Computer Security Symposium 2017
23 - 25 October 2017

イベント依存モデルによる不正アクセスの推定

樫木 惟人[1]　曽根 直人[2]　森井 昌克[1]

概要：
先に，我々は不正アクセスを予測するためにイベント依存モデルを提案した．IDS(侵入検知システム) のシグネチャー情報をもとに依存関係を構築し，実行されている攻撃が成功すれば，そこから派生する可能性のある攻撃を絞り込み，次に受けうる攻撃を管理者が予測できることを示した．本稿では，イベント依存モデルをグラフデータベースを用いて再実装し，事前に入力したシステムの定義情報と IDS の出力するアラート情報を関連付け，より高精度な不正アクセスの推定を試みた．

キーワード：不正アクセス, IDS（侵入検知システム）, 依存モデル

Prediction of Malicious Access by Event Dependent Model

Korehito KASHIKI[1]　Naoto SONE[2]　Masakatu MORII[1]

Abstract: Previously, we proposed event dependent model to predict malicious access. Dependencies were built based on IDS(Intrusion Detection System) signatures. If the malicious access being executed is successful, we narrow down the one that may be derived from it, and showed that the administrator can predict the one that be accepted next. In this paper, we reimplemented event dependent model using the graph database. We tried to predict the malicious access with higher accuracy by correlating the definition information of the system entered in advance with the alert information outputted by IDS.

Keywords: Malicious Access, IDS(Intrusion Detection System), Event Dependent Model

1. はじめに

IDS(侵入検知システム:Intrusion Detection System) とは，システムやネットワークの資源および活動を監視し，不正アクセスの兆候を検知し，管理者に通知するシステムである．IDS は外部ネットワークからサーバを守る手段の一つとして利用されており，ファイヤーウォールと併せて導入するケースが一般的となっている．

IDS はネットワーク型とホスト型に大きく分けることができる．ネットワーク上を流れるパケットを監視し，不正アクセスの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 をネットワーク型 IDS と呼ぶ．監視対象サーバに直接インストールし，自分のホストに流れてきたパケットやシステムファイルやログなどを，定期的またはリアルタイムに検査する IDS をホスト型 IDS 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ローカルドメインのネットワーク管理者に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，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こと，及び 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からである．また IDS は不正アクセスを検知するのみであり，検知後の対応は管理者に任せられる．これは不正アクセスに対して IDS は事前に対処するものではないことに起因している．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

[1] 神戸大学
Kobe University
[2] 鳴門教育大学
Naruto University of Education

管理者は正しく IDS を運用することが難しい．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 [1] や被害解析支援システム [2] 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．遠隔監視サービスや被害解析支援システムを用いることで，発生した不正アクセスに対して事後の対処を行うことができる．しかしながらこれらのシステムを用いても今後発生しうる不正アクセスを未然に防ぐことはできない．そのため，不正アクセスを契機として，今後発生しうる被害を予測し，迅速に対応することで被害を最小限に抑えることが必要とされている．

我々はこの問題を解決するため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可能性の高い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した [3]．本モデルを使うことでローカルドメインのネットワーク管理者は被害を抑えるための対策方法を容易に得ることができる．そして，得た対策を実施することで不正アクセスに対して事前予防が可能となる．しかし従来の方法では RDB(Relational DataBase) を用いているため，柔軟な依存関係の記述ができなかった．

本研究では，これを解決するために我々はグラフデータベースを用いて依存関係の記述を行う．また，IDS の分解能を上げることで，より詳細な依存関係の構築を検討する．イベント依存モデルは IDS のアラート情報をもとに依存関係を構築して被害予測を行う．IDS のアラートはシグネチャー情報によるため，アラート内容よりさらに詳細な攻撃の情報を得ることができない．これを解決するために IDS の出力するアラートの詳細情報に関する依存関係を考慮し，より高精度な攻撃手法の推定を試みる．実際の攻撃を模擬するものとして，本稿では Nmap[4] の脆弱性スキャン用スクリプトの分解能に着目する．本来 IDS では Nmap を検知した場合，スクリプトの検知までは行えるがそれ以上の通知は得ることができない．しかし，例えば Wordpress であれば通信ログの URL 情報まで確認することでどのような脆弱性を狙っているか判明するものも有る．これにより，Nmap の脆弱性スキャン用スクリプトのイベント依存モデルへの適用を検討する．2 章で先に提案した被害予測システムとその問題点について述べる．3 章でイベント依存モデルの概念また作成方法, そして Nmap の脆弱性スキャン用スクリプトの分解能について説明し，4 章でイベント依存モデルの動作例について紹介する．

