情報処理学会論文誌 Vol.61 No.9 1397–1413 (Sep. 2020)

広域ネットワークスキャンに基づくオープンソースハニーポットの運用実態調査

森下 瞬[1,a)] 上野 航[1] 田辺 瑠偉[2] カルロス ガニャン[2,3] ミシェル ファン イートゥン[2,3]
吉岡 克成[4,5] 松本 勉[4,5]

受付日 2019年11月25日, 採録日 2020年6月1日

概要：インターネット上で発生している攻撃を観測するために，オープンソースハニーポットの研究や運用が行われている．しかし，オープンソースハニーポットの特徴は攻撃者によって検知可能であり，回避される可能性がある．本研究では，あらかじめ作成した 20 種類のハニーポット検知用のシグネチャを用いて，攻撃者が容易に検知可能なバナー等の応答をカスタマイズしていない 14 種類のオープンソースハニーポットの利用状況を調査する．そして，現状の運用者のハニーポット検知に対する問題意識を把握し，注意喚起により検知への対策を促進することを目指す．評価実験の結果，637 の AS 上で運用される 19,208 のハニーポットが容易に検知可能な状態で運用されていることが判明した．多くが研究機関のネットワークで運用されていたが，企業やクラウドでも運用されていた．そのうちのあるハニーポット群は著名なセキュリティセンタで実運用されていることが判明した．このうち，11 組織のハニーポット運用者に連絡をとったが，4 つの組織からしか返答が得られなかったことから，ネットワークやハニーポットの管理に十分な注意が払われていない可能性がある．加えて，ある国立研究機関のネットワークの運用者は，ハニーポット検知の問題を認識していなかった．また，いくつかのハニーポットが攻撃者によって，マルウェアの配布に悪用されている事例を発見した．検知されたハニーポットの運用者に通知を行い，シグネチャベースの検知を回避するためのカスタマイズを推奨した．同様に，ハニーポットの開発者に対しても通知を行い，本研究成果を共有した．そのうちの開発者の 1 人は我々の開示を考慮し，ハニーポットのリポジトリにカスタマイズの記述を追加した．このように，本研究はハニーポットの適切な運用に貢献できたと考える．

キーワード：ハニーポット，ハニーポット検知，ネットワークスキャン

An Internet-wide View of Self-revealing Honeypots

Shun Morishita[1,a)] Wataru Ueno[1] Rui Tanabe[2] Carlos Gañán[2,3] Michel J.G. van Eeten[2,3]
Katsunari Yoshioka[4,5] Tsutomu Matsumoto[4,5]

Received: November 25, 2019, Accepted: June 1, 2020

Abstract: Open-source honeypots are a vital component in the protection of networks and the observation of trends in the threat landscape. Their open nature also enables adversaries to identify the characteristics of these honeypots in order to detect and avoid them. In this study, we investigate the current situation of honeypot operator's awareness of honeypot detection by investigating the prevalence of 14 different open-source honeypots that do not customize responses such as banners, which make them easily detectable by attackers. We provided recommendations for customization and other information with honeypot operators and developers in order to counter honeypot detection. We discovered 19,208 honeypots across 637 Autonomous Systems that are trivially easy to identify. Concentrations are found in research networks, but also in enterprise, cloud and hosting networks. One cluster of honeypots was confirmed to belong to a well-known security center and was in use for ongoing attack monitoring. Concentrations in an another cluster appear to be the result of government incentives. We contacted 11 honeypot operators and received response from 4 operators, suggesting the problem of lack of network hygiene. In addition, the operator of a national research institute said that they were not aware of honeypot detection issues. Finally, we find that some honeypots are actively abused by attackers for hosting malicious binaries. We notified the owners of the detected honeypots via their network operators and provided recommendations for customization to avoid simple signature-based detection. We also shared our results with the honeypot developers.

