Web ブラウザを用いたセキュリティセンサの共有ログ情報視覚化システム

金 子 博 一† 秀 島 裕 介†† 小 池 英 樹†

分散 IDS のログを比較する事で１つの IDS ログだけでは得られない情報を得る事ができる。しかし，実際にはログのフォーマットが共通でない等の問題があるため分散 IDS のログ比較は難しい。
本研究では分散 IDS のログ比較の一例として、The Honeynet Project に焦点を当て、複数拠点のログ情報の比較を行うことができる視覚化システムの提案及び実装を行った。これにより、攻撃の概要、詳細を直感的に把握でき、更に個々の拠点間の攻撃情報を視覚的に比較することが可能となった。

Web Browser System for Cyber Threat Monitoring Using Multiple Senssors

Hirokazu Kaneko,† Yusuke Hideshima†† and Hideki Koike†

It is important that comparing distributed IDS data for network security. But, in fact,Making Systems is difficult for log format, log trading and so on.
By comparing distributed IDS logs, it is possible to obtain useful information which could not be obtained from one IDS log. It is, however, difficult to do such analysis since the distributed IDS logs are often recorded in their own format. This paper described a web-based visualization system which can visualize multiple IDS logs in one geographical map by focusing on the logs shared by The Honeynet Project. The system enable us to understand an overview and details of attacks intuitively as well as to visually compare the attack information at different locations.

1. はじめに

インターネットが社会インフラとして重要な役割を占めるようになり、インターネットに接続された計算機を標的としたサイバー攻撃の問題が深刻になっている。例えばコンピュータワームやコンピュータウィルス、ボット等のサイバー攻撃が増加している。これらの攻撃によってメールシステムや Web サービスといったものを停止させることがあり、経済活動や公共に大きな影響を与えている。

これらのサイバー攻撃はログとして計算機に蓄積される。だが、こういった攻撃の解析には膨大なテキストデータを読む必要があり、とても一件一件を精査することはできない。そのため情報視覚化技術を用いて解析をしやすくすることが多い。

近年、インターネット上のこれらの攻撃を監視することにより、攻撃の早期発見や攻撃の予知に役立てる研究が行われている。そういった研究の一つとして、分散 IDS(不正侵入検知システム) の比較の研究が行われている。これは一つの IDS による検知ログではわからない攻撃も、多くの分散した IDS によるログ比較を行うといったことで統合的に攻撃を解析するものである。しかし、ログの比較にはお互いのフォーマットや、そもそもログの提供を望めない場合が多く、実現は難しい。

これに対し，攻撃情報を共有することを目的とした国際的プロジェクト，The Honeynet Project がある The Honeynet Project は、ネットワークを監視、解析を行う行うツールの一つである Honeypot を運用している大きな団体の一つであり、世界のセキュリティ調査員はこれを用いて監視、解析を行っている。The Honeynet Project ではログのフォーマットがほぼ共通であり、交換が行いやすいという特徴があり、上記の問題を解決できる。しかし、世界中にある拠点間で交流が少ないため、データのやりとりも少ない。

本研究では、分散 IDS のログの比較の一例として The Honeynet Project の個々の拠点でのデータ比較を行うことを目的とし、

そこでログ情報を共有していることを前提に、解析結果を地理的視覚化を用いてブラウザ上で表現する視覚化システムを考案、実装した。

† 電気通信大学大学院 情報システム学研究科
The University of Electro-Communications
†† ソネットエンタテインメント株式会社
So-net Entertaionment Corporation

2. 分 散 IDS

IDS は計算機における不正侵入と思われる攻撃をログに残すものであり、ネットワークセキュリティにおいて欠かせないものである。多くの場合セキュリティ研究者は IDS を用いてネットワーク上の攻撃を監視、解析することで世の中の攻撃を知り、それに対する対策を打ち出してく。しかし、一つの拠点の IDS ではその拠点に対する攻撃しかわからない。