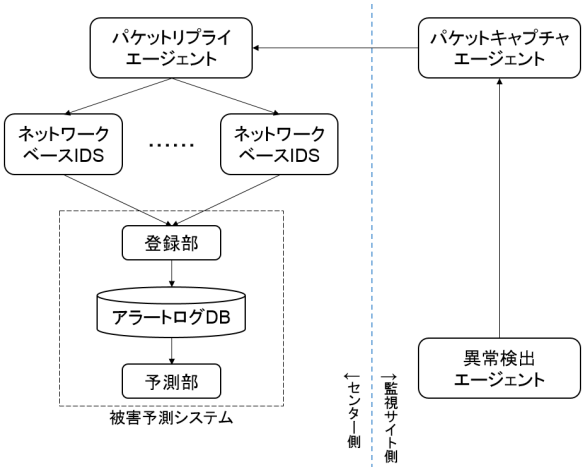

図 1　被害予測システムの構成と処理の流れ

2. 従来のイベント依存被害予想システム

2.1 概要

我々が提案した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被害を予測することである．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．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する．そして，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，将来の被害を予測する．不正アクセスを受けたサイトのネットワーク管理者に提示される通知結果には，予測される被害とその対策が含まれる．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，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．この問題を解決するために，監視形態をセンター集中型にすることで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 を配置しておき，受け取った監査データを分析する．センターに配置された被害予測システムでは数種類の IDS が出力したアラートから被害を予測する．その際，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，被害を予測する．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被害とその対策を通知する．

2.2 構成

図 1 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異常検出エージェント，パケットキャプチャエージェント，パケットリプレイエージェント，数種類のネットワークベース IDS，登録部，アラートログ DB と予測部から構成される．パケットキャプチャエージェントは監視サイト側のゲートウェイ付近に設置され，監視対象を出入りする全ての通信を記録する．パケットリプレイエージェントと数種類のネットワークベース IDS はセンター側のシミュレーションネットワーク上に配置される．監視対象に設置された異常検出エージェントはホストの状態やファイアウォールのログを監視する．ホストの状態やファイアウォールのログから異常が検出された場合，異常検出エージェントはパケットキャプチャエージェントに指示を出す．これにより，パケットキャプチャエージェントは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．パケットリプレイエージェントは受け取った監査データをシミュレーションネットワーク上に再発生させ，数種類のネットワークベース IDS に分析させる．数種類のネットワークベース IDS が出力したアラートは被害予測システムの登録部に送られる．登録部では各アラートから送信元 IP などの通信に関する情報が抜き出され，アラートログ DB に登録される．予測部はイベント依存モデルを用いアラートログ DB に登録された情報から被害を予測する．そして，予測した被害とその対策を含めた報告書を監視サイトの管理者に通知する．次に，上で述べた各要素について説明する．

[異常検出エージェント]

異常検出エージェントの役割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ことである．もし異常検出エージェントが異常を検出した場合，インシデントの分析を開始させるために，パケットキャプチャエージェントに指示を出し，監査データをセンターに送信させる．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として，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である．そのため，監視サイトの出入り口であるゲートウェイ付近に設置される．異常検出エージェントよりインシデント分析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．この際，記録している全ての監査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パケットリプレイエージェントに送信する．なお，パケットキャプチャエージェントでは監視サイトから出ていく通信も記録する．これは，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り，被害予測時に用いるためである．

[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側のシミュ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ベース IDS で分析される．数種類の IDS によって監査データを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間があいても被害予測が可能となる．

