L-028

DNS に対する高度な攻撃を検出するためのデータマイニング
Data Mining To detect Sophisticated Attacks On DNS

湯原大二郎 † Daijirou Yuhara
宇井哲也 ‡ Tetsuya Ui
鈴木彦文 ¶ Hikofumi Suzuki

1. まえがき

近年, ネットワーク技術や計算機等の発達により，様々なサービスの実現やサーバの運用が可能となった．しかし, 公開性の高いサービスやサーバはセキュリティの脅威に曝されることが多く, その対応は非常に困難であり，攻撃の脅威に曝されるだけでなく，次の攻撃の踏み台となることも多い．

そこで, 防衛手段の一つとして, ポリシーに基づいた通信の制御を行う FireWall や IPS(侵入防止システム、Intrusion Prevention System)/IDS(侵入検知システム、Intrusion Detection System)，UTM(統合脅威管理, Unified Threat Management) 等のような装置が発達し，組織の安全性を確保している．これらの装置は様々な通信の制御に対して多くの機能を提供しているが，多くの場合，閾値やシグネチャパターン等に基づいた制御である．この制御方法は，シグネチャーパターンの開発が高コストになりや，高帯域・高速通信においてはボトルネックになることが非常に多い．また，近年では，DoS(サービス妨害攻撃、Denial of Service attack) のような攻撃であっても，前述のような制御を行う機器をすり抜けるような手法が主流となりつつある．

我々は，このような問題を解消するセキュリティエンジン・機器の研究と開発を行っている．その手法として，膨大な通信のログデータから攻撃をデータ解析・データマイニングし検知する手法を研究開発し，かつ，ボトルネックを解消するシステムの提案を行っている．しかしながら，(1) 研究に利用可能な大規模ネットワークの通信記録,(2) 個人情報の保護や通信事業法などの観点から研究開発することが難しく, 未発達な分野である．そこで本研究では信州大学で使用している UTM(統合脅威管理, Unified Threat Management) 装置による通信ログに対してデータマイニングを行った. 本論文では対象ネットワークの概略とデータマイニングの手法, 及び結果について述べる．

2. 解析対象とする通信記録

本研究では通信記録をデータ解析・データマイニングし攻撃性の高い通信やホストを特定する．しかし，上述したように現実の大規模な通信をターゲットとし分析を行う必要があり非常に困難である．特にセキュリティに関係する研究の場合，利用できる標準的な通信記録はなく，存在していたとしても最先端の攻撃手法とは異なってしまう恐れがある．そこで，今回は信州大学全域における現在の通信記録を利用することとした．

信州大学は図 1 で示すように県内各地にキャンパスが存在しているため, 各キャンパスを接続するためにネットワークの接続範囲は市町村の枠を超えて広大なものとなっている．また総合大学であり，大学の規模としては常勤職員と学生の合計で 14,000 人となり地方自治体程度の規模がある．そのため通信量も日に 3 千万〜1 億件近くと非常に多く, 様々な国から不審, 正常含めた多くのアクセスがあるなど通信内容は多様であり, 実験環境として理想的な環境となっている．本研究ではネットワークを管理している UTM 装置が生成する通信ログを使用した. 本研究では通信記録をデータ解析・データマイニングし攻撃性の高い通信やホストを特定する．しかし，上述したように現実の大規模な通信をターゲットとし分析を行う必要があり非常に困難である．特にセキュリティに関係する研究の場合，利用できる標準的な通信記録はなく，存在していたとしても最先端の攻撃手法とは異なってしまう恐れがある．そこで，今回は信州大学全域における現在の通信記録を利用することとした．

信州大学は図 1 で示すように県内各地にキャンパスが存在しているため, 各キャンパスを接続するためにネットワークの接続範囲は市町村の枠を超えて広大なものとなっている．また総合大学であり，大学の規模としては常勤職員と学生の合計で 14,000 人となり地方自治体程度の規模がある．そのため通信量も日に 3 千万〜1 億件近くと非常に多く, 様々な国から不審, 正常含めた多くのアクセスがあるなど通信内容は多様であり, 実験環境として理想的な環境となっている．本研究ではネットワークを管理している UTM 装置が生成する通信ログを使用した.