Keywords: honeypot, honeypot detection, network scan

1. はじめに

インターネットに接続される機器は増加の一途をたどっており，Windows マシンに加え，ブロードバンドルータをはじめとする通信機器やビデオレコーダ等の家電製品，プリンタ，監視カメラ，自動車，等多くの組み込みシステムが接続されるようになった．しかし，その一方で，ネットワークサービスの脆弱性を突いてその権限を奪取するリモートエクスプロイト攻撃や脆弱なパスワードが設定されている機器への不正侵入が増加しており，インターネット上の重大な脅威となっている．実際に，ダークネットに届くパケットの統計情報を日ごとにまとめた NICTERWeb [44] によれば，2019 年 11 月現在，リモートエクスプロイト攻撃と思われる 445/tcp や 9000/tcp 番ポート宛のパケット，パスワードクラッキング攻撃と思われる 22/tcp や 23/tcp，3389/tcp 宛のパケットが数多く観測されており，様々なネットワークサービスが狙われている．

このため，脆弱なネットワークサービスを模擬する囮システム，いわゆるハニーポットを用いた攻撃の観測が行われている．ハニーポットをインターネット上に設置することで，脆弱性を狙うサイバー攻撃の観測，マルウェアの収集，侵入者の挙動の調査を行うことができる．また，従来のファイアウォールや IDS（不正侵入検知システム）のような防御システムでは観測することができなかった詳細な攻撃も観測することができるため，ハニーポットは情報セキュリティ分野における重要な基礎技術であるといえる．ハニーポットの種類は多岐にわたるが，オープンソースのハニーポットはシステム構築が容易であるため広く運用されている．実際に，様々な研究機関がインターネット上にオープンソースのハニーポットを展開しており，攻撃の観測を行っている [63]．

しかし，オープンソースのハニーポットの多くはエミュレーション技術を用いており，攻撃者がエミュレーションと実際のサービスの差異からハニーポットを検知して回避する可能性がある．実際に，ハニーポットの検知に関する研究が行われており，論文 [36] では，ハニーポットに用いられる仮想環境やデバッガを検知するアプリケーションレベルの検知手法が提案されており，論文 [14] では，TCP コネクションの特徴から検知するネットワークレベルの検知手法が提案されている．また，ハニーポットを検知するツールやサービスが公開されており [50], [52], [56], [58]，これらの中には高い拡張性を持つものも存在する．たとえば，ZMap [33] のような高速にインターネット空間をスキャンするツールに実装できるものがある [66]．ハニーポットが攻撃者に検知されてしまった場合，攻撃の実態を正確に観測できなくなる可能性がある．実際に，Linux コマンドを用いてハニーポット検知を行った攻撃の観測事例が報告されている [37]．また，後述のようにハニーポット自体が攻撃者に悪用されてしまい，セキュリティ上の脅威になる恐れがある．そのため，ハニーポットを運用する際は検知への対策を講じることが重要であるが，その対策の実態は明らかではない．

本研究では，オープンソースハニーポットの特徴的なバナー等に着目し，侵入行為を行わずに外部からハニーポットの利用状況を調査する．そして，特徴的なバナー等のカスタマイズが行われておらず，容易に検知可能なハニーポットがインターネット上に多数存在することを明らかにする．具体的には，オープンソースハニーポットの特徴的なバナー等の応答に着目してシグネチャを作成する．そして，広域ネットワークスキャンによりインターネット上に存在するハニーポットの利用状況について調査を行い，現状のハニーポット運用者のハニーポット検知に対する問題意識を明らかにする．この調査結果を受けて，検知対策を促進するためにハニーポットが集中的に発見された組織に対して直接注意喚起を行った．また，ハニーポットの開発者に対して情報提供を行った．さらに，本論文の公表により，注意喚起に対する返答がない運用者や，連絡先が特定できず直接注意喚起ができない運用者，今後オープンソースハニーポットを運用する運用者に対して，より広く注意喚起を行い，ハニーポット検知という問題が認識され，対策が促進されることを期待する．

調査では，広域ネットワークスキャンによりインターネット上に設置されている攻撃者が容易に検知可能であるバナー等の応答をカスタマイズしていないハニーポットの運用について大規模な調査を行う．具体的には，オープンソースハニーポットの特徴的な応答に着目し，これをシグネチャとして用いる．これらの特徴的な応答のほとんどは，ハニーポットの設定変更により変更が可能であるため，シグネチャベースのハニーポット検知は回避が容易であるにもかかわらず，多数のハニーポットがこのような最低限の検知対策さえ講じられていない状況であることを示す．また，実際のハニーポット運用者やハニーポットの開発者に

[1] 横浜国立大学
Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[3] デルフト工科大学
Delft University of Technology, Jaffalaan 5, 2628 BX Delft, The Netherlands
[4] 横浜国立大学大学院環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[5] 先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[a)] shun_morishita@outlook.com

The primary version of this work was presented at 2019 IFIP/IEEE IM [42].

