未接続IPアドレス空間へのハニーポット動的設置によるネットワークの監視手法

伊藤 達哉† 栃窪 孝也‡

†日本大学大学院 生産工学研究科
数理情報工学専攻
citt13002@g.nihon-u.ac.jp

‡日本大学 生産工学部
数理情報工学科
tochikubo.kouya@nihon-u.ac.jp

あらまし 近年，特定の企業や個人をターゲットにした情報窃取を行う標的型サイバー攻撃が増加している．標的型サイバー攻撃ではスパイウェアが内部ネットワークへ侵入し，目的のサービスへ攻撃を仕掛けるためにポートスキャンや脆弱性の調査などのスパイ活動を行う．本稿では内部ネットワークから一時的に切断されたホストとハニーポットを動的に置き換えることで，スパイウェアからのポートスキャンを検出するシステムを提案する．提案システムではハニーポットの設置時にIPアドレスとMACアドレスとの対応関係を考慮した置き換えが可能である．

Network Monitoring Method with Dynamic Honeypots for Unconnected IP Addresses

Tatsuya Ito† Kouya Tochikubo‡

†Graduate School of Industrial Technology,
Nihon University

‡College of Industrial Technology,
Nihon University

citt13002@g.nihon-u.ac.jp

tochikubo.kouya@nihon-u.ac.jp

Abstract In recent years, targeted cyber-attacks against a specific person or company, which cause a leakage of private information, have been increasing. In targeted cyber-attacks, a spyware which broke into the internal network performs port scan and attacks the vulnerability. In this paper, we propose a network monitoring system with dynamic honeypots. The proposed system can detect port scan by replacing the host with a honeypot when the host is disconnected from the network.

1 はじめに

近年，企業や組織を標的にするサイバー攻撃が世界各地で確認されている．サイバー攻撃者たちは標的となる企業や組織の機密情報を窃取するため，標的とする組織に気づかれないように可能な限り隠密に情報を収集する．隠密な情報収集の例としてIDSをすり抜けることができる新種の脆弱性攻撃やポートスキャンなどが挙げられる [1]．それらの脅威を検出するための手法として，ネットワーク上にハニーポットを設置してネットワークに流れるデータを収集し分析する手法 [2, 3] が提案されているが，被攻撃者にとって攻撃の隠密性が高いほど攻撃の検出が困難となる．この手法を用いることで，新たな脅威の発見や攻撃者を重要なシステムから攻撃の注意をそらすことができるなどの効果が

得られる．しかし，ハニーポットの IP アドレスや MAC アドレスを攻撃者に知られた場合，上記のような効果が得られなくなるという問題がある．そこで，ハニーポットを用いてネットワークの未使用 IP 空間の監視を行う研究として，溝口らは DHCP を使って動的にハニーポットを設置することでネットワークの監視を行う手法を提案している [4]．この手法では DHCP によってクライアントに貸し出ししていない IP アドレスを未使用 IP アドレスとみなし，オープンソースのハニーポットである honeyd[5] を動的に設置する．設置された honeyd はプロキシとして動作し，特定のホストへリダイレクトを行う．しかし，リダイレクトを用いるため，ハニーポットの応答にだけ遅延が発生するという問題がある．また下田らは，TCP SYN パケットに対して SYN/ACK パケットが返らないフローの送信元に対してハニーポットから遅延応答を返すことで，そのフローを仮想センサとして利用する手法を提案している [6]．この手法ではハニーポットからの応答に遅延が発生するため応答速度をフィンガープリントとして，ハニーポットであることが攻撃者に検出されてしまう [7].

