# ダークネットに設置したハニーポットへのアクセス解析

笹渕 美寛 †　　曽根　直人 ††　　森井 昌克 †††

† 神戸大学工学部
657-8501 兵庫県神戸市灘区六甲台町 1-1
sasabuchi@stu.kobe-u.ac.jp

†† 鳴門教育大学大学院学校教育研究科
772-8502 徳島県鳴門市鳴門町高島字中島 748
naosone@naruto-u.ac.jp

††† 神戸大学大学院工学研究科
657-8501 兵庫県神戸市灘区六甲台町 1-1
mmorii@kobe-u.ac.jp

**あらまし**　近年，不正アクセスなどのサイバー攻撃による被害が増えている，これらの対策のためには攻撃を検知・解析する必要がある．本研究では攻撃手法の解析のためにダークネット上に観測点を複数設置し，観測点に飛来したパケットを DNAT を用いてハニーポットへ転送する．この方法により複数の観測点を 1 台のハニーポットで観測でき，広域なネットワーク空間に対しての攻撃の検知が可能になる．本研究で用いるハニーポットの Kojoney は SSH，Dionaea は HTTP, MySQL 等のサービスをシミュレート可能であるため，アプリケーション層での攻撃の情報を解析できる．

# A Study of Malicious Traffic Analysis to Honeypots in a Darknet

Yoshihiro Sasabuchi†　　Sone Naoto ††　　Masakatu Morii †††

†Faculty of Engineering, Kobe University
1-1 Rokkodai-cho Nada-ward, Kobe 657-8501, Japan.
sasabuchi@stu.kobe-u.ac.jp

††Graduate School of Education, Naruto University of Education
748, Nakashima, Takashima, Naruto-cho, Naruto-shi, 772-8502 Japan.
naosone@naruto-u.ac.jp

†††Graduate School of Engineering, Kobe University
1-1 Rokkodai-cho Nada-ward, Kobe 657-8501, Japan.
mmorii@kobe-u.ac.jp

**Abstract**　It is necessary to take measures against unauthorized access and cyber-attacks. In this paper, we install multiple observation points in a darknet to analyze these attacks and obtain the information. Packets arrived at the observation points are transfered to honeypots by DNAT. This enable to observe a wide network area with one honeypot. We operate two honeypots, Kojoney and Dionaea, to analyze the attacks at application layer.

# 1　はじめに

今日では，パーソナルコンピュータやスマートフォンの普及に伴い，多くの人々がインターネットを利用し，ネットワークに常時接続するようになった．増大したネットワークトラフィックの中にはセキュリティ対策が十分になされていない端末に対し攻撃を行うマルウェアや不正アクセス等の不正なトラフィック存在する．これらの不正なトラフィックに対して対策を行うため，攻撃者の挙動やサイバー攻撃の検知を行う必要がある．不正なトラフィックを検知，阻止するためにIDS(Intrusion Detection System)やIPS(Intrusion Prevention System) といったシステムが運用されている．また，ハニーポットと呼ばれる囮サーバをネットワーク上に設置し，接続してくる通信を観測，分析する研究が行われている [1]．しかし，正規のトラフィックと不正なトラフィックが混在するネットワーク上ではそれらを正確に分離し不正なトラフィックだけを解析するのは困難である．そこで，未使用のIPアドレス空間（ダークネット）を利用する [2]．ダークネットには原理的に正規のトラフィックが発生しないことから，ダークネットに届くパケットは正規のパケットではないと見なすことができ，不正パケットの解析を効率的に行うことができる．しかし，ダークネットの観測は広域な空間を簡単に観測できるが，応答を返すサーバが存在しないため不正トラフィックの解析をするには得られる情報量が少なくなる．一方，ハニーポットは不正トラフィックから得られる情報量は多くなるが個々のアドレスに設置すると観測する領域の拡大に伴い運用コストが増大する．

我々はNAPT技術を応用し，ダークネットにある複数のIPアドレスを一台のハニーポットで観測するシステムを運用している [3, 4]．そのシステムを用い，観測点となるIPアドレスを設定し，それらの観測点へ飛来するパケットをハニーポットへ転送し，ダークネット上においても応答を返すホストを擬似的に設定することでさらに詳細な攻撃情報を収集する．このハニーポットで得られる情報を解析し，攻撃傾向について考察する．

# 2　不正トラフィックの観測システム

本章ではダークネット上に観測点を設置しハニーポットへのパケット転送によって，不正トラフィック解析を行うシステムを説明する．2.1節にダークネットについて，2.2 節に運用するハニーポットについて述べる．