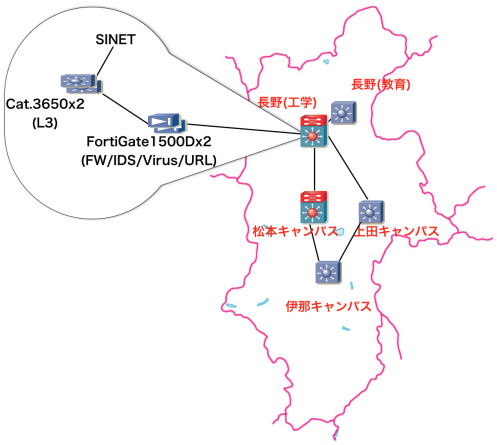

図 1: 信州大学のネットワーク構成

†信州大学大学院総合理工学研究科
‡信州大学大学院理工学系研究科
¶信州大学総合情報センター

3. 通信データの解析を利用した通信システムの概要

本研究では通信記録をデータ解析・データマイニングするエンジンを研究開発することを目的としている. このエンジンを用いて例えば次のような機器やシステムを構築することにより，高いスループットを実現できるセキュリティシステムの提案を行っている.

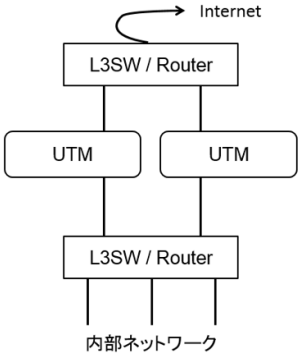

図 2: 一般的なセキュリティシステムの構成概略図

図 2 に一般的なセキュリティシステムを構築したネットワークの概略図を示す. すべての通信は UTM 装置を通過し一見セキュアな環境を構築できているように見えるが、大規模で高速なネットワークを構築したい場合この環境に耐えうる UTM 装置は非常に高価なものに限定され、実現の難易度は非常に高い.

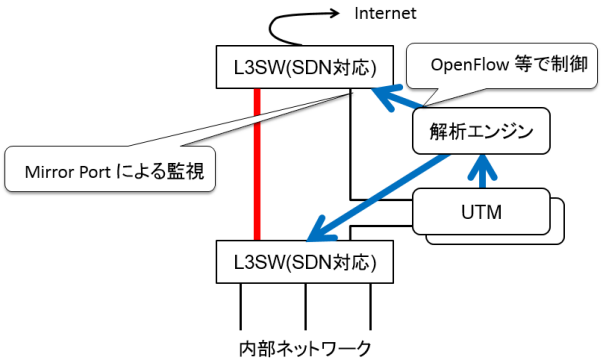

図 3: 提案するセキュリティシステムの構成例

一方で我々が提案するセキュリティシステムの概略を図 3 に示す.UTM 装置が存在する点では似通っているが、UTM 装置自体での厳密な判定を求めず、ある程度怪しいパケットを判別し、厳密な判定は解析エンジンに任せる. これならば UTM 装置にはそこまで高度な判定は求められないため比較的安価で済み、かつ通常の通信に対しては従来の方式と同等のペイロードを求めることができる. 本研究は図 3 における UTM 装置部分の判定に有効な方策を求める試みの一端である.[3]

4. 実施したデータマイニングによる解析

データマイニングには外れ値検出、非階層型クラスタリング、自己組織化マップの 3 つの手法を用いた.

4.1. 外れ値検出

以前、2015 年 11 月 26 日に実施された電子情報通信学会においてトラフィックログに対して外れ値検出を行うことがスパムメール検出に有効であることを示したが、対象ネットワークの機器に更新が入り環境の変更があったことが予想される. そこで先回の結果が環境の変更によっても変わらず得られることの検証も含めて再度外れ値検出手法によるデータマイニングを行う.[1]

