ABLA：エージェント・P2P ネットワークを利用した個人ユーザ参加型インターネット観測システムの開発

-利用者の環境に合わせたインターネット観測情報の提供-

1 背景

近年，ネットワークや計算機の多くが，マルウェアと呼ばれるプログラムによる脅威にさらされている．マルウェアとは，ワームやウィルス等の不正プログラムの総称であり，特に OS やソフトウェアの脆弱性を利用し感染活動を行い，被害を拡大させていくものが増加している．

これらマルウェアによる攻撃やトラフィック増加を早期に発見し，被害の拡大を未然に防ぐための試みとして，インターネット上で発生している攻撃の動向やトラフィックの発生状況観測をリアルタイムで行うことを目的とした，インターネット観測システムの運用が行われており，国内においては JPCERT/CC の ISDAS[1] や警察庁の@Police[2] がある．

これらの観測システムは，多数の固定された観測点を運用しており，観測点において受信したパケットのログや侵入検知システムのアラート情報を収集し解析を行い，定期的に観測結果や動向情報を提供している．

既存のインターネット観測システムの問題点

このようなインターネット定点観測システムには次のような問題点がある．

1. 観測システムの設置者によって観測結果の解析が行われた後の情報しか利用できない

利用者のネットワークや計算機環境に合致した独自の対策を行うために，利用者が観測システムによって収集された情報に対し別の角度から解析を行うことはできない．

2. 対策を実施する際に参照する観測システムの観測情報がその時点では既に古い

観測情報の更新を既存の観測システムに対し要求する事が実質的に困難なためである．結果として，利用者は適切なセキュリティ対策を行えない可能性がある．

3. 観測結果を観測システムに提供することは困難

利用者は独自の観測点として観測システムの観測点を補完できる可能性があるが，既存の観測システムにおいては，事実上，特定の利用者は観測システムに協力することができない．

2 目的

本プロジェクトでは，既存のインターネット観測システムが持つ問題の解決方法として，P2P ネットワークとモバイルエージェントを利用した新しいインターネット観測システム ABLA(Agent Based Log Analyzing System) を提案し開発を行った．

[1] JPCERT/CC，Internet Scan Data Acquisition System (ISDAS)，http://www.jpcert.or.jp/isdas/

[2] 警察庁 @Police，インターネット定点観測，
http://www.cyberpolice.go.jp/detect/observation.html

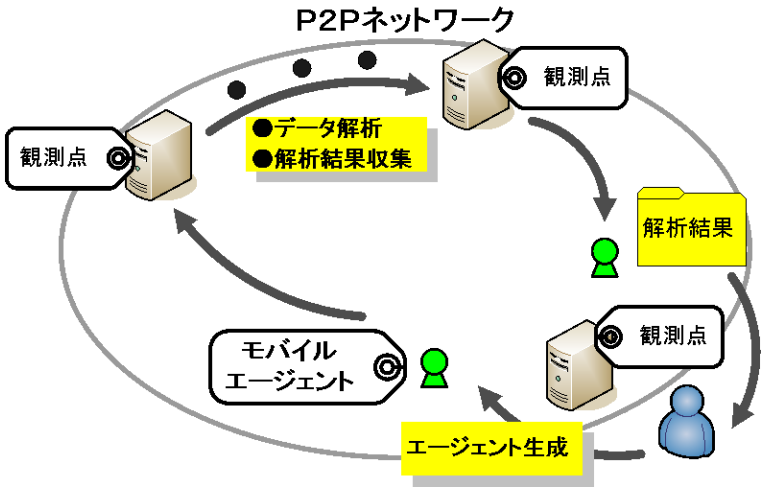

図 1: ABLA 概要

ABLA は複数の観測点 より P2P ネットワークを構築し，観測点において収集したネットワーク上のパケットやシステムのログを，モバイルエージェントにより解析，収集するインターネット観測システムであり，

1. 個人ユーザを含む，一般的なインターネット利用者がインターネット上の攻撃動向を把握し，恒久的なセキュリティの確保・維持を行うための利便性の向上
2. 多数の観測点を確保し，かつ悪意あるプログラムによる観測点のスキャンに対応するために観測点の固定的な設置から解放し，観測範囲を既存の観測システムよりも拡大させることによる観測精度の向上