## 2.1　ダークネット

ある組織等に割り当てられたグローバルIPアドレス空間のうち，未使用のIPアドレス空間をダークネットと呼ぶ．ダークネットは未使用の空間のため，パケットに対する応答を行うサーバやクライアントは存在しない．そのため本来であればダークネットに送られるパケットは存在しない．しかし実際にはダークネットに送られるパケットは存在する．このパケットが存在する原因としては次の3つが考えられる．

- 誤設定による通信
- マルウェア等が実行するスキャン
- ソースアドレスをダークネットに詐称されたパケットのバックスキャッター

サーバやクライアントが存在するネットワーク上では，正規の通信と不正な通信が混在しており，正確な分離は困難である．しかしダークネットに向けての通信は正規の通信ではなく，ダークネットに向けての通信を観測することにより不正な通信の解析が可能となる．ダークネットを観測することにより広域的なネットワークで発生している，攻撃・スキャン行為を検知することができるが，ダークネット上にはホストが存在しないため，パケットの送信元に対し応答パケットを返信することはない．よって接続を試みた後の攻撃者の挙動を把握することはできない．

## 2.2　ハニーポット

ハニーポットは意図的にセキュリティホールや脆弱性を持たせ，マルウェアや不正アクセスを

おびき寄せる囮として働くサーバやネットワーク機器を指す．ハニーポットでは，通信や実行されるコマンドなどアプリケーション層におけるログを収集でき詳細な攻撃手段の解析が可能である．アプリケーションやOSの応答をシミュレートして返答を行うハニーポットを低対話型ハニーポット，実際のシステムを用いたハニーポットを高対話型ハニーポットと呼ぶ．低対話型ハニーポットはシミュレート環境上で稼働するため比較的運用しやすいが，シミュレート性能が不十分であると攻撃者にハニーポットであると見破られる可能性が高くなる．それに対し高対話型ハニーポットは実際にアプリケーションやOSが行う返答を返すので攻撃者にハニーポットであると見破られる可能性は低く，詳細な情報を得る事ができる．しかし実際のシステムと同様に脆弱性が存在した場合，ハニーポットそのものに侵入され攻撃を受けるリスクの高さから，慎重な運用が必要であり運用コストが高くなる．また低対話型ハニーポットのシミュレートする応答を比較的容易に変更することができ，応答を変更することにより攻撃者の挙動の変化を観測することが出来る．しかし，広域なネットワーク空間から情報を得ようとハニーポットを複数台運用することは運用コストが増える問題がある．

#### 2.2.1 Kojoney

KojoneyはSSH（Secure Shell）をシミュレートする低対話型ハニーポットである [5]．SSHは主にLinuxでリモート通信を行うために使用されるサービスであり．Kojoneyはあらかじめ設定した偽のユーザ名とパスワードでSSH接続をシミュレートする．SSHサーバへの接続する際に用いたユーザ名，パスワードをログに記録し攻撃情報を得る．

#### 2.2.2 Dionaea

dionaea[6] はハニーポットNepenthes[7] の後継として開発された低対話型ハニーポットである．マルウェアを収集することができ，MySQL[8] やHTTP等のサーバをシミュレートしている．

表 1: Kojoneyの対応サービス

| 対応サービス | ポート番号 |
|---|---|
| SSH | 22 |

表 2: Dionaeaの対応サービス

| 対応サービス | ポート番号 |
|---|---|
| FTP | 21 |
| HTTP | 80 |
| MICROSOFT-DS | 445 |
| MYSQL | 3306 |

攻撃パケットの中のシェルコードをパターンマッチングによって検出した上で，設定された応答を返すことで脆弱性をシミュレートしている．

## 3 観測システム

### 3.1 複数IPでのハニーポット運用

広域なネットワーク空間から情報を得ようとするにはハニーポットを各IPアドレスに設置する必要がある．しかし，運用コストが高いハニーポットを複数台同時に運用することは難しい．そのため，観測システムではダークネット上に複数の観測点を設置し，観測点に飛来したパケットを一箇所のハニーポットに転送する．観測点からの転送ではLinuxルータを用いハニーポットへ転送しハニーポットの応答を送信元へ返答する．転送にはパケットのIPヘッダを書き換えるNAT(Network Address Translation)を使用する．観測点に到達したパケットはまず，攻撃元からのIPパケットの宛先IPアドレスをハニーポット宛に変換する (DNAT), そしてハニーポットからの応答パケットも同様に攻撃元IPアドレスへと宛先を変換する．また，宛先ポート番号により対応しているサービス毎に転送するハニーポットを分けることによって，これにより，攻撃者からあたかも観測点IPアドレスに設置されているホストと通信を行っているように見える（図1）．さらに，ダークネットを観測することにより観測点付近へのスキャ