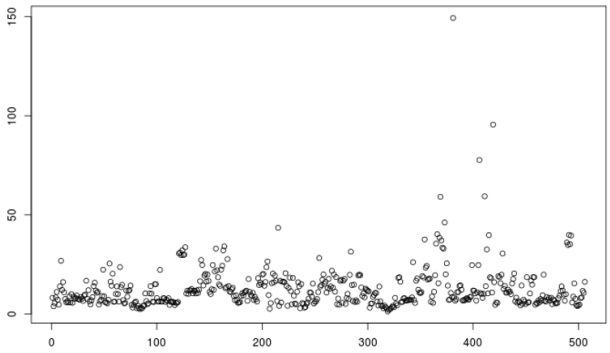

図 4: 外れ値検出のサンプル図

図 4 は、サンプルデータのうち、住宅データを用いて出力したものである. 縦軸が異常度であり、縦軸の数値が高いほどそのデータがその他のデータに比べて異常であることを示している. この場合の住宅データとは建築年数、付近住民の平均資産、家自体の価格など計 14 項目の数値データから成り立っている. 結果出力された 4 では、一つの住宅が他の住宅と比較して抜きんでていることが見て取れる. ただし、この場合優良か不良かはまだ判別できない. 判別したければ要素について調査し、判断する必要がある.[2]

4.2. 非階層型クラスタリング

非階層型クラスタリングとは、異なる性質の集団から複数のクラスタを作成する手法の一つであるが、階層型クラスタリングとは異なり、あらかじめいくつのクラスターに分けるかを決定しておく手法を指す. 本論文では k 平均法と呼ばれる手法を使用した.

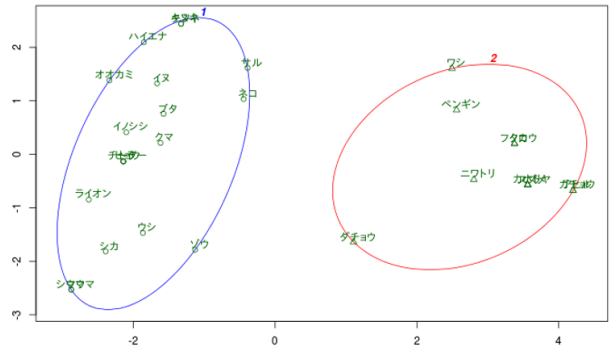

図 5: 非階層型クラスタリングのサンプル図

図 5 は動物の持つ特徴を四足、たてがみ、羽など細分化し、動物毎にその特徴を持つ場合は 1 、持たない場合は 0 といった具合に表を作り、その結果をクラス

タリングしたものである. 非階層型クラスタリングではクラスタの数は自動で決定されないため、クラスタ数はこちらで 2 つと指定してある. 結果的にクラスタは羽の有無から明確に分かれたことが見て取れる.[2]

4.3. 自己組織化マップ

自己組織化マップはニューラルネットワークの一種であり、教師なしニューラルネットの一つとして知られている. またクラスタリングの一種としても有名である. 自己組織化マップのサンプル図を図 6 へ掲載する.[2]

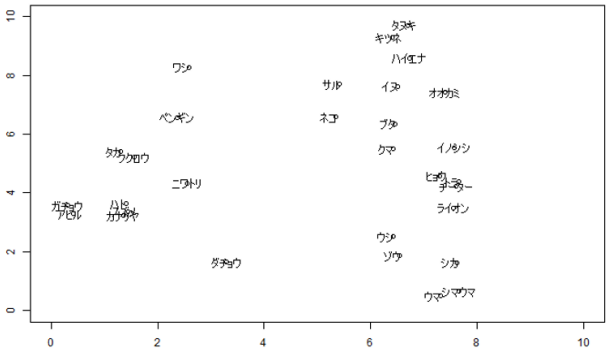

図 6: 自己組織化マップのサンプル図

自己組織化マップは非階層型クラスタリングとの比較のため非階層型クラスタリングと同様に動物の特徴データを使用してデータを出力した. 図 6 を見ると、多少の違いはあるものの、左右対称にした非階層型クラスタリングとほぼ同等の結果が出ていることがわかる.

5. データマイニングによるログ解析

今回は信州大学の UTM 装置ログから 2016 年 1 月 26 日のログを一時間ごとに区切ったデータを使用した. ログからは複数の項目を抜き出し、各値をまとめてデータマイニングした. ログの件数は一日で 1 億近くあり、対象が信州大学サーバであるパケットのみに絞っても 1 時間当たりの通信量は 300 万パケットを超える. また比較用にペネトレーションテストを行っていないログは午後 0 時台のログを同時に掲載し、ペネトレーションテストを行った午後 6 時台のログと並行して掲載する. また実施したペネトレーションテストを並行して行った、記録を表 1 に掲載する.