対して連絡を行い，その実態について明らかにするとともに，ハニーポットの検知について情報提供を行った結果を述べる．

評価実験では，設定のカスタマイズを行っていない（以降では，デフォルト設定とよぶこととする）ハニーポットの特徴的な応答に着目し，14 種類のオープンソースハニーポットに対して 20 種類のシグネチャを用意した．そして，Alexa ランキングの上位 10,000 サイト，公式の FTP ミラーサーバ，実際に使用されているメールサーバ，IoT 機器の Telnet サービスに対してシグネチャを適応し，誤検知がないことを確認した．その後，Censys のスキャンデータと我々が行ったネットワークスキャンの結果に対してシグネチャを照合し，全 IPv4 空間上で，変更が可能なバナー等の応答をカスタマイズしていないまま運用されているオープンソースハニーポットを発見した．その結果，637 の AS 上で運用される 19,208 のハニーポットが容易に検知可能な状態で運用されていることが判明した．その多くが研究機関のネットワーク上で運用されていたが，企業やクラウドのネットワークでも運用されていた．また，これらのハニーポットの中には著名なセキュリティセンタで運用されているものが存在した．

さらに，シグネチャにより容易に検知されるデフォルト設定のハニーポットと，シグネチャによる検知を回避するためにカスタマイズしたハニーポットの両方を運用し，その観測結果を比較したが，現時点では観測結果に大きな差異は確認されなかった．このため，現状そのような検知やハニーポット回避が広く攻撃者によって行われている状況ではないことが分かった．しかし，変更が可能なバナー等の応答をカスタマイズしていないハニーポットは高速な広域ネットワークスキャンにより容易に検知されてしまうものであり，*Pastebin* において SSH ハニーポットのリストが実際に攻撃者の間で共有されている事例が報告されている [48]．また，評価実験で発見したハニーポットの中には，攻撃者によってマルウェアの配布に悪用されているものが存在し，ハニーポット自身がセキュリティ上の脅威になりうることが確認された．そこで，11 組織のハニーポット運用者に対して連絡をとり，ハニーポット検知の脅威について言及するとともに，ハニーポットの検知を難しくする方法を提案した．このうち，4 つの組織から返信をもらうことができた．一部の専門家は，攻撃者によるハニーポットの検知は大きな問題ではないと主張しており，これは，自身のハニーポットが大量のトラフィックを観測できているためだと思われる．しかし，変更が可能なバナー等の応答をカスタマイズしないままハニーポットを運用している場合には，攻撃者に回避され，本来観測すべきネットワークトラフィックを見逃してしまっている可能性がある．そこで，6 つのハニーポットの開発者に対して連絡を行い，ハニーポットの検知について情報提供を行った．このうち，2 人の開発者から返信を受け取った．そのうちの開発者の 1 人は我々の開示を考慮し，ハニーポットのリポジトリにカスタマイズの記述を追加した．このように，本研究はハニーポットの適切な運用に貢献していると考えられる．

本論文の構成は以下のとおりである．2 章で関連研究を紹介する．3 章では，オープンソースハニーポットの特徴的な応答に着目し，広域ネットワークスキャンによってハニーポットの運用実態を調査する．そして，4 章では，ハニーポット検知によってハニーポットの観測結果にどのような影響が出るのか調査する．5 章では，研究倫理について述べる．最後に，6 章でまとめを述べる．

2. 関連研究

ハニーポットとは，ネットワーク上で起きている攻撃を観測することを目的とした囮システムであり，脅威の分析 [4], [7], [34], [39], [53]，マルウェア検体の収集 [47], [55]，未知の攻撃の検知 [10], [49] 等を行うことができる．これまでに多数のハニーポットが開発されている．また，近年では，ハニーポットの検知やハニーポットの検知回避に関する研究が行われている．

