3-5　ダークネット観測網の災害時応用技術

鈴木未央

大規模な災害時においては、停電やネットワーク機器、光ファイバ等の物理的損傷により、インターネットの機能不全が発生する。本稿では、このような災害時における、ネットワークセキュリティ技術の活用方法の１つとして、大規模ダークネット観測網によるインターネットの死活状況の推定について検討する。

1　はじめに

2011 年 3 月 11 日に発生した東日本大震災以来、あらゆる分野において災害への備えを行うという意識が高まってきている。著者らはこれまでサイバーセキュリティ分野において長年ダークネット観測を行ってきた [1]–[3] が、その観測結果を災害時や災害後の復興に生かすべく、現在、ダークネット観測を用いた災害時のネットワーク死活状況を推定する死活監視の検討に取り組んでいる。

大規模な災害時においては、停電、ネットワーク機器や光ファイバ等の物理的損傷により、インターネットの機能不全が発生する。これらの機能不全を正確に俯瞰して把握することは、復興のために有意義であると考えられる。しかし、インターネットは自律分散方式のネットワークであるため、それらの機能不全の情報は一般的には発生した組織内部で閉じ、外部から組織横断的に知ることは難しい。

著者の研究室では大規模ダークネット観測網を活用したインシデント分析センター NICTER（Network Incident analysis Center for Tactical Emergency Response）の実験運用を定常的に続けている。本稿ではその運用で得られる情報を、他の一般公開されている情報と組み合わせることで、インターネットの死活監視を行える可能性 [4][5] について検討する。また、その死活監視を県単位、市単位、AS 単位において組織横断的に、ネットワークに負荷を与えないパッシブモニタリングにより迅速に行える可能性についても検討し、続いて監視を自動化するシステムの設計と実装について述べる。

2　ダークネット観測

ダークネットとは、インターネット上で到達可能かつ未使用の IP アドレス空間のことを指す。未使用の IP アドレスに対しパケットが送信されることは、通常のインターネット利用の範囲においては起こる可能性が低いが、実際には相当数のパケットがダークネットに到着している。これらのパケットの多くは、リモート感染型のマルウェアが送信するスキャンやエクスプロイトコード、送信元 IP アドレスを詐称した SYN フラッド攻撃に対する応答であるバックスキャッタ等、インターネット上での不正な活動に起因している。そのため、ダークネットに到着するパケットを観測することで、インターネット上で発生している不正な活動の傾向把握が可能になる。ダークネット観測の最大の利点は、トラフィックを正・不正で区別する必要がなく、大半のパケットを不正なものと見なすことができる点にある。

ダークネット観測を行う場合、センサと呼ばれるパケット収集・応答用のサーバマシンを観測対象のネットワーク内に設置する。センサは、パケットの送信元に対する応答の程度によって様々に分類される。それらの分類のうち、代表的なセンサの１つがブラックホールセンサである。

ブラックホールセンサはパケットの送信元に対し、全く応答を行わないセンサである。このセンサはメンテナンスが容易であり大規模なダークネット観測に向いている。また、無応答であるため、外部からセンサの存在を検知することが困難であるという利点もある。ただし、マルウェアの感染活動の初期段階であるスキャンは観測可能であるが、それ以降の挙動を観測することはできない。

著者の研究室で研究開発を進めている NICTER では、日本国内外に点在する複数のダークネット（合計 30 万アドレス以上）にブラックホールセンサを設置し、定常的な観測を行っている [1]–[3]。

3　大規模ダークネット観測網を用いた送信元アドレス地理情報に基づくネットワーク死活監視

本節では、前述のダークネット観測の技術と送信元アドレス地理情報を組み合わせることにより、災害時の死活監視の可能性について検討していく。

3.1　基本アイデア

大規模なダークネット観測網には、世界各国から常時膨大な量の（前述のとおり、その多くは不正な）パケットが到来する。その中には、当然、日本国内のホストからダークネットに向けて送信されるものも存在する。ダークネットへパケットを送信してきたホストは、それが不正なものであれ、インターネット上で活動状態にあることが確認できる。そこで、大規模災害の発災前後において、ダークネットで観測されたホスト群と物理的な地理情報とをマッピングすることで、被災地周辺のインターネットの死活状況の推定を行える可能性がある。換言すると、ダークネットへの不正なトラフィックを逆手に取り、ネットワークに負荷を与えないパッシブモニタリングによってインターネットの死活監視を実現するという着想である。以下ではこの基本アイデアについて、東日本大震災時の実データを用いた検証を行う。