一方，ハニーポットを設置せずにパケットのデータを解析することでネットワークの監視を行う手法として，下田らはフローデータからの Dark IP 抽出による脅威観測法 [8] を提案している．この手法は未使用の IP アドレス空間の監視方法として，パケットのフローデータを解析する手法が用いられている．また今間らは，ブリッジとしてルータの直前に監視システムを設置し，使用済 IP アドレスを自動抽出しながら、未使用アドレス宛へのパケットを収集する手法を提案している [9]．これらの研究ではハニーポットを用いないため，未使用 IP アドレス空間は攻撃者へ応答を返さない．よって攻撃者は，応答を返さない IP アドレスにはホストが存在しないと考えて，攻撃を行わない可能性がある．

そこで本稿では，ハニーポットを動的に設置してハニーポットの IP アドレスと MAC アドレスとの対応を変化させることで，攻撃者がハニーポットの場所を把握できなくなることを目的としたネットワーク監視システムを提案する．なお，ハニーポットの IP アドレスと MAC アドレスは実際にネットワークに接続されているコンピュータ (以下クライアントコンピュータ) を基に変化させる．また本稿は，外部からアクセスできない内部ネットワークを対象とし，内部ネットワーク上の未使用 IP 空間にハニーポットを設置することで，内部でのスパイ活動を検出することを目的としている．したがって，インターネットに設置するハニーポットに比べて攻撃を受ける量が少ないため，収集データの分析量を軽減できる．

2 ネットワークの監視手法

2.1 IDS によるネットワーク監視

IDS(Intrusion Detection System) は侵入や攻撃を監視するシステムである．また，ネットワークに対して侵入や攻撃を監視する IDS はネットワーク型 IDS と呼ばれる。IDS の検知方式はシグネチャ型とアノマリ型の 2 つに分類される．アノマリ型は正常な動作を定義して正常でない動作が観測された場合に攻撃であると判定する．一方，シグネチャ型は，シグネチャと呼ばれる攻撃パターンを定義し，パターンに合致した場合に不正と判断する方式である．しかし，IDS には誤検知や攻撃を見逃すという問題がある [10]．アノマリ型は正常な通信も攻撃と判断してしまう場合があり，シグネチャ型は既知の攻撃パターンを利用するため未知の攻撃には対応することができない．

2.2 ハニーポットによる監視

ハニーポットとは，攻撃を受けるために設置される囮のシステムである．ハニーポットの種類は対話のレベルや実装によって様々であるが，一般的にネットワーク監視に用いられているハニーポットには以下のようなものがある．

- 低対話型ハニーポット
  攻撃者との対話を制限したハニーポットで

ある．特定のオペレーティングシステムやサービスをエミュレートする．攻撃者の行動は制限されるためシステムが侵害されるリスクが低い．

- 高対話型ハニーポット
  実際のオペレーティングシステムとアプリケーションをインストールし，低対話型ハニーポットと比べてシステムが侵害された場合のリスクが高い．
- 仮想ハニーポット
  仮想マシンで構成されたハニーポットである．ホストを侵入前の状態へ容易に戻すことができ，リスクを抑えることができる．

3　提案手法

3.1　システムの構成

図 1 に提案システムの構成を示す．提案システムは，DHCP サーバと honeyd を管理するサーバ (以下 honeyd 管理サーバ) から構成され，内部ネットワークのスパイ活動を検出するために LAN 内に設置する．DHCP サーバは ISC DHCP ver4.2.4[11] を用いてクライアントコンピュータの接続と切断の管理を行い，honeyd 管理サーバへクライアントコンピュータの接続状態の変化を通知する．提案システムの DHCP サーバには，コンピュータの接続状態を honeyd へ通知を行う機能を追加している．また，クライアントコンピュータが honeyd 管理サーバへアクセスすることを防ぐために，ファイアーウォールによってフィルタリングを行う．

本監視手法は，DHCP によって貸し出されている IP アドレスで，アイドル状態のクライアントコンピュータをハニーポットへ置き換えるシステムである．攻撃者にハニーポットの設置を気付かれてはいけないので，置き換える前のクライアントコンピュータの MAC アドレスに設定した honeyd を設置する．