[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” で述べたどのシグネチャにも含まれ，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 節で述べるイベント依存モデルを用いて被害を予測する．予測部では複数の視点から被害を予測する．不正アクセスが同一の IP から実施された場合，その送信元 IP に関する情報をアラートログ DB から抜き出し被害を予測することが有効だと考えられる．また，不正アクセスが IP を変更しながら実施された場合，アラートログ DB に保存されている全ての情報から被害を予測する．

2.3 問題点

一般的に IDS は大量のアラートを出力する．膨大なアラートから攻撃を把握し，影響範囲を予測するには，高度なネットワーク知識を持つ必要があるが，対応できる管理者は不足している．このような問題を解決するため，我々はイベント依存モデルを提案したが，依存関係の記述に RDB を使用していたため，依存関係の柔軟な記述ができていなかった．またアラートが大量に発生した場合には，イベント依存モデルを作成するための検索時間が増加するという問題がある．イベント依存モデルは IDS のアラート情報をもとに依存関係を構築して被害予測を行う．IDS のアラートはシグネチャー情報によるため，アラート内容よりさらに詳細な攻撃の情報を得ることができない．IDS の分解能をあげることが可能であれば，より詳細な依存関係

を記述することができ，不正アクセスの推定がより高精度なものになると考えられる．

3. 提案システム

本章では，2 章で説明した従来の被害予想システムの問題点を改善した新しい被害予想システムを提案する．

3.1 グラフデータベース

近年，NoSQL と呼ばれるデータベースが注目を集めている．NoSQL では RDBMS がテーブルを中心にデータ処理を行うのに対して，より多彩な形式でのデータの保存，検索が行なえるため，より柔軟な設計が可能になっている．NoSQL の一種にグラフ構造の保存に適したグラフデータベースがある．イベント依存モデルが対象とする構造は，グラフとして記述することができるため，本研究ではデータベースとしてオープンソースのグラフデータベース Neo4j[5] を採用した．

グラフデータベースはノード (node)・属性 (property)・関係性 (relationship) という 3 つの基本要素により構成され，ノード間の関係性を表現することができる．またデータの操作は SQL ライクな CypherQL(Cypher Query Language) を使用して行い，Neo4j 標準の WEB インターフェースやシェル，REST API など複数の方法で実行できる．これを利用することで，RDB よりも柔軟に依存関係を記述し，RDB では対応が難しい検索であっても，クエリ言語で簡単に指定した依存関係そのものを検索することができる．また管理者にとっては視覚的であり，自分自身の環境を直感的に把握しやすい特徴を持つ．

3.2 被害予想システム

3.2.1 概念

不正アクセスの多様性には，攻撃対象の環境による多様性と不正アクセス手法の進化による多様性の 2 種類がある．攻撃対象の環境による多様性とは，攻撃対象にインストールされている OS の種類やバージョンなどの環境に攻撃者が実施する不正アクセスが依存するということである．不正アクセス手法の進化による多様性とは，日々新たな不正アクセス手法が考え出されるということである．そのため，不正アクセスの傾向をあらかじめデータベース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，IDS のアラートなどの不正アクセスの痕跡から得られる情報のイベント情報から依存関係を調べる．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．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がわかれば，ある不正アクセスを検知した場合に，数多ある不正アクセス手法の中から次に起こりうるだろう不正アクセスを絞り込むことができる．さらに，ある不正アクセスが実施された場合，今後に実施される不正アクセスを予測できることができ，それにより被害を予測することが可能となる．なお本稿では不正アクセスの痕跡を示す情報の一つである IDS のアラートからイベント依存モデルを作成する．

3.2.2 観測対象システムのモデル化

IDS で監視を行う対象について，監視対象ごとにシステム環境が大きく違うと考えられる．それゆえに，それぞれの環境に適したイベント依存モデルを作成する必要がある．監視対象システムをモデル化するに当たって，まず初めに監視対象で稼動しているシステム情報を取得しておく必要がある．またそのシステム上で使用されているソフトウェアなどにおいて，すでに確認されている脆弱性情報またそれによって引き起こる被害を CVE(Common Vulnerabilities and Exposures)[6] や CWE(Common Weakness Enumeration)[7] などから取得しておく．以上のように取得した情報をまとめ，事前にグラフデータベースにすることで監視対象の環境を把握することができる．システムの定義情報の作成例として図 2 を挙げる．図 2 の環境ではあるサーバの Apache 上で Wordpress が運用されている．そして Apache，Wordpress，また Wordpress で使用されているプラグインそれぞれで確認されている脆弱性を記している．このように監視対象の環境を調査し，そしてその環境で確認することができる脆弱性情報また被害をまとめることで事前にシステムの定義情報のモデルを作成する．