そこで、一つの IDS ではわからない情報でも、複数の IDS を比較することで得られる情報というものがある。例えば、ある攻撃が広域的に行われているのか、それとも特定 IP に対して集中的に行われているのかといった情報は他の IDS のログと比較してはじめてわかることである。この場合、特定 IP に対する攻撃は広域的な攻撃よりも特徴的で危険な攻撃である可能性が高い。このような情報を得るため、複数の IDS のログを比較することは有用である。

3. The Honeynet Project

以前のネットワークセキュリティは、受け身的なものに過ぎなかった。ファイアーウォール、IDS や暗号化といった全てのメカニズムは、各自のリソースを守る為に受け身として用いられていた。そのため、問題が起きるまでは対処のしようがなく、常に攻撃者が主導権を握っている状況にあった。The Honeynet Project はこの状況を変えるために作られたものである。

The Honeynet Project の目標は、世に広まっている攻撃に対する情報を集めることである。例えば悪意ある攻撃用のツール、攻撃手法、攻撃動機といったものが挙げられる。情報を収集するツールとして主に Honeypot を用い、現在では世界 23 拠点で活動的に攻撃の監視、解析を行っている。

3.1 Honeypot

ネットワーク攻撃は日々進歩している。そのため、世の中にどのような攻撃が出回っているか知る事はネットワークセキュリティ的に有益である。

Honeypot は脆弱な PC を模擬することで攻撃者をおびきよせ、攻撃者の行動を逐一ログにとることで監視、解析を行うセキュリティセンサの一つである。Honeypot には以下の利点を挙げられる。

- 誤検知が少ない

  通常の計算機のログを見ると、正規のユーザーが行った行動、例えば Web アクセスによるファイルのダウンロードといったものも検知してしまい、ログに記録される。Honeypot は正規のユーザーを持たず、脆弱な PC を模擬するマシンを置くシステムなので、ログに残っている情報は攻撃、あるいは IP アドレスを間違えてアクセスしようとした人間となる。従って通常のログよりも誤検知を極端に減らす事ができる。
- 暗号化されていても活動できる

  ハニーポットはネットワークなどの途中の経路ではなく, 最終的な通信対象であるホストにおいて情報を捕足するため, ネットワークベースのファイアウォールや侵入検知システムでは対応できない SSL や IPsec といった様々な暗号化プロトコルを使用している環境や, 攻撃自体が暗号化されている状況であってもその活動を捕足することができる.
- 柔軟性

  また, ハニーポットは様々な環境に応じて柔軟にカスタマイズすることができ, 他のセキュリティアプリケーションと組み合わせて利用する事も可能である. ハニーポットはその柔軟性から, 例え組織内の犯行による情報漏洩などといった, 他のセキュリティ対策では対応不可能な問題にも適用する事ができる.

3.2 Honeynet における問題

Honeypot は日進月歩のネットワークセキュリティにおいて、攻撃者の攻撃動機を知る上で重要なツールである。しかし、各々の研究者が Honeypot を設置する台数は限られる。そのため監視、解析している Honeypot のログの絶対量が多いとは言えず、今後個々の研究者が世の攻撃の発展に追従する事ができなくなる可能性がある。また、The Honeynet Project 同士で互いに交流は浅いことが多く、情報を提供しあったり解析情報を公開するといった、協力して物事を進めることは少ない。

また、少数の研究者では解析しきれなくなり、重要な攻撃動機を見落としてしまう可能性がある。今日のネットワークセキュリティにおいて、攻撃側の技術も日進月歩に飛躍し続けている。そのため未知の全く新しい攻撃に対して少数の研究者では気づけない可能性があり、これによって攻撃に対する対策が遅れる要因となりうる。

そして、ネットワークセキュリティの研究は一般に困難だと言われている。大量のログデータを見る必要があり、明らかな攻撃であっても初心者には分かりづらい。そのため新しくネットワークセキュリティの研究を始めようとする考えが生まれづらいものとなって

おり、攻撃を助長させる一つの要素となっている。

4. システムの基本設計

4.1 ログ情報の共有

ログ情報の公開は個人情報にもなりうる。企業や個人でも IDS を運用している場合があるが、そのログを公開することはその企業や個人の IDS のデータを利用者に公開する必要があるため全世界の IDS のユーザを対象にすることは難しい。