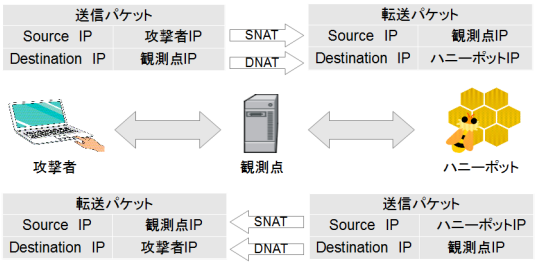


図 1: NAT によるパケット転送

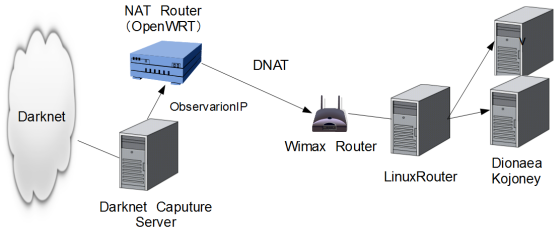


図 2: ネットワーク構成

ンに対し，ハニーポットが与える影響も観測できる．

### 3.2 観測システムの構成

観測システムのネットワーク構成を図 2 に示す．ダークネットに向けられたパケットを NAT により転送を行う．そのために観測システムでは OpenWrt をルータにインストールしパケットを転送する．ダークネットの IP アドレス空間の中に 32 個の観測点を設置し，観測点の IP アドレスに向けたパケットを OpenWrt をインストールしたルータへルーティングする．観測点以外のダークネットに向けられたパケットのヘッダ情報はパケット観測用ホストに情報を保存する．OpenWrt ルータは DNAT を行い観測点に向けられた宛先アドレスを変換し，ハニーポット側へパケット転送を行う．ハニーポット側では，WiMAX を用いたサービスを運営している UQWiMAX[9] の回線を利用してインターネットに接続する．ハニーポットには dionaea と SSH ハニーポットとして Kojoney を使用する．WiMAX 到着したパケットは Linux ルータを用いて対応するサービス毎にパケットを送る

表 3: 観測環境

| | |
|---|---|
| ダークネット | /18　（16384 アドレス） |
| 観測点 | ダークネットに 32 点設置 WiMAXIP アドレスで 1 点計 33 地点 |
| 観測点設置ルータ | バッファロー BHR-4RV |
| ハニーポット使用回線 | UQ WiMAX |

ハニーポットを振り分ける．また WiMAX ルータの IP アドレスに向けて送られたパケットも同様にハニーポットへ転送する．よってハニーポットが観測する IP アドレスはダークネット上の 32 地点と WiMAXIP アドレスの合計 33 箇所である．

## 4 観測結果と考察

本節では 3 章にて述べたシステムを用いて観測した結果を示し，考察する．

### 4.1 アクセス傾向

ハニーポットがホストとして働いている 21, 22, 80, 445, 3306 番ポート宛のパケット，ハニーポットが稼働していない 3389 番ポート宛のパケットの 1 日当たりのアクセス数の遷移を表したグラフを図 3 に示す．パケット観測ホストが停止していた期間（8 月 14 日〜17 日）はデータが存在していない．図 3 より，異なるポート番号においてアクセス数の相関は見られない．このことより，攻撃ツールは複数のポート宛に同時攻撃は行わず，特定のポートに向けての攻撃を行っていると考えられる．今回の実験期間では，ハニーポットの設置がダークネットに影響を及ぼしている例は観測できなかった．

### 4.2 Kojoney で得られた情報

Kojoney へのアクセスのうち，ログイン成功後，コマンドを実行した形跡が 3 例観測された．

表 4: Kojoney を用いた観測

| 対応サービス | ポート番号 |
|---|---|
| 観測日時 | 2013/8/12　16:30 〜8/14 18:00 |
| 接続回数 | 11133 回 |
| ログイン試行回数 | 16667 回 |
| ログイン成功後コマンド入力があった回数 | 3 回 |
| ログインに成功するユーザ名とパスワードの組み合わせ | 23752 通り |