3.2　動的なハニーポットの設置

提案システムでは DHCP サーバが IP アドレスの返却の通知 (以下 DHCP Release) を受け取ると，honeyd 管理サーバへクライアントコンピュータの切断通知を送る．次に honeyd 管理サーバは返却された IP アドレスと切断されたクライアントコンピュータに使用されていた MAC アドレスを用いて，honeyd を起動する．切断されたクライアントコンピュータが再度接続を試みた場合，当該 MAC アドレスを使った honeyd を停止する (図 1)．DHCP セグメントと honeyd 管理サーバを分離するのは honeyd の侵害によるリスクを軽減するためである．クライアントコンピュータがネットワークから切断される場合は必ずしも DHCP サーバーに DHCP Release を送るわけではないので，本システムでは ARPrequest[12] を定期的に送ることでクライアントコンピュータが異常切断されていな

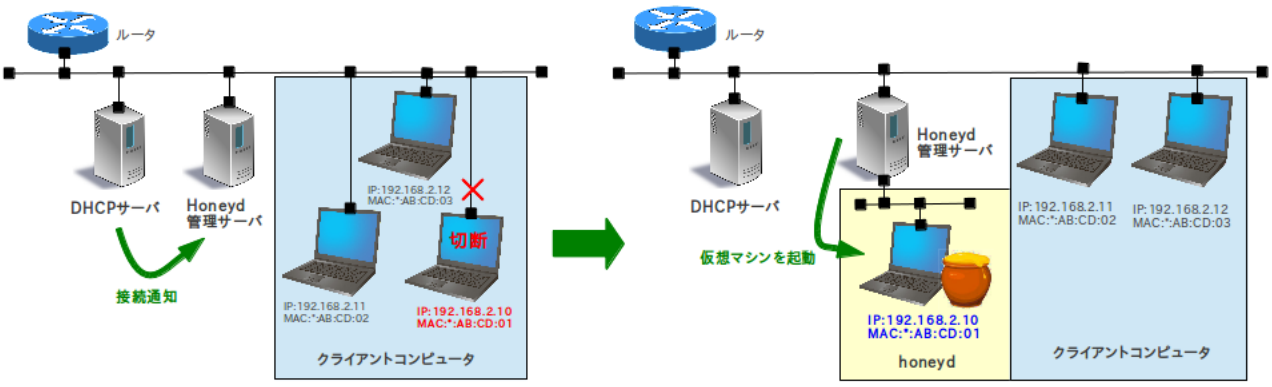

図 1: システムの構成

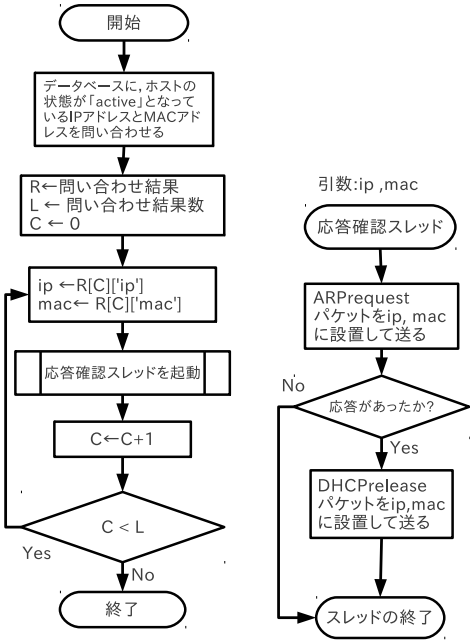

図 2: クライアントコンピュータの切断確認手順

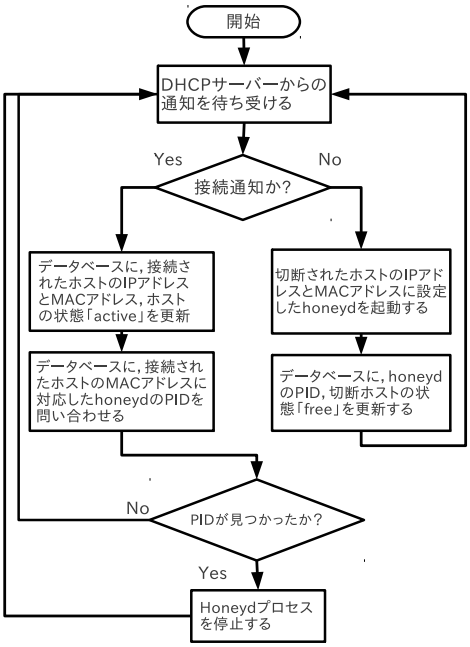

図 3: honeyd 管理サーバの処理手順

いか監視する．ARPrequest による切断確認アルゴリズムは，図 2 に示す通りである．マルチスレッド処理を用いるのは，切断を監視するクライアントコンピュータの数が増大した場合に処理時間を短縮するためである．

3.3 ハニーポットの管理