を目的としている．

3 開発の内容

ABLA の概要

ABLA の概要を図 1 に示す．ABLA は複数の観測点より P2P ネットワークを構築し，観測点において収集したネットワーク上のパケットやシステムのログを，モバイルエージェントにより解析，収集する．

ABLA の動作環境

ABLA(Agent Based Log Analyzing System) の動作環境として，Linux，FreeBSD などの PC-UNIX を想定している．ABLA はオープンソースとして公開しており，起動におい

て必要となるライブラリやインストール方法の詳細は ABLA のウェブサイト[3] に記載している．

ABLA の実装概要

本プロジェクトでは，以下の項目を中心に開発を進めた．

1. ユーザインタフェース作成
   CUI，GUI の二つのユーザインタフェースを備え，ログデータの管理や設定，観測結果の可視化など ABLA の操作における優れたユーザビリティの実現．ABLA の GUI を図 2 に，得られる観測結果の例を図 3 に示す．

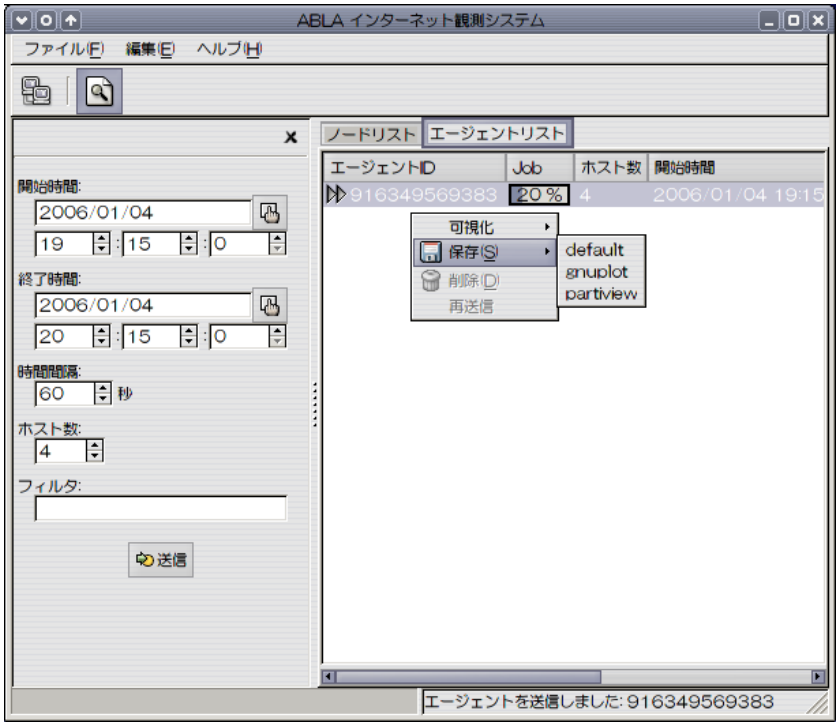

図 2: ABLA のユーザインタフェース (GUI)

[3] http://abla.sourceforge.jp/

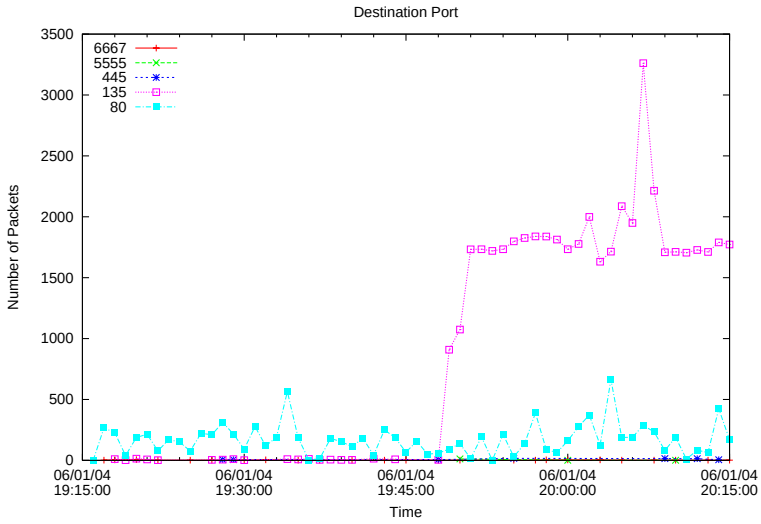

図 3: ABLA により得られる観測結果の例

2. エージェントの移動アルゴリズムの作成
   ABLA により構築された P2P ネットワーク上を効率的に移動することを考慮した，優れた移動アルゴリズムの考案と実装.