そこで、The Honeynet Project 内部の Honeypot ユーザならば個々の情報を公開、共有して問題ないとすることができる。ログを共有することで、研究者同士が積極的に助け合い、The Honeynet Project における問題に対処できると考えられる。特に、日進月歩のネットワークセキュリティの攻撃に対し、新しい不審な攻撃や特徴的な攻撃の早期発見につながり、周囲の攻撃ログとの比較を簡単に行う事ができる。そのため世に広まっている攻撃情報を正しく扱え、各国の特徴的な攻撃や、全世界で流行している重要な問題に対しても積極的に情報が出回るようになると考えられる。

4.2 対象とするユーザ

本システムでは、The Honeynet Project の研究員を対象としている。

インターネット定点観測システムでは、複数のセンサの情報を統合し、統計解析を行う。そのためインターネット定点観測の結果が即座に本システムが対象としているユーザにとって有益な情報であるとは限らない。そのためユーザは警告ログの解析ツールを構築する必要が有る。しかし、これらの解析ツールの構築は煩雑で、適切な運用を行う為には定期的なメンテナンスも必要であるためユーザに負担を強いることになる。

また、Honeynet における問題として、各研究者が持っているログは運用できる Honeypot の数に制限があるため少ないと言える。

本研究ではこれらの問題を解決するため、ログ情報を共有していることを前提とした、ウェブアプリケーションとしてシステムを構築した。ウェブアプリケーションの利点については後述することにする。

4.3 ウェブアプリケーションでの実装

本システムはウェブアプリケーションとして実装した。ウェブアプリケーションには以下のような利点がある。

- 特別な環境を必要としない
  本システムは全世界の The Honeynet Project を対象としているため、特別な環境に依存しないものが好ましい。ウェブアプリケーションはウェブブラウザさえあればどこからでもアクセスが可能であるため、特殊な装置や環境を必要としない。ユーザはプラットフォームの違いもマシンの違いも意識することなく、統一的な動作でアプリケーションを利用することが可能である。
- メンテナンスフリー
  ウェブアプリケーションはユーザにとってメンテナンスフリーで利用できる。システムはサービスを提供するサーバに構築されているため、システムのアップデートがあたとしても、サービスを提要する側だけの作業となる。そのためユーザは普段通りウェブブラウザからシステムにアクセスするだけでよく、特に特別な操作を必要としない。

5. システムの実装

本研究では分散 IDS のログ比較の一例として、The Honeynet Project を対象としたサイバー攻撃の地理的視覚化システムの提案及び実装を行った。

5.1 システム概要

本システムはサイバー攻撃の地理的視覚化システムである。これは The Honeynet Project の研究員を対象として作成した。また、ウェブアプリケーションとして実装している。

ユーザは事前に Honeypot に、本システムを利用するためログの転送システムを設置する必要が有る。その後ウェブウラウザを用いて本システムにアクセスし、解析情報にフィルタリングをかけることによって地図上に適切な解析情報を出力する。

これによりユーザは特別な環境を必要とせずウェブブラウザさえあれば手軽に解析情報を知る事ができ、また他の拠点の The Honeynet Project のデータを参照することで攻撃の特徴をとることが可能になる。

5.2 システム構成

(1) Honeypot のデータをサーバに転送する
  Honeypot にある不正検知システムのログデータを自動で送信する。今回、高対話型 Honeypot の IDS のログデータの内、Snort と Iptables を用いている。

(2) データを格納する
  MySQL を用いて送られてきたデータを格納する。

(3) ブラウザを用いて HP にアクセスする
  特定のマシン、特定の環境、特別な設置が必要なものを避けるべく、大部分のマシンで動くブラウザで実装。

(4) 解析データを視覚化する

PHP で MySQL を用いて格納したデータを参照し、そのデータから重要拠点のデータを読み込む。読み込んだデータを GeoIP を用いて緯度経度に変換し、その情報を元に GoogleMaps を用いて地図上に描画する。このとき、どのデータを参照するかといったフィルタリングができるようにした。

