“WEB IIS msadcs.dll access” に対しては図 7 のト

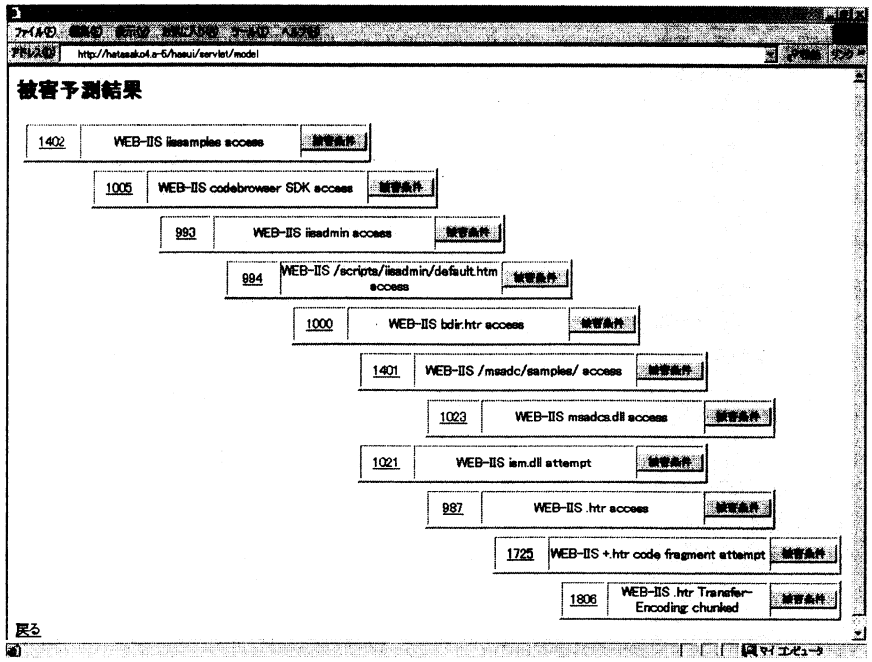

図 6 被害予測結果

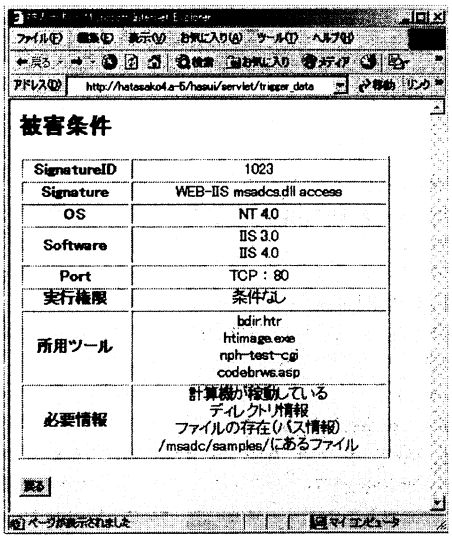

図 7 トリガ情報の出力結果

リガ情報から，ネットワーク管理者は "htimage.exe" を削除することで被害を未然に防ぐことが可能となる．

6. ま と め

本稿ではイベント依存モデルを用いた被害予測方法について述べ，被害予測システムの実験結果を示した．既存の IDS では将来起こり得る不正アクセスを予測することはできない．そこで被害予測システムを使うことで，管理者は将来実施される恐れのある不正アクセスの情報を容易に得ることができる．そのため事前に不正アクセスに対応することができ，被害を最小限に止めることができる．

文 献

[1] Internet Security Systems, Inc., RealSecure intrusion detection system, http://www.iss.net/.

[2] Tripwire, Inc., Tripwire, http://www.tripwire.com/.

[3] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks," Proc. of 13th Systems Administration Conference(LISA'99), pp.229–238, 1999.

[4] P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proc. of 9th ACM Conference on Computer and Communications Security, pp.245–254, 2002.

[5] 岡本 忠志, 白石 善明, 大家 隆弘, 森井 昌克, "なりすましに対する不正侵入検知システム (IDS-M)," 信学技報, OFS99-15, pp.39–46, 1999.

[6] KDDI 株式会社, セキュリティ監視サービス, *available at http://www.kddi.com/.*

[7] Internet Initiative Japan Inc., IIJ ネットワーク侵入検知サービス, *available at http://www.iij.ad.jp/.*

[8] Y. Tachibana, H. Takeuchi, H. Kurauchi and M. Morii, "Damage Analysis Support System for Illegal Access," Proc. of 7th World Multi-Corference on Systems, Cybernetics and Informatics(SCI2003), Jul. 2003.

[9] 鴨田 浩明, 馬場 達也, 小久保 勝敏, 松田 栄之, 矢口 博之, "ニューラルネットワークを利用した不正アクセス被害予測方式," コンピュータセキュリティシンポジウム 2002(CSS2002), pp.131–136, Oct. 2002.

[10] Y.Shiraishi, T.Kuribayashi and M.Morii, "Center Management Type Intrusion Detection System," Proc.of 7th World Multi-Corference on System, Cybernetics and Informatics(SCI2003), pp.337-381, Jul. 2003.

[11] Snort, Snort Rules Database, *available at http://www.snort.org/snort-db/.*