3. Peer-to-Peer(P2P) ネットワーク 部分の作成
   多数の計算機を繋ぐ観測システムおいての基盤とするため，独自の改良を加え耐故障性，冗長性に優れたネットワークの実現として，分散ハッシュテーブルを用いた P2P ネットワーク構築アルゴリズム Chord[4] を参考に実装を行った．Chord を利用して構築した P2P ネットワークの可視化例を図 4 に示す.

4 従来の技術 (または機能) との相違

モバイルエージェントと P2P ネットワークを利用したインターネット観測システム ABLA (Agent Based Log Analyzing System) により，既存のインターネット観測システムが持つ，

1. 利用者は観測情報を自身の環境に合わせた解析を行えない
2. 利用者から更新要求を発行できない
3. 利用者がインターネットを観測した観測結果を観測システムに提供

といった問題点を解決することが可能である.

[4] Ion Stoica., Robert Morris., David Karger., M. Frans Kaashoek., Hari Balakrishnan.: Chord: A Scalable Peer-to-Peer Lookup Service for Internet, Proceedings of the 2001 ACM SIGCOMM Conference, pp.149–160, 2001.

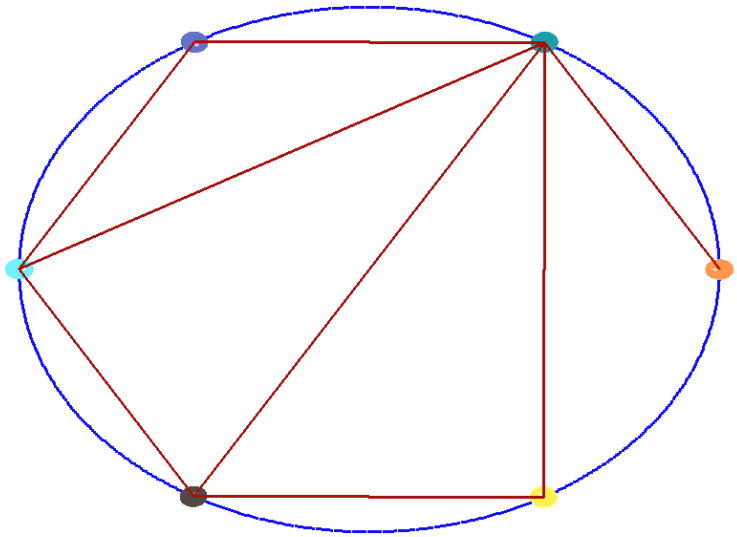

図 4: Chord を利用し構築した P2P ネットワークの可視化例

5　期待される効果

ABLA によって，固定観測点を持たない個人ユーザ参加型のインターネット観測システムが実現可能であり，インターネット上で発生する世界的なトラフィック情報等の把握と，利用者による様々な角度からの解析が可能となる．その結果，マルウェアによる攻撃やトラフィックの増加を早期に発見し，被害の拡大を未然に防ぐための対策を行うことが可能となる．

6　普及 (または活用) の見通し

ABLA(Agent Based Log Analyzing System)，`http://abla.sourceforge.jp/` にて，ソースコードの公開，配布と ABLA の紹介，解説，利用マニュアル，インストール方法等を掲載している．今後は，開発者自身が ABLA による観測システムの観測点を常駐的に設置し，個人ユーザに対して普及活動を行う予定である．

7　開発者名 (所属)

- 葛野 弘樹 (奈良先端科学技術大学院大学 情報科学研究科)
- 中井 優志 (岩手県立大学大学院 ソフトウェア情報学研究科)
- 渡邊 集 (岩手県立大学大学院 ソフトウェア情報学研究科)
- 川原 卓也 (岩手県立大学大学院 ソフトウェア情報学研究科)