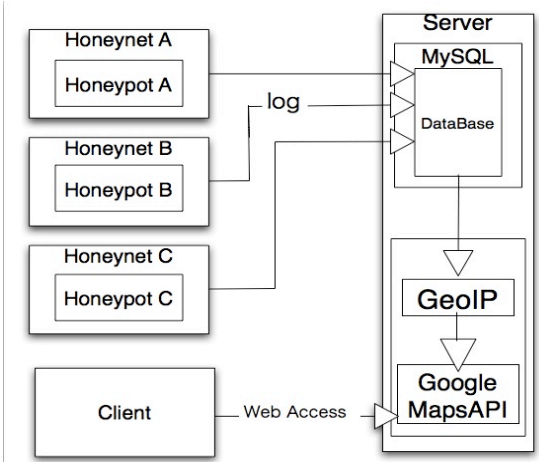

図 1 システム構成図

今回は 3,4 部分について実装、考察を行った。

5.3 描　　画

本システムの利用者は世界各国にある The Honeynet Project に所属している人々である。そのため機種依存が激しいものや、特別な設置方法が必要なものは避けるべきである。そこでブラウザを用いて Web ベースの視覚化を行うことにする。

- 地図表示部

  操作部で指定した解析情報を基に、GeoIP を用いて攻撃元または攻撃先の IP から GeoIP を用いて地理情報に変換し、GoogleMapsAPI を用いて地図上にマーカーを描画している。　今回、マーカーは 3 台の Honeypot1,2,3 をそれぞれ赤、緑、青で色分けし、複数台の Honeypot にとっての重要拠点の場合その複合色で表現している。また、そのマーカーをクリックすることで更に詳細な情報を得ることができ、現在は攻撃があった時間、攻撃の種類、拠点の IP アドレスを一件毎に表示させている。また、複数の Honeypot への攻撃をしている拠点の場合、拠点毎にタグが設けられており、それを選択することでそれぞれの Honeypot のログを見る事ができる。

- 操作部

  検知の種類、攻撃の向き、Honeypot の指定を行い、このデータを地図表示部で反映させる。検知の種類は現在「Snort」,「Iptables」の二種類選択可能になっている。攻撃の向きは外部から内部への「INBOUND」と内部から外部への「OUTBOUND」の二種類、Honeypot の指定はそれぞれ赤、緑、青に対応させた Honeypot1,2,3 が割り振られている。Honeypot は複数選択可能になっており、特定の拠点の情報のみの表示が可能になっている。

5.4 システム動作例

動作例では一日分のデータを対象とし、日本を拠点とした高対話型 Honeypot3 台のトラフィックを監視していた HoneyWall のデータの内、不正侵入検知システムの一つ「Snort」のデータを用いている。このとき、Honeypot1,2 は実際に攻撃を受けて侵入されたことのある Honeypot で、Honeypot3 はポートスキャン程度しか受けていなかった。また、Honeypot1,2 は共に外部へのポートスキャンを実行するプログラムを実行されていた。

システム動作例 1 図では、Honeypot1,2,3 のデータを外部から内部への接続に対するデータを表示させている。Honeypot1 と 3 はほぼ同様の場所から攻撃があることに対し、Honeypot2 への攻撃はほぼ独立した場所からの攻撃だった。また、日本からのあるポイントのみ Honeypot1,2,3 への攻撃があった。このことからそのポイントは広域的に攻撃が行われていることがわかる。また、Honeypot2 に対する攻撃は 1,3 と比較して特徴的な攻撃であることがわかった。

システム動作例 2 図では Honeypot1,2,3 の Honeypot 内部から外部への接続を見ている。これを見ると、緑一色に染まっていることがわかり、Honeypot2 のデータであることがわかる。そのほとんどは左程問題のないものであるが、赤と青は全く描画されていない。

同様に外部へのポートスキャンが実行されていた Honeypot1 は実は外部への接続がなかった。このポートスキャンは第一、第二オクテットを指定してその範囲でスキャンをかけるものらしく、Honeypot1 はスキャンし終わっていたのかもしれない。以上から日本拠点の 3 つの Honeypot だけでも特徴がとれることがわかり、そのうち Honeypot2 は特徴的だといえる。