3.2　東日本大震災時における東北 6 県のユニークホスト数

本節では、2011 年 3 月 11 日の東日本大震災の前後において、ダークネット観測から得られる東北 6 県のユニークホスト数の変動を集計した結果を示す。集計の元となるデータとして、2011 年 3 月 1 日から 31 日までの 1 か月間に、NICTER の保有するクラス B のダークネット（IPv4 アドレス数約 65,000）に届いたパケットを使用した。また、送信元 IP アドレスから地理情報へのマッピングには、MaxMind 社の GeoIP City Database（2011 年 4 月版）を使用した。

図 1 に、東北 6 県からダークネットにパケットを送信した 1 日あたりのユニークホスト数を示す。ここからのグラフは特に断りがない限り、縦軸に単位時間あたりに観測されたユニークホスト数、横軸に日時、図中の縦赤線が発災の日時となる。グラフから、発災以後ユニークホスト数に明らかな減少傾向が見られ、その後、穏やかに回復していく傾向が見て取れた。

次に、県単位に絞った場合について見ると、東北 6 県のうち、青森以外の各県は発災後、ユニークホスト数に明らかな減少傾向が観測されていた。ここでは一例として、図 2 に、宮城県に絞った 1 日あたりのユニー

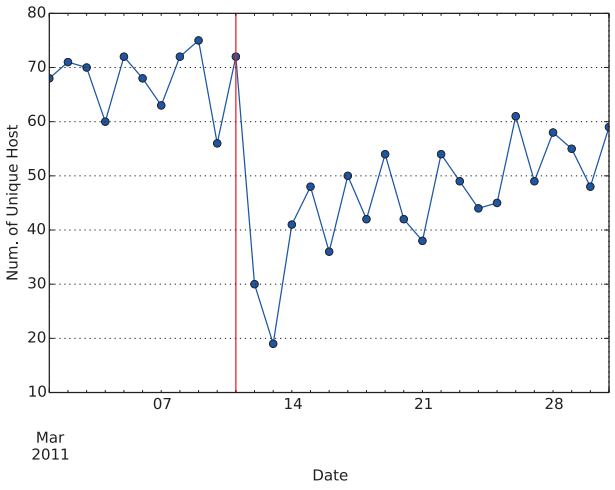

図 1　東北 6 県の 1 日あたりのユニークホスト数

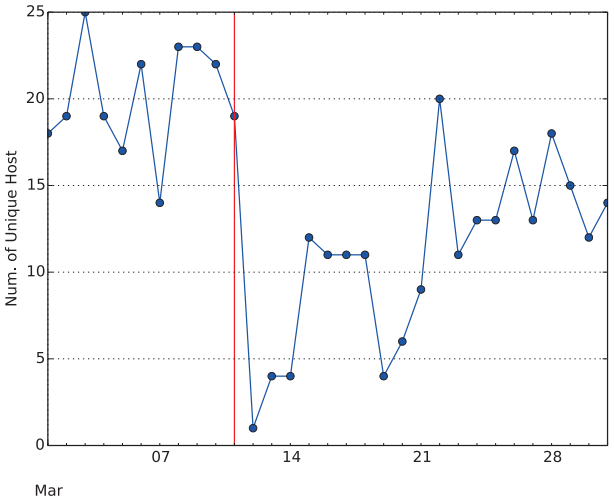

図 2　宮城県の 1 日あたりのユニークホスト数

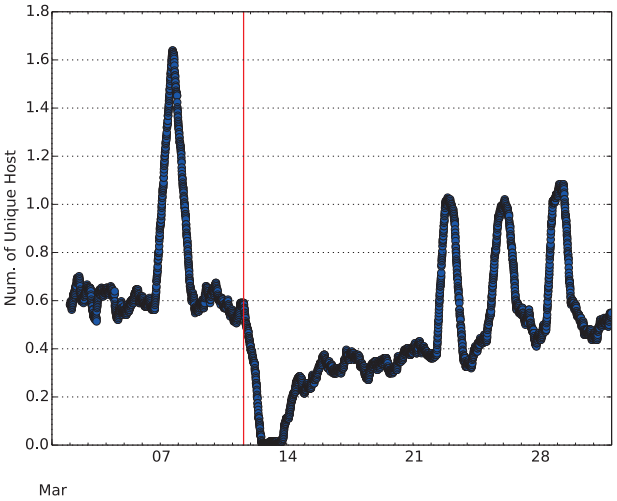

図 3　宮城県の 10 分あたりのユニークホスト数（144 区間移動平均）

クホスト数を示す。この場合でも、おおむね東北 6 県の場合と同様の傾向が見て取れた。

ここまでは、1 日単位のダークネット観測結果を用いてきたが、迅速なインターネットの死活監視を行うためには、ユニークホスト数の集計間隔を短縮することが望ましい。そこで、ユニークホスト数の集計間隔を 10 分に短縮し、単純移動平均（144 区間）を適用したものを図 3 に示す。このグラフからも発災直後のユニークホスト数の減少とその後の回復を確認することができた。