5.1. 外れ値検出

外れ値検出結果を図 7 に掲載する. 縦軸が異常度を表しており、異常度が高いほど他と比較して外れた通信だということが分かる. この時間帯に信州大学へ向けて発信された通信は約 313 万件だった. 図 7 は 2016 年 1 月 26 日 12:00-13:00 のログに対する外れ値検出の結果である. 数点異常と検出されているログが存在することがわかるが、基本的にほとんどが通常の通信であることが分かる.

表 1: 試験攻撃を行った日時と回数

日付	時間	攻撃回数
2016/01/25	10:48:14	10,000
2016/01/26	00:11:59	20,000
2016/01/26	17:37:27	20,000
2016/01/26	18:34:47	4,000
2016/01/27	15:39:50	50,000
2016/01/28	02:26:45	100,000
2016/01/28	02:52:42	100,000
2016/01/28	03:11:45	65,000
2016/01/28	10:45:16	115,000
2016/01/28	15:03:58	115,000
2016/01/28	18:21:42	115,000
2016/01/29	21:25:20	110,000
2016/01/29	02:34:40	115,000
2016/01/29	23:18:29	115,000

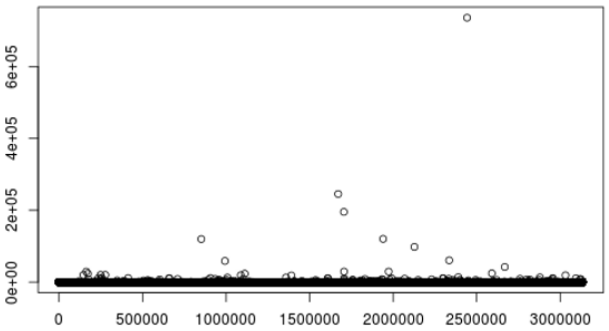

図 7: 2016 年 1 月 26 日 12:00-13:00 のログに対する外れ値検出 [1 つの○は 1 session を示す]

同様に、午後 6 時台のログに対する外れ値検出結果を以下に掲載する. 午前 10 時の物と比較して異常と予測される通信が多く観測されているのが見て取れる. 信州大学へ向けて発信されたパケットは 315 万件だった.2016 年 1 月 26 日 18:00-19:00 のログに対する外れ値検出の結果を示した図 8 より、図 7 に比べて異常度の高い通信が増加していることが見て取れる.

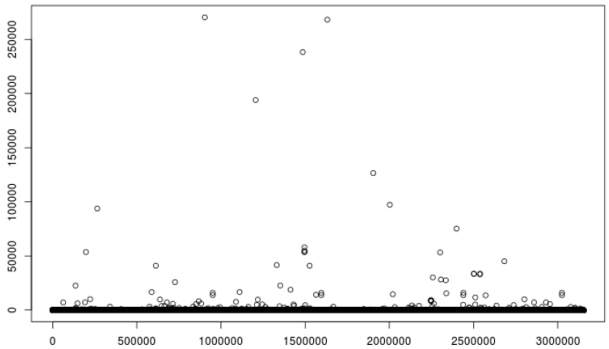

図 8: 2016 年 1 月 26 日 18:00-19:00 のログに対する外れ値検出 [1 つの○は 1 session を示す]

ただし、ペネトレーションテストには DoS 攻撃を使用している.DoS 攻撃は短期間に大量のパケットを送信す

るというものであるため、異常度の高い通信に固まった通信が見て取れなくてはいけない. そのため DoS 攻撃を検知できているとは言えない.

5.2. 非階層型クラスタリング

非階層型クラスタリングの結果を図 9 に掲載する. 使用したログデータは外れ値検出と同く 1 月 26 日 12:00〜13:00 のデータであり、313 万件のログから作成した.