次に，IDS からリアルタイムに吐き出されるログをもとに，事前に作成したシステムの定義情報のモデルに情報を挿入していく．これにより，不正アクセスの影響範囲を推定するイベント依存モデルを作成する．本稿では，IDS としてオープンソースである Suricata[8] を利用する．Suricata はマルチスレッドに対応し，ルールセットを利用したネットワークトラフィックの監視や Lua スクリプトをサポートすることで複雑な脅威の検出を行うことができる．Suricata では様々なプロバイダが開発したルールセットを使用することが可能である．代表的なものとして，Snort[9] の VRT ルール [10] や Emerging Threats[11] などが挙げられるが，今回は VRT ルールを利用することとする．

VRT ルールセットではルールごとに Summary や Impact,Detailed information などいくつかの項目に分けられアラートの情報がまとめられている．この中で，Affected System の項目に着目し，この情報をもとにイベント依存モデルを作成していく．Affected System の項目にはアラートが発生した際に，影響を与えるシステム名についてバージョン情報も含め記述されている．IDS からアラートが発生した場合には，そのアラートのルールから Affected System の項目を取得し，該当するシステムが自身の環境に含まれていた場合，そのアラートをグラフデータベース

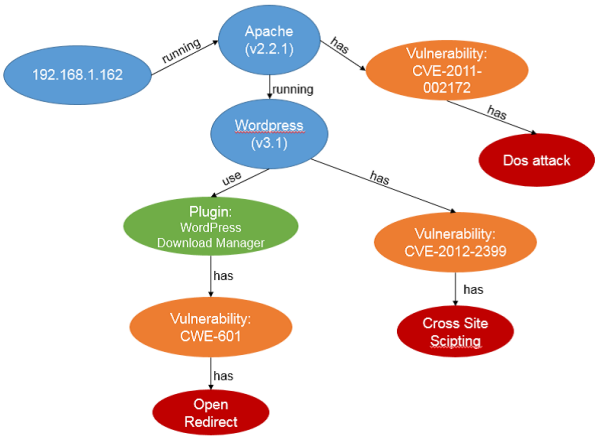

図 2　システムの定義情報の例

```
18:12:37.648678  [**] [1:2009358:5]
ET SCAN Nmap Scripting Engine User-Agent Detected
(Nmap Scripting Engine)
[**] [Classification: Web Application Attack] [Priority: 1]
 {TCP} 192.168.1.51:54868 -> 192.168.1.162:80
```

図 3　Nmap 脆弱性スキャン用スクリプトの IDS 検知例

に記述する．

3.3　IDS アラートの分析

イベント依存システムでは，導入しているシステムに応じたアラートを得ることができれば，より正確な被害予測が可能になる．しかし IDS のアラートをそのまま利用する場合には，アラートの分解能が不足する場合がある．IDS では Nmap の脆弱性スキャン用スクリプトを検知した場合，どのスクリプトを用いた場合であっても，図 3 のようなアラートが表示される．図 3 からわかるように，管理者は Nmap の脆弱性スキャン用スクリプトを用いてスキャンされたという事実は把握できるが詳細な情報は不明のため，攻撃者が何を目的にスキャンを実行したのか知ることができない．

しかし，実際には IDS の詳細ログからどのスクリプトが用いられたのかを特定可能な場合もある．例えば，非常に普及した CMS(Contents Management System) である Wordpress を対象とした Nmap の脆弱性スキャン用スクリプトは複数存在しているが，アラートから得られるのは Nmap によるスキャンという情報のみである．しかし，IDS の詳細ログに含まれているスクリプトがアクセスした URL の情報から，どのような脆弱性スキャン用スクリプトが実行されたか判別することができる．スクリプトを特定することができれば，どのような脆弱性を対象としているのか把握することができ，そこから派生する被害をイベント予測モデルを用いて推測することができる．