処理の流れは図 3 に示す通りである。はじめに honeyd 管理サーバが，DHCP サーバからクライアントコンピュータの接続通知を受け取ると，honeyd 管理サーバは接続されたクライアントコンピュータの IP アドレスと MAC アドレスをデータベースに記録する．そしてクライアントコンピュータの切断通知を受け取ると，データベースに登録された IP アドレスと MAC アドレスを用いて honeyd を起動する．honeyd が振る舞う OS については，あらかじめデータベースへ MAC アドレスに対応する OS を手動で設定しておくことで変化させることが出来る．

3.4 IP アドレスの重複

ハニーポットが起動している状態で，同一の IP アドレスで接続を試みようとする場合，IP アドレスの重複が発生してしまう．Microsoft Windows 7 や Apple MAC OS X(10.8) などの OS では DHCP サーバへ IP アドレスの貸出要求 (以下 DHCP Request) を行う前に ARPrequest を用いて利用予定の IP アドレスが既に利用されていないかを確認する．そのため DHCP サーバが DHCP request を受け取る前に honeyd を停止する必要がある．そこで，honeyd 自身が ARP パケットを読み取り宛先 MAC アドレスが honeyd 自身の MAC アドレスと同一の場合，同じサブネットに同じ MAC アドレスのマシンが接続されているので，自己停止を行うように honeyd を改善している．しかし，攻撃者も honeyd の MAC アドレスに偽装した ARP パケットを不正に作成することで honeyd を停止することが出来る．そこで honeyd が停止した場合，一定時間内に honeyd と同じ MAC アドレスのクライアントコンピュータが DHCP によって IP アドレスの貸出を受けなかった場合に攻撃と判定するように実装している．