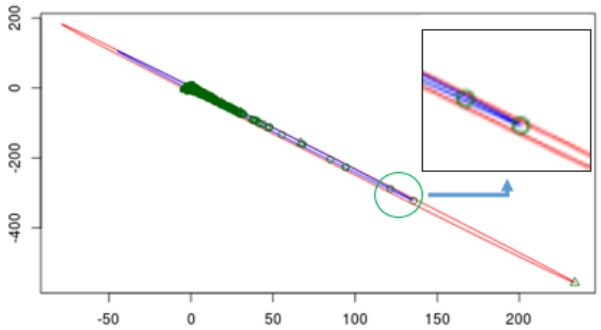

図 9: 2016 年 1 月 26 日 12:00-13:00 のログに対する非階層型クラスタリング [1 つの○は 1 session を示す]

外れ値検出同様に、18:00〜19:00 のログに対する非階層型クラスタリングも行った. 図 10 がそれである.

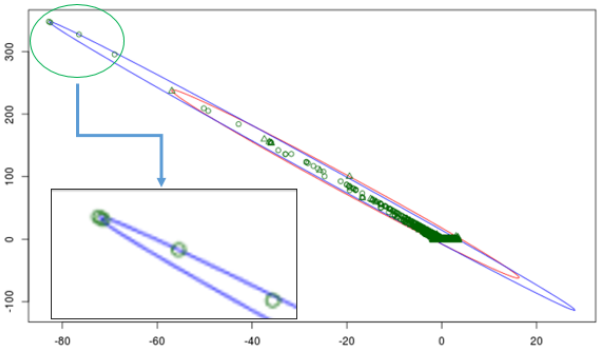

図 10: 2016 年 1 月 26 日 18:00-19:00 のログに対する非階層型クラスタリング [1 つの○は 1 session を示す]

比較してみると、原点付近が最も通信が集まり、原点から離れるほどに通常の通信から見ると異常だということがわかる.18 時台にはペネトレーションテストにより大量のパケットを送信しているが、攻撃パケットは恐らく原点から少しずれたあたりに集中していると考えられる.

5.3. 自己組織化マップ

自己組織化マップによるデータマイニング結果を図 11 に掲載する. こちらも同じく 1 月 26 日 12:00〜13:00、313 万件のログを使用した.

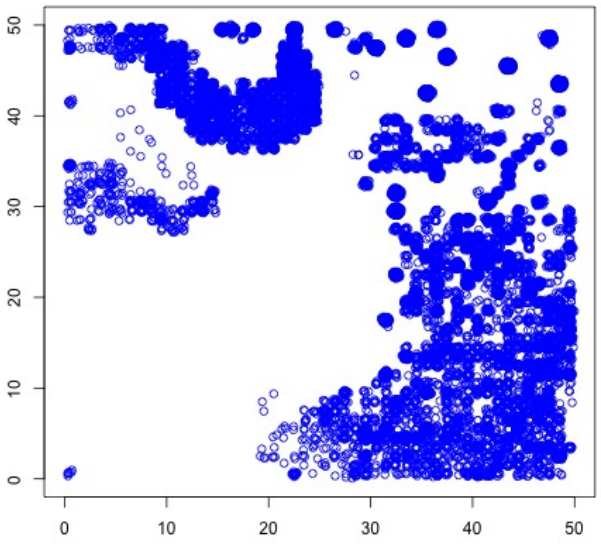

図 11: 2016 年 1 月 26 日 12:00-13:00 のログに対する自己組織化マップ [1 つの○は 1 session を示す]

前述した 2 方式に比べて、独特なマップを形成していることが分かる. 同様に 18 時台の解析結果についても以図 12 へ掲載する.

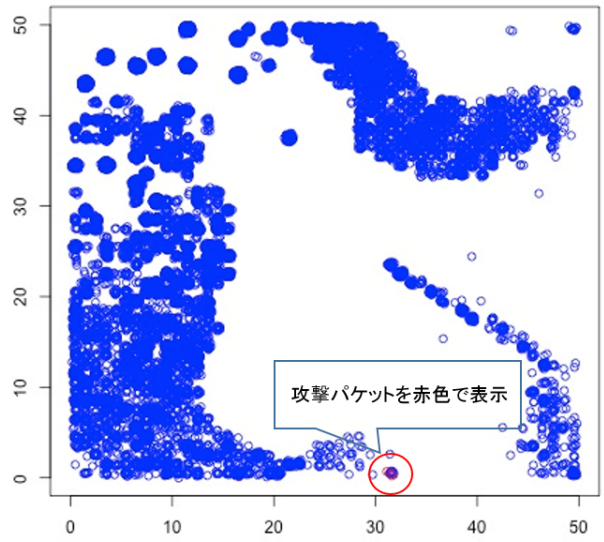

図 12: 2016 年 1 月 26 日 18:00-19:00 のログに対する自己組織化マップ [1 つの○は 1 session を示す]