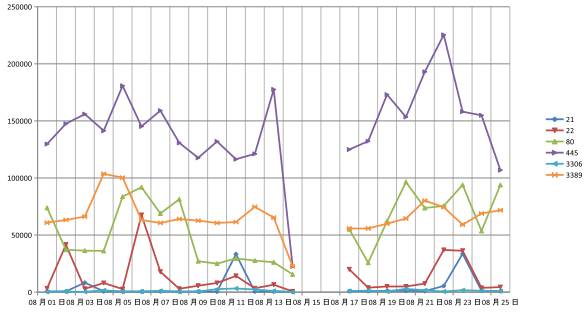


図 3: 各種ポートに対するアクセス回数

本節ではスクリプトを用いた攻撃について述べる．コマンドを実行した 3 例のうち手動で攻撃されたと考えられる 2 例については 4.3 節で述べる．Kojoney へのアクセスにおいて，認証に失敗した場合，Kojoney の標準設定では 3 回まで認証を試みることが出来る．Kojoney に対する 11133 回の接続において，ログイン認証が行われた回数は 16667 回であり，平均して 1 回の接続あたり 1.5 回のログイン認証が行われている．ログイン認証の際に行われる一般的な攻撃の流れを図 4 に示す．認証に失敗した場合，接続を切断して別のユーザ名とパスワードを用いてログインを試みている．失敗した場合，1 回の接続が行われている時間は大多数は 10 秒以内であり，自動化して攻撃をしていると考えられる．成功した場合，接続を断ち再び別のユーザ

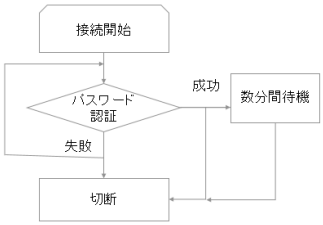


図 4: 一般的な攻撃の流れ

名で接続を試みるものと，接続をしたまま数分間何も実行しないものに分かれることがわかった．ログイン成功後，コマンドを入力されるという事象は 3 例のみ観測された．そのうち 1 例は 1 回目に入力されたユーザ名と，パスワードの組み合わせが同じであり，2 回目の認証の時だけ，パスワードを変化させてログインを試みていた．その他大多数の攻撃が一度ログイン認証に失敗し切断した場合は，すぐさま次の接続を試みているが，この攻撃者は切断後次の攻撃まで 270 秒の間隔があった．この攻撃者がログイン認証に成功した場合 “ls” のコマンドを入力した後切断している．接続からログイン認証をを試みて切断するまで 4 秒足らずであり，接続の挙動が一定であることから自動化されたツールからの攻撃であると推測できる．同じ自動化された攻撃でも挙動が異なり，いくつかの自動化の手法があると考えられる．ここで “ls” 以外のコマンドの入力がなかったのは，コマンドに対する応答からハニーポットであると見破られた事が原因，またはログイン後に “ls” のコマンドを実行するだけのスクリプトであるいう原因が考えられる．

## 4.3　SSH への攻撃例

手動と判断される攻撃について考察する．大多数を占める自動化された攻撃と異なる特徴は以下の通りである．

- SSH クライアント名
- ログインに要する時間
- 同時刻に他の IP への攻撃が見られない

観測期間中，手動と判断できる攻撃を 2 例検知した．表 7 と表 8 に接続の際入力されたコマンドを入力順に示す．コマンド入力の際にコマンドの入力誤りが観測出来たことから明らかに，手動での攻撃であると判断できる．手動の攻撃の際，入力されたユーザ名とパスワードは 2 例とも，誤ったパスワードを入力することなく “username: alex password: alex” の組み合わせでログインに成功していた．2 度目の攻撃が確認できた，その 2 日前に 1 度目の攻撃があり，その 2 日前のログデータにこのユーザ名とパスワードの組み合わせを試みている自動化された攻撃が観測された．その際に試みられたユーザ名とパスワードの組み合わせを入力順に表 5 に示す．

表 5 より，ログイン認証に使用したユーザ名とパスワードの組み合わせを試みた順番はアルファベット順である．ログインに成功した後でも，続けてコマンドの入力は行わず接続を絶って次のユーザ名とパスワードでログイン認証を試みている．また，同時刻に複数の同じユーザ名とパスワードを用いた組み合わせのログインが行われている．観測期間中 “username: alex password: alex” の組み合わせで認証を行われたのはこの攻撃の時だけであった．手動によるログインが 2 例とも 1 度目でログインに成功しているのは事前に自動化されたパスワード解析の結果パスワードを知り得ていたからだと推測できる．ここから推測できる攻撃者の挙動は，事前にブルートフォース攻撃でログイン可能なユーザ名とパスワードの組を記録して，後日手動で攻撃していると予想される．

ログイン後の攻撃者の挙動は，1 回目の侵入では実行プロセスを確認し，CPU の情報得ようとしてその後，切断した．接続から切断までは 83 秒であった．2 回目の侵入では，プロセスの確認後，各種ログファイルと履歴の削除，加えて新たなログファイルの作成を行なった．その後パスワードファイルの閲覧を試みてその後切断した．この接続の時間は 116 秒であった．