すなわち、ダークネットにパケットを送信してくるユニークホスト数を計測することで、県単位のインターネットの死活状況を、10 分程度で迅速に推定できる可能性があることを示せた。

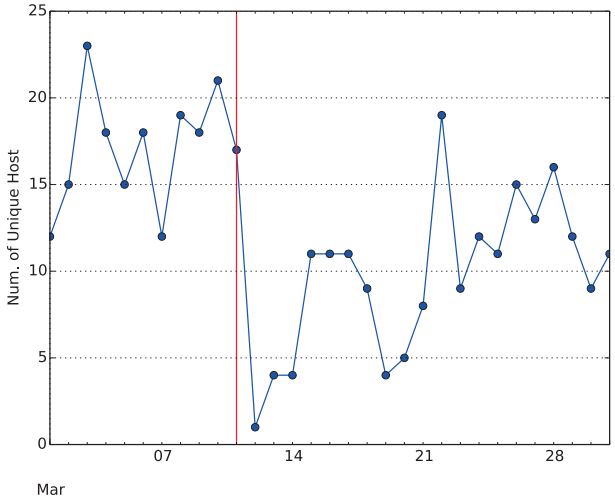

図 4　宮城県仙台市の 1 日あたりのユニークホスト数

3.3　東日本大震災時における市単位のユニークホスト数

著者の研究室ではこれまで、ダークネット観測におけるユニークホスト数について、県単位までの集計を行ってきたが、本稿では GeoIP City Database の市単位のデータとの突き合わせを行い、その結果を集計してグラフ描画を行った。

まず、過去の NICTER の知見から、観測されるユニークホスト数は人口にある程度の相関があるため、東北 6 県の最大人口を持つ市である宮城県仙台市に着目する。参考までに仙台市の 2014 年 12 月現在での推計人口は 1,074,125 人である。図 4 に、仙台市からダークネットにパケットを送信した 1 日あたりのユニークホスト数を示す。また、図 5 に 1 時間あたりのユニークホスト数を 24 区間移動平均で描画したものを、図 6 に 10 分あたりのユニークホスト数を 144 区間移動平均で描画したものを示す。

すべて、図中の縦赤線が発災の日時となる。

グラフの傾向としては、前節で示した県単位のグラフと同様の傾向を示している。

ただし、1 時間あたりと 10 分あたりのユニークホスト数のグラフにおいては、単位時間あたりに観測されているユニークホスト数が最大 2.8 や 1.6 と少なく、偶発的な複数のユニークホストの増減により、容易に傾向が変化してしまうことが予想される。実際に、ほかの複数の市についてグラフを確認したところ、最大ユニークホスト数が少ないグラフにおいては、傾向が読み取れない場合が多数であった。

これらの結果から、市単位の集計においても、ある程度の数のユニークホストが存在する場合は、インターネットの死活状況を 10 分程度で迅速に推定できる可能性があると言える。