図 12 では、攻撃に使用した通信をあらかじめ特定し、そのパケットを赤く表示した. そしてその周辺の通信に対して調査を行い、攻撃を特定することが可能かどうかを調査した. 通信の配置が多岐にわたり、調査対象を絞り込むことが困難だと判断されたためである.

6. データマイニング結果の評価

攻撃検知が行えているかを 3 種類のデータマイニング (外れ値検出, 非階層型クラスタリング, 自己組織化マップ) を用いて攻撃対象の検出を試みた. ペネトレーションテストを行ったのは午後 6 時台のため, 午後 6 時台のデータマイニングに絞って評価を行う.

外れ値検出
今回選定したセッションを基にしたパラメータを用いた解析では，本研究において用意した攻撃手法の検出はできなかった．

非階層型クラスタリング
今回選定したセッションを基にしたパラメータを用いた解析では，ある程度標準 (原点) から外れた通信が確認されたが，本研究において用意した攻撃手法の検出はできなかった．

自己組織化マップ
今回選定したセッションを基にしたパラメータを用いた解析では，本研究において用意した攻撃手法でのアクセスでクラスタが形成されており，ある程度の見込みを持って攻撃の検知ができる可能性を示せた．

7. まとめと今後の予定

今回は 2016 年 1 月に実施した試行的な攻撃を基にデータマイニングの基礎理論及び活用法について検証した．残念ながら，想定した 3 つの方法 (外れ値検出, 非階層型クラスタリング, 自己組織化マップ) の内，外れ値検出，非階層型クラスタリングでは有意な結果を得ることはできなかった. しかし，まだ多くの手法を試行する余地が残されているため，引き続き調査を行い，より精度の高い検出を高速に行うデータマイングについて研究していく予定である．

今後の予定としては次のようなテーマをもって研究を推進していく予定である．

- 様々なデータマイニングによる検証

  現在 3 種類の方法で検証しているが，サポートベクターマシンなど様々な方法での解析を実施し比較していく．また出力としてもデンドログラムを利用するなどしてクラスターがより明瞭になる手法も検証していく予定である．

- 様々なパラメータによる検証

  現在の解析対象は UTM の通信記録を基にしており，様々な情報が通信記録として記録されている．データマイニングするにあたり，現在は session と通信量についてのみ情報として利用しているが，application などより高度な情報をある程度取り入れる．ただし，本研究の最終的な目標として高速な処理を実現することを目標としているため，可能な限り高度なセキュリティ装置で無くても収集できる通信記録を基に解析したいと考えている．

- 攻撃方法の再現

  攻撃手法や攻撃の結果取得される標準的な情報の取得は困難であるため，攻撃に関する研究開発も併せて実施する．現在は DNS Flood 攻撃の再現を試みているが，http に関して [3] と同様な攻撃方法の再現し比較することにより，セキュリティの研究をより広めていく予定である．

8. 謝辞

本論文を作成するにあたって使用された UTM(統合脅威管理, Unified Threat Management) 装置による通信ログは, 信州大学情報総合センターの協力を得て取得致しました．

参考文献

[1] 湯原大二郎, 鈴木彦文, ”高度な攻撃を検出するためのセキュリティ装置におけるデータマイニング ”, 電子情報通信学会, 平成 27 年度信州大学学生ブランチ B-4(2015/12/14 信州大学)

[2] 豊田秀樹,2012 年 ”データマイニング入門 ”, 東京図書,” 東京図書株式会社”,http://www.tokyo-tosho.co.jp/（最終確認 2016 年 6 月 25 日）

[3] 林祐平, 西山聡史, 阪井勝彦, 鈴木昭徳, 工藤伊知郎, ” パケット連続到着時間を尺度とした攻撃検知法 ”, 電子情報通信学会総合大会講演論文集 2016 年 通信 (2), 27, 2016-03-01