4 評価実験

4.1 ハニーポットの起動時間と台数の関係

コンテナ型仮想環境である LXC[13] を用いて図 6 に示すように，複数台のクライアントコン

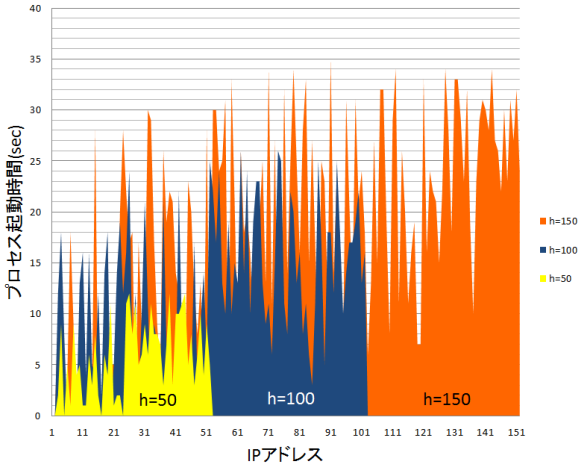

図 4: ハニーポット切り替えの時間変化

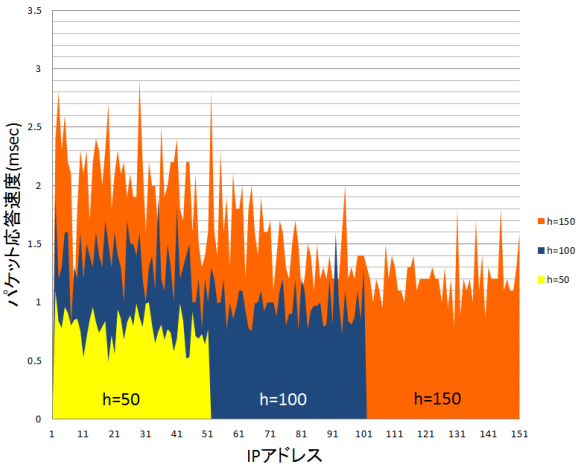

図 5: ハニーポットの台数と応答速度の関係

表 1: 実験環境

	DHCP サーバ	honeyd 管理サーバ	LXC マシン
CPU	AMD Athlon 64 X2 2.50GHz	Intel Core i5-2400 3.10GHz	Intel Core i5-2415M 2.30GHz
メモリ	3.00GB	8.00GB	8.00GB
カーネル	Linux 3.5.0-37-generic	Linux 3.5.0-37-generic	Linux 3.5.0-37-generic
OS	ubuntu server 12.04	ubuntu server 12.04	ubuntu server 12.04

ピュータをネットワークに接続し，LXC マシンをネットワークから切断することで，連続で honeyd を起動させ，ホストが切断され honeyd が起動完了するまでの時間と起動する honeyd の台数との関係を評価する実験を行った．実験環境は表 1 の構成で行い，実験では図 4 のような結果が得られた．図中の h は honeyd の起動台数，縦軸は honeyd が起動した時間，横軸は IP アドレスのホスト部を表している．また，実験では 1 台目の honeyd の起動時間を 0 秒としている．結果から honeyd の起動台数が 50 台の場合は最大で 12 秒以内，100 台では 25 秒以内，そして 150 台では 35 秒以内で honeyd プロセスの起動が完了出来ることが分かる．また，それぞれの平均プロセス起動時間は 50 台の場合 6 秒，100 台の場合 12.53 秒，そして 150 台の場合 18.52 秒であった．本システムでは ARP パケットによる切断確認を 25 秒間隔で実行する．よって honeyd を 150 台起動する場合，1 分以内に起動を完了することが出来る．

4.2 ハニーポットの応答速度

表 1 の honeyd 管理サーバの環境を用いて，honeyd の起動台数がそれぞれ 50 台，100 台，150 台の場合でのパケット応答速度を計測し，honeyd の起動台数が通信の応答速度に与える影響を評価する実験を行った．応答速度の計測には ARPrequest を用いた．結果は図 5 に示す．図中の h は honeyd の起動数，縦軸は応答速度で横軸は IP アドレスのホスト部を表している．またホスト部が 12 と 31 の IP アドレスは honeyd ではなくクライアントコンピュータが接続されている．実験の結果から，パケットの応答速度は honeyd もクライアントコンピュータもパケット応答速度はほとんど変わらないことが分かる．また honeyd の数が多くなると平均応答速度が遅くなっている．これはネットワークに流れるパケットの総量が多くなりスイッチングハブやルータへ負荷がかかるためであると考えられる．

4.3 ネットワークに与える負荷

実装したシステムがネットワークに与える負荷を評価する実験を行った．ARPrequest パケットサイズは実装したシステムでは 60 バイトであった．ARPreplay パケットサイズも約 60 バイトとすると，発生するトラフィック量 = (切断確認を行うホストの数＋接続されているホスト数) × 60 バイト となる．ネットワークに接続されているホストが 150 台の場合は最大 18K バイトとなる．20 秒に 1 回の間隔で監視する場合は 1 分間に 54k バイトのトラフィックが発生する．実際にネットワークに接続されたホストが 150 台の場合，1 分間に観測できた ARP パケットは表 2，3 のような結果であった．また実験には GS108E[14] のスイッチングハブを使用した．実験の結果からシステムが発生させた ARP パケットは，ARPreplay と ARPrequest がそれぞれ 450 パケットで合計 900 パケットとなりトラフィック量は 54k バイト，非システムから発生した ARP パケットは 19 パケットでトラフィック量は 1140 バイトであることが分かる．よって，900 パケットで 54k バイトのトラフィックは無視できる量である．