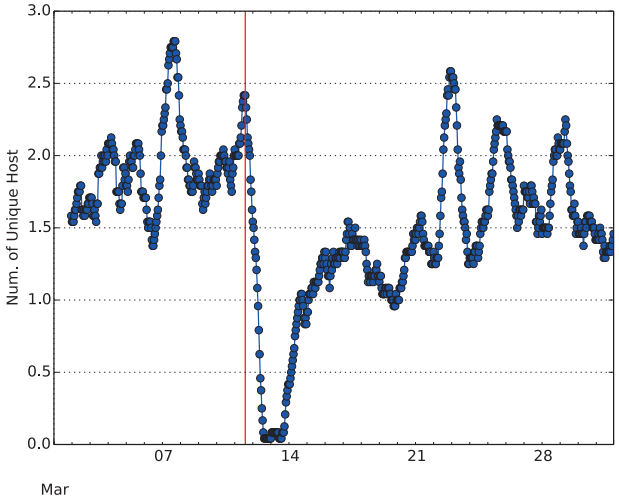

図 5　宮城県仙台市の 1 時間あたりのユニークホスト数（24 区間移動平均）

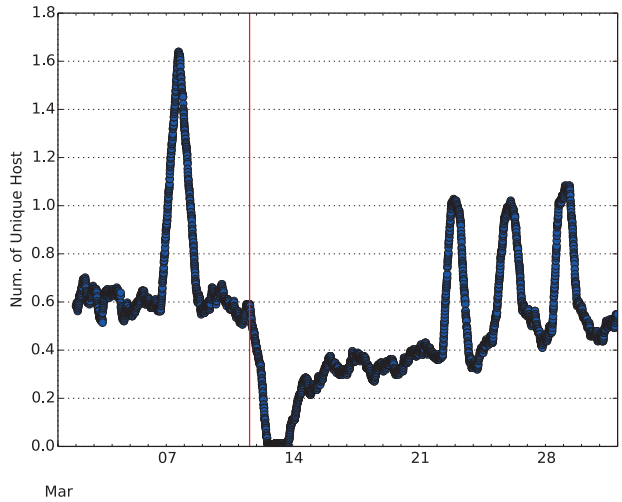

図 6　宮城県仙台市の 10 分あたりのユニークホスト数（144 区間移動平均）

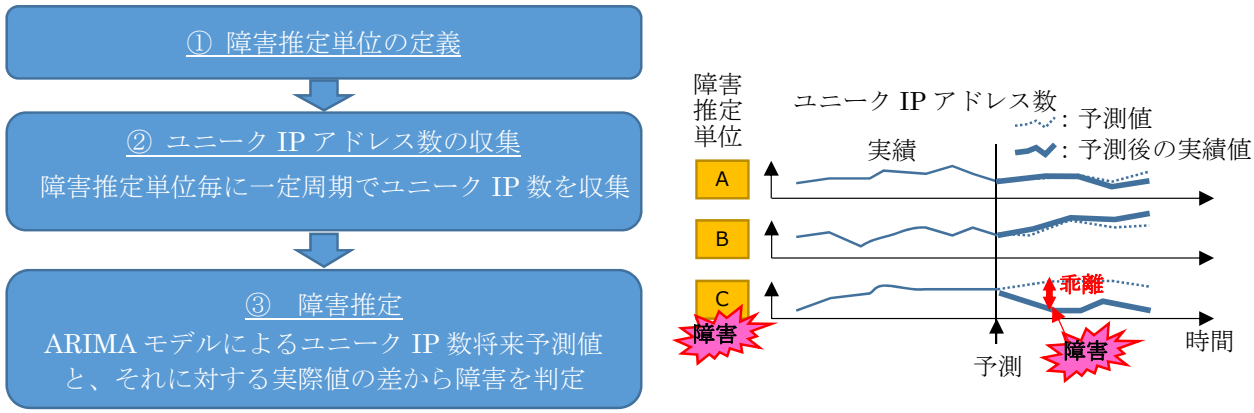

図 7　死活監視システムでのネットワーク障害推定の流れ

4　死活監視システムの設計と実装

3 で検討した可能性を元に、死活監視を自動化するため、システムの設計と実装を行った。図 7 に死活監視システムでのネットワーク障害推定の流れを示す。

死活監視システムでのネットワーク障害推定の流れとしては、まず集計の単位となる障害推定単位を定義し、システムに設定した後、その障害推定単位について決められた集計周期ごとにユニークな IP アドレス数を観測する。その集計周期ごとのユニーク IP アドレス数について、時系列解析手法を用いて未来の値の予測を行う。その状態で観測を続け、予測値と実際の観測地のずれを検出して、障害を推定する。この障害推定の流れで重要となる、障害推定単位、ユニーク IP アドレス数の収集、障害推定の方法について **4.1** 以降で述べる。