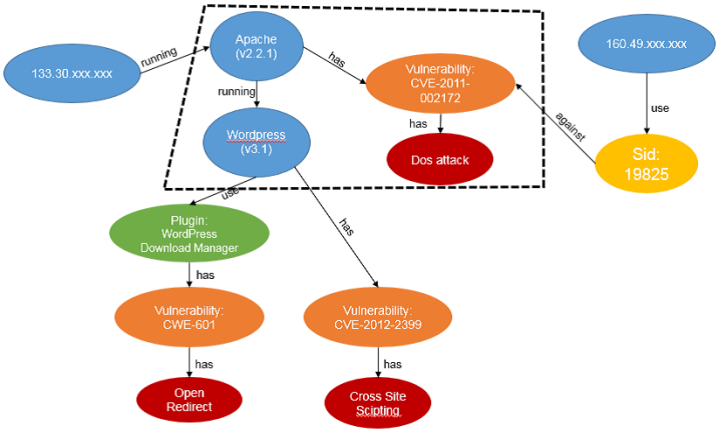

図 4　イベント依存モデル運用例

4.　イベント依存モデルによる推定

本章では，3 章で述べたイベント依存モデルの利用方法について説明する．図 4 は，実装したシステムから出力された結果の一部をイベント依存モデルとして図示したものである．各ノードには IP アドレス，システム，サービス，脆弱性，被害などが表示されている．図 4 では IP アドレス 160.49.xxx.xxx からの通信により，シグネチャ ID(Sid)19825 のアラートが検出されている．このシグネチャからは，Apache HTTPD Server の version1.3/2.x に影響を与えるという情報を得ることができる．よって Sid のノードから Apache(v2.2) のノードへの依存関係を記述することができる．そしてグラフデータベースの検索を行うことで，今後影響を受ける可能性がある範囲 (点線で囲っている部分) を検索することができる．例えば Apache が DoS 攻撃を受けてしまった場合，Apache 上で稼動している Wordpress についても依存関係からサービスに影響が出るということが検索可能となる．

5.　まとめ

従来は大規模かつ粒度の大きなイベントに注目していたが，提案システムではより粒度の細かいイベントに注目することが可能なシステムを提案した．例えば，Nmap の脆弱性スキャン用スクリプトの場合，従来ではそのスキャンが何を対象としたものか区別していなかったが，今回のシステムでは，詳細なアクセス URL の情報を利用し，どのような脆弱性を狙ったスクリプトかを判断することができる．また事前に観測対象のシステムをデータベースに記述することにより，より具体的な情報をシステム管理者へ提供することが可能となった．

参考文献

[1]　不正アクセス監視サービス (IDS),
http://www.intellilink.co.jp/security/services/scrutiny/01.html”,

accessed in Aug.2017.
[2] Y.Tachibana, H.Takeuchi, H.Kurauchi and M.Morii, "Damage Analysis Support System for Illegal Access," Proc. of 7th World Multi Conference on Systems,Cybernetics and Informatics(SCI2003),Jul.2003.
[3] 栗林利光, 白石善明, 森井昌克,"イベント依存モデルによる不正アクセスの被害予測," 2004 年暗号と情報セキュリティシンポジウム (SCIS2004), 2004 年 1 月.
[4] NMAP, https://nmap.org/",accessed in Aug.2017.
[5] Neo4j, https://neo4j.com/",accessed in Aug.2017.
[6] Common Vulnerabilities and Exposures, https://cve.mitre.org/",accessed in Aug.2017.
[7] Common Weakness Enumeration, https://cwe.mitre.org/",accessed in Aug.2017.
[8] Suricata, https://suricata-ids.org/", accessed in Aug.2017.
[9] Snort, https://www.snort.org/",accessed in Aug.2017.
[10] Talos, https://www.snort.org/talos", accessed in Aug.2017.
[11] Emerging Threats rules, https://rules.emergingthreats.net/", accessed in Aug.2017.