表 2: 1 分間に発生した ARPrequest

	パケット数	トラフィック (バイト)
システム	450	27000
非システム	10	600

表 3: 1 分間に発生した ARPreplay

	パケット数	トラフィック (バイト)
システム	450	27000
非システム	9	540

4.4 IDS による攻撃の検出

スパイ活動を検出するためには，ハニーポットによって収集したデータを基に攻撃を判定する手段が必要である．そこで IDS を用いることで攻撃の判定を行う実験を行った．実験では，ネットワーク上で頻繁にやりとりされる ARP パケットの脆弱性を利用して盗聴を行う arpspoofing 攻撃とポートスキャン，そして脆弱性スキャンの検出を行った．攻撃の検出については，honeyd 管理サーバに流れるパケットをオープンソースの IDS である snort[15] へミラーリングすることで監視を行った．snort を用いて arpspoofing 攻撃を検出する場合，あらかじめ IP アドレスと MAC アドレスのホワイトリストを作成し，リストにマッチしない ARP パケットを発見した場合に攻撃と判断する．実装システムでは DHCP によって IP アドレスと MAC アドレスの対応関係が管理されているため，arpspoofing を検出するためのホワイトリストを作成することは容易である．実験では ettercap[16] を用いて arpspoofing を行い，snort によって攻撃を検出する

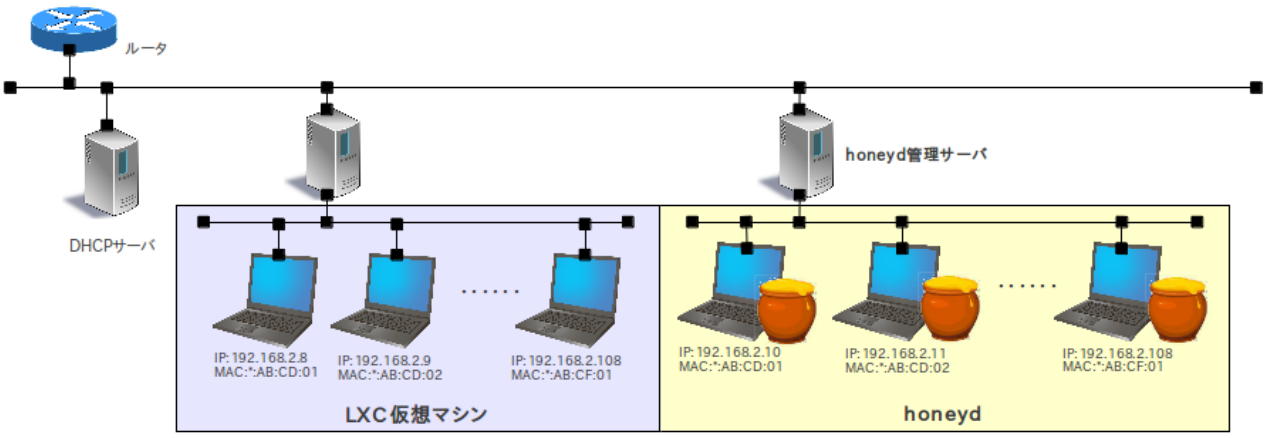

図 6: 実験環境の構成

ことが出来た．また，ポートスキャンについては nmap[17] を用いて実験を行った．実験は表 1 の honeyd 管理サーバ上に honeyd を 150 台起動させた状態で，1 台の honeyd のポート 22 番と 80 番に対して，IDS の検出を回避するステルスポートスキャンを行った．実装したシステムでは，すべての honeyd が 1 台のマシンで管理されているため，honeyd 以外のトラフィックが発生せず正しくポートスキャンを正しく検出することができた．脆弱性スキャンは metasploit-framework[18] を用いて，1 台の honeyd のポート 22 番と 80 番に対して利用可能な 238 種類の脆弱性スキャンを行った結果，76 種類の脆弱性スキャンを検出することが出来た．またスキャンの時間間隔を変化させた場合も検出数に変化が見られなかった．これは snort に登録されていないシグネチャを持った脆弱性スキャンを検出することが出来なかったと考えられる．