4.1　障害推定の単位

障害推定の単位は、**2** で述べた地域以外に、AS、IP ネットワークアドレス、ドメイン名などが考えられる。これらの単位は GeoIP City Database といった付加的な情報を用いることで、最終的にはアドレス範囲に変換可能である。また、アドレス範囲はグループ化が行えるような形とする。例えば北米というグループには、アメリカ、カナダ、メキシコなどの国が含まれ、それぞれの国が複数のアドレス範囲を持つという構造とする。このグループを障害推定の単位としてシステムに登録され、単位ごとに観測・収集が行われる。

4.2　ユニーク IP アドレス数の観測・収集

死活監視システムでは、登録した障害推定単位について、設定される単位時間ごとに、ユニークな IP アドレス数を観測し、記録する。単位時間は **3** で述べた検討結果を基に、10 分間ごと、1 時間ごと、1 日ごととする。

4.3　障害推定の方法

4.2 で観測・収集した単位時間ごとの時系列のユニーク IP アドレス数について、ARIMA（Auto Regressive Integrated Moving Average）モデルでモデル推定を行い、そのモデルを基に未来の値の予測を行う。また、本モデルの更新は定期的に行う。その状態で観測を続け、予測値と実際の観測地のずれを検出して、障害を推定する。

ARIMA モデルは、時系列解析手法の 1 つであり、過去のデータから未来を予測するものである。ARIMA モデルは AR モデル（Auto Regressive、自己回帰モデル）と MA モデル（Moving Average、移動平均モデル）をデータの差分に対して適応したモデルである。この ARIMA モデルを 10 分間ごと、1 時間ごと、1 日ごとの短期の予測に用いる。なお、予測に用いる変数は過去の 1 変量データのみである。

また、障害推定のために閾値を狭信頼区間上下限、広信頼区間上下限の 4 段階設定する。各信頼区間は、その区間に入る確率で定義する。その状態で、ユニーク IP アドレス数の観測値が、広信頼区間の下限以下となったとき、障害と推定する。

5　おわりに

本稿では、著者の研究室が定常的に実験運用を続けている NICTER システムの大規模ダークネット観測網を活用し、ほかの情報と組み合わせることで、県単位、市単位、AS 単位のインターネットの死活監視を、組織横断的に、ネットワークに負荷を与えないパッシブモニタリングにより迅速に推定できる可能性について述べ、続いて監視を自動化するシステムの設計と実装について述べた。検討の結果、ある障害推定単位について観測されるユニーク IP アドレス数が十分であれば、障害推定が可能であると言える。

今後は、システムの運用により問題点の発見と改善

を行いつつ、実際の災害時に役立つシステムに作り上げていきたいと考えている。

【参考文献】

1 K. Nakao, K. Yoshioka, D. Inoue, and M. Eto,“A Novel Concept of Network Incident Analysis based on Multi- layer Observations of Malware Activities,” The 2nd Joint Workshop on Information Security (JWIS07), pp.267–279, 2007.

2 D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J.Nakazato, K. Ohtaka, and K. Nakao,“nicter: An Incident Analysis System toward Binding Network Monitoring with Malware Analysis,” WOMBATWorkshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp.58–66, 2008.

3 K. Nakao, D. Inoue, M. Eto, and K. Yoshioka, “Practical Correlation Analysis between Scan and Malware Profiles against Zero- Day Attacks based on Darknet Monitoring,” IEICE Trans. Information and Systems, vol.E92-D, no.5, pp.787–798, 2009.

4 井上大介，中里純二，島村隼平，衛藤将史，中尾康二，”災害時における大規模ダークネット観測網の活用に関する検討，”情報通信システムセキュリティ研究会 (ICSS2011)，2011 年 3 月.

5 鈴木未央，島村隼平，中里純二，井上大介，衛藤将史，中尾康二，”大規模ダークネットを用いた送信元アドレス地理情報および AS 情報に基づく災害時ネットワーク死活監視，”情報通信システムセキュリティ研究会 (ICSS2015)，2015 年 2 月.

鈴木未央　（すずき　みお）

サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究員
博士 (工学)
ネットワークセキュリティ、ネットワーク運用