また、全体的に中国、アメリカ、日本からの攻撃は多いが、欧米や南米からの攻撃は少ない。この結果は日本ならではの結果ではないかと推測される。

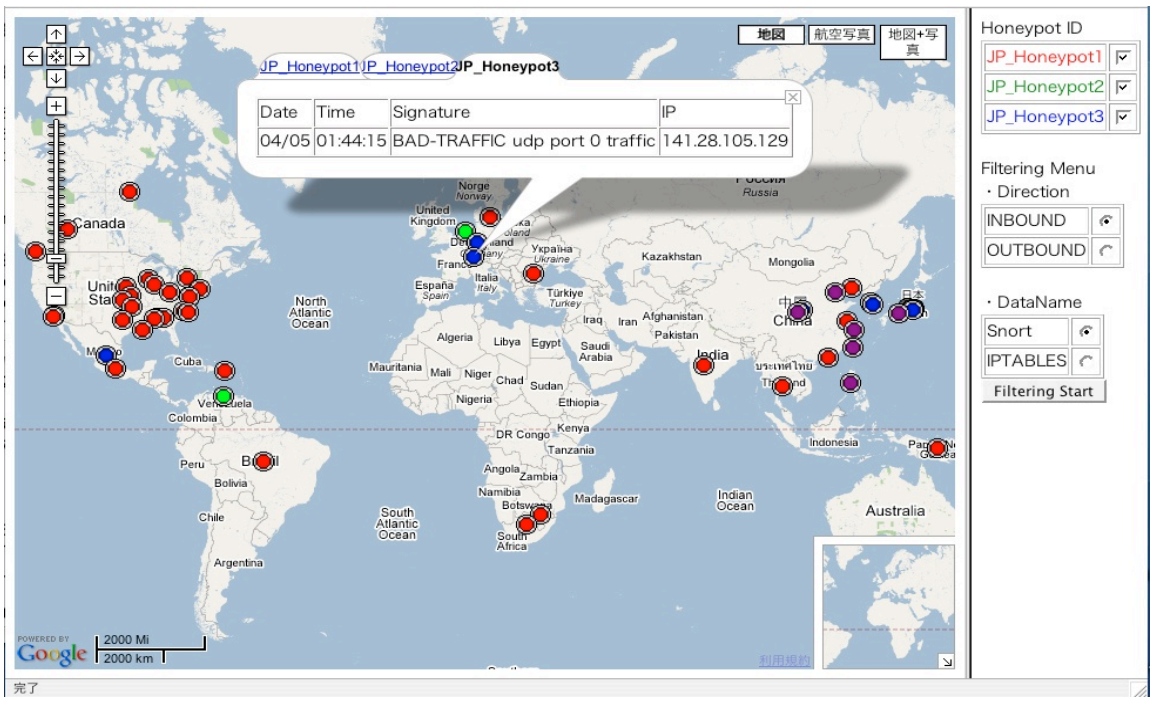

図 2　システム動作例 1

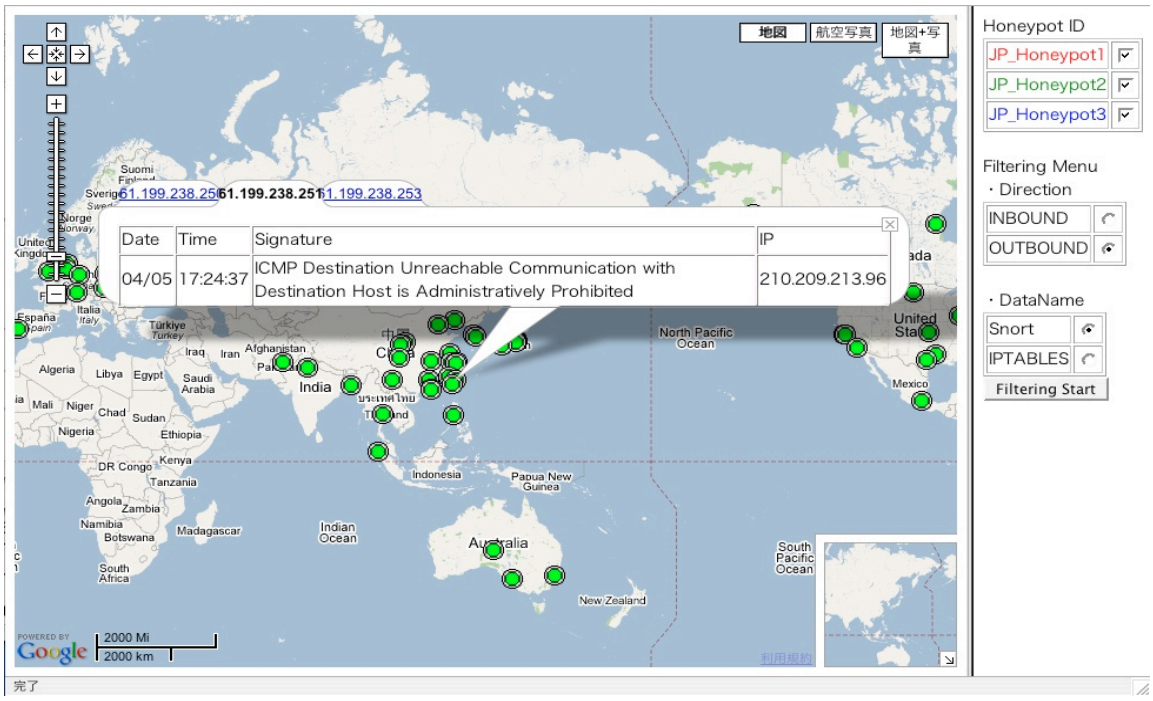

図 3　システム動作例 2

6. 考　　察

各 Honeypot のデータを簡単に比較でき、個々の特徴がとらえやすくなった。特別な装置を必要とせず、解析情報を即座に見る事ができた。また、解析情報のフィルタリングといった機能を複雑な説明もなしにできるようになった。

7. 今後の課題

本システムの課題として、以下の事項が挙げられる。

- ログの共有

  本システムで提言している IDS のログの共有において、自動で解析ログをサーバーに格納するシステムが必要だと考えられる。現在のシステムは直接解析データから読み取っているため、サーバーに解析データを読み込ませさえすればそれを反映することができる。

- 時間軸

  インターネット広域監視システムにおいて、早期に発見し対策をとることが重要である。また、目的の攻撃に対して何度かステップを踏む場合がある。そのためリアルタイムであることといった時間的な要因は重要であると言える。そこで、警告ログがいつ行われたかを視覚的にわかりやすくする必要がある。

- 攻撃量

  一般にネットワークセキュリティにおいて、特定拠点からの攻撃量が大きい程、DoS といった攻撃が行われている可能性がある。そのため攻撃量が一目でわかるような視覚化を施す事は重要なことと言える。本システムではまだ攻撃量の大小に関する視覚化は行われておらず、攻撃があったか否かでしか攻撃ポイントを表現していない。この点において改良が必要だと考えられる。

8. ま と め

本研究では分散ログを比較するためのログ情報共有視覚化システムの提案を行い、その一例として The Honeynet Project のログ共有視覚化システムの視覚化部分の実装を行った。また日本拠点で集められたデータを基に、視覚化システムの効果を示した。今後はログの共有部分を実装、システムの改良を進めシステムの完成を目指す。

参 考 文 献

1) 秀島裕介、小池英樹、「サイバー攻撃の論理的及び地理的視覚化に関する研究」、平成 18 年度電気通信大学大学院修士論文
2) The Honeynet Project, http://www.honeynet.org/index.html
3) Snort, The Open Source Network Intrusion Detection System, http://www.snort.org/
4) DShield, http://www.dshield.org/
5) Christopher P. Lee 、John A. Copeland、FlowTag: A collaborative attack-analysis, reporting, and sharing tool for security researchers