5 おわりに

本稿では実在するホストと同じ IP アドレス，MAC アドレスのハニーポットを動的に生成し設置することにより，攻撃者によるハニーポット検出を困難にすることを目的としたハニーポットの設置方法を提案および実装した．

提案手法では IP アドレスや MAC アドレスが変化しないため，従来の方式と比べてハニーポット検出が困難となる．また NIDS を併用することで，ARP スプーフィング攻撃に対応出来るように改善した．

今後は，シグネチャ型 IDS では検出することが出来なかった攻撃を検出するために，アノマリ型 IDS を用いることで検出を行い評価する．

参考文献

[1] 二木 真明, 佐藤 元彦, 山崎 文明, 内田 勝也, “標的型サイバー攻撃と APT に関する考察,” Vol.2012-CSEC-56 No.20, pp.2-5, 2012.

[2] H.Artail, H.Safa, M.Sraj, I.Kuwatly, and Z.A. Masri, “A hybrid honeypot frarnework for improving intrusion detection systems in protecling organizational networks,” Computers & Security 25, pp.274-288, 2006.

[3] M.Vrable, J.Ma, J.Chen, D.Moore, E.Vandekieft, A.C. Snoeren,G.M. Voelker and S.Savage, “Scalability, Fidelity, and Containment in the Potemkin Virtual Honeyfarm,” In Proceedings of the twentieth ACM symposium on Operating systems principles (SOSP ’05), pp.148-162, 2005.

[4] 溝口誠一郎, Le Malecot Erwan, 堀 良彰, 桜井 幸一, “DHCP によって管理されたセグメントに存在する未使用 IP アドレスの監視手法,” Vol.2008-CSEC-41 (10) , pp.59-60, 2008.

[5] honeyd, `https://github.com/DataSoft/Honeyd`

[6] 下田晃弘, 森達哉, 後藤滋樹, “DarkFlow 検出によるリアルタイム・インターネット脅威検出システム,” 電子情報通信学会 ネットワーク仮想化研究会 (NV2011-4), pp.2-4, 2011.

[7] T.Kohno, A.Broido, and K.C. Claffy, “Remote physical device fingerprinting,” IEEE Transactions on Dependable and Secure Computing vol.2 no.2, pp.93-95, 2005.

[8] 下田晃弘, 後藤滋樹, “フローデータからの Dark IP 抽出による脅威観測法,” 電子情報通信学会論文誌 B, vol.J92-B, no.1, pp.163-173, 2009.

[9] 今間俊介, 福田健介, 廣津登志夫, 菅原俊治, “断片ダークネットのためのパケット観測用ブリッジの提案,” 第 9 回インターネットテクノロジーワークショップ (WIT2008), pp.2-3, 2008.

[10] 小埜勇貴, 有馬竜昭, 永山聖希, 吉田和幸, “Snort とのログ比較による scan 攻撃検知システム検知結果の精度調査,” 情報処理学

会九州支部 火の国情報シンポジウム 2011
論文集 , pp.6-7, 2012.

[11] isc-dhcp-server,June 2012
ftp://ftp.uwsg.indiana.edu/linux/
debian/pool/main/i/isc-dhcp/isc-dhcp
_4.2.4.orig.tar.gz

[12] An Ethernet Address Resolution Protocol
http://www.ietf.org/rfc/rfc826.txt

[13] LXC, Mar 2009
http://lxc.sourceforge.net/man/lxc.html

[14] GS108E
http://www.netgear.jp/
products/details/GS108E.html

[15] snort, Jul 2013
https://www.snort.org

[16] ettercap, Feb 2013
http://ettercap.github.io/ettercap/

[17] nmap, Jun 2012
http://nmap.org/

[18] metasploit-frarnework
http://www.metasploit.com/