表 5:
使用ユーザ名とパスワード (2013/8/21)

| ユーザ名 | パスワード | 可否 |
|---|---|---|
| adiza | muielumata | false |
| admin1 | dementel22 | false |
| admin | pentrudealerudavid | false |
| admin | seth1985 | false |
| ale | aicumine | false |
| alex | alex | true |
| alex | ubeandramondialu | false |
| altibase | altibase | false |
| anthony | password | false |

表 6:
使用ユーザ名とパスワード (2013/8/23,25)

| ユーザ名 | パスワード | 可否 |
|---|---|---|
| alex | alex | true |

## 5 まとめ

鳴門教育大学が所持する /18 のダークネットに観測点を複数接置し，観測点に向けられた接続をハニーポットに転送することで SSH への攻撃傾向を観測した．ハニーポットとダークネットの観測データを照合する事により，ハニーポットへのアクセスの原因である．その結果，辞書攻撃を行っている例を確認し，実際に侵入した際の挙動を観測した．辞書攻撃が行われた際，ログイン認証に成功した場合においても続けてログイン認証を試みており，ログインに成功する組み合わせを増やした場合，ハニーポットだと見破られる可能性がある．ログイン認証に成功した場合の挙動で何もせず待機していることがほとんどであった．接続可能な時間を変化させることによりハニーポットへの攻撃手法，ダークネットへのスキャンに影響を与える可能性があり，今後はハニーポットの応答によって攻撃手法に変化が見られるか観測を行う．

今回観測できたログイン後の挙動をさらに深

表 7: 1 度目の接続で入力されたコマンド

| 入力順 | 入力コマンド |
|---|---|
| 1 | w |
| 2 | id |
| 3 | uname -a |
| 4 | sudi (入力ミス) |
| 5 | id |
| 6 | cat /rp (入力ミス) bash |
| 7 | cat /proc/cpuinfo |
| 8 | w |
| 9 | c (入力ミス) |
| 10 | id |
| 11 | cat /proc/cpuinfo |
| 12 | 切断 |

表 8: 2 度目の接続で入力されたコマンド

| 入力順 | 入力コマンド |
|---|---|
| 1 | id |
| 2 | w |
| 3 | unset; rm -rf (ログの削除) |
| 4 | w |
| 5 | ls -a |
| 6 | u(入力ミス) cat /etc/passwd |
| 7 | passwd root |
| 8 | id |
| 9 | c uname -a |
| 10 | su - |
| 11 | id |
| 12 | passwd root |
| 13 | cat /pr cp |
| 14 | cat /etc/issue |
| 15 | cat /etc/passwd |
| 16 | ls -a |
| 17 | bash |
| 18 | 切断 |

く知るためにはハニーポットであると見破られないことが重要である．Kojoney は SSH ログイン後のシミュレート性能が不十分であるので攻撃者にハニーポットであると見破られる可能性が高い．コマンド応答の改良を行い，さらに詳しいログイン後の挙動を観測する必要がある．しかし，エミュレーションには限界があり低対話型ハニーポットでは得られる情報に限界がある．DNAT を用いたこの観測システムでは出口監視 IPS の台数も減らすことができ，高対話型ハニーポットを運用するコストを減らすことが可能である．今後は現在のシステムに加えて高対話型ハニーポットを併設し観測を行う．

## 参考文献


[1] The Honeynet Project `http://www.honeynet.org/`.

[2] 井上大介, “ダークネット観測の技術動向と観測事例,” 情報セキュリティ技術動向調査 (2008 年下期), `http://www.ipa.go.jp/security/fy20/reports/tech1-tg/2_07.html`.

[3] 曽根直人, 正力達也, 鳥居明久, 村尾岳人, 森井昌克, “可視化によるダークネットの不正パケット解析 - ハニーポットとの併用による相関分析,” 信学技報, *ICSS2011-46*, pp.43-48, Mar. 2012.

[4] 宇都宮理人，土田耕平，曽根直人, 森井昌克, “ダークネット観測に対してハニーポットが与える影響,” *SCIS2013*,2013.

[5] “Kojoney - A honeypot for the SSH Service, ” available at `http://kojoney.sourceforge.net/`.

[6] “dionaea - catches bugs, ” available at `http://dionaea.carnivore.it/`.

[7] ““Nepenthes Pharm,, ” available at `http://www.honeynet.org/node/501/`.

[8] “MySQL ” `http://dev.mysql.com/`

[9] UQ コミュニケーションズ, “UQ WiMAX,” `http://www.uqwimax.jp/`.