ハニーポット：ハニーポットはその実現方法から低対話型と高対話型の 2 種類に分類することができる．高対話型ハニーポットの多くは実際のネットワークサービスを用いて構築されるため，攻撃を詳細に観測することができる．一方，低対話型ハニーポットはネットワークサービスの一部しか模擬していないため観測できる攻撃は限られるが，ハニーポットが攻撃者に乗っ取られることを防ぐことができる．低対話型ハニーポットが人気を集めており，これまでにオープンソースのハニーポットが多数公開されている．**表 1** にオープンソースのハニーポットをまとめる．ここで，Honeynet Project [63] とはネットワークに対する攻撃を調査している著名な研究機関であり，ハニーポットを開発するとともに全世界に展開している．また，このほかにも多くの開発者がハニーポットを公開している．

ハニーポット検知：ハニーポットの検知に関する研究が行われている [9], [65]．論文 [36] では仮想環境とデバッガを検知する方法が提案されており，論文 [14] では，ネットワークのレイテンシを利用した検知手法が提案されている．また，論文 [67] では，悪性トラフィックを送信することで検知する手法が提案されており，論文 [35] では，機器の証拠を収集する方法が，論文 [1] では，ネットワークの特徴をフィンガープリントした検知手法が提案されている．このように，通常のサーバとハニーポットを区別する研究が行われている．

さらに，ハニーポットを検知するためのツールが公開されている．Honeypot Hunter [56] はプロキシからハニーポットを判定するツールである．ネットワークスキャナの一種である Nmap [46] には，ハニーポットを検知するためのシ

表 1 オープンソースハニーポットと待ち受けポート（TCP）
Table 1 Open-source honeypots and listening port (TCP).

Honeypot	Version (Installed date)	Listening Port (TCP)
Kippo [25]	(08/13/2017)	22*, 2222
Cowrie [18]	1.2.0	22*, 23*, 2222, 2223
telnetlogger [29]	0.2	23
MTPot [26]	(10/18/2017)	23
Telnet IoT honeypot [28]	(09/14/2017)	23*, 2222
Glastopf [21]	3.1.3-dev	80
Shockpot [27]	(10/18/2017)	80*, 8080
Wordpot [31]	(09/14/2017)	80
HoneyThing [24]	1.0.0	80, 7547
Conpot [17]	0.5.1-default-template	80, 102, 502
Nepenthes [6]	0.2.2	21, 25, 42, 80, 110, 135, 139, 143, 220, 443, 445, 465, 993, 995, 1023, 1025, 2103, 2105, 2107, 2745, 3127, 3140, 3372, 5000, 5554, 6129, 10000, 17300, 27347
Dionaea [20]	0.1.0	21, 42, 80, 135, 443, 445, 1433, 1723, 3306, 5060, 5061
Amun [15]	0.2.3-devel	21, 23, 25, 42, 80, 105, 110, 135, 139, 143, 443, 445, 554, 587, 617, 1023, 1025, 1080, 1111, 1581, 1900, 2101, 2103, 2954, 2967, 2968, 3127, 3128, 3268, 3372, 3389, 3628, 5000, 5168, 5554, 6070, 6101, 6129, 7144, 7547, 8080, 9999, 10203, 27347, 38292, 41523
HoneyPy [23]	0.6.3-linux-profile	7*, 8*, 21*, 22*, 23*, 25*, 53*, 80*, 88*, 110*, 111*, 139*, 143*, 389*, 443*, 636*, 873*, 2049, 3306, 5432, 6000, 10007, 10008, 10021, 10022, 10023, 10025, 10053, 10080, 10088, 10110, 10111, 10139, 10143, 10389, 10443, 10636, 10873

アスタリスク（*）の付いたポート番号は，ハニーポット運用者がより多くの攻撃を観測するために，追加で設定する必要があるポートを示している．

グネチャが存在する．脆弱性スキャンツールである Metasploit [51] には，Kippo [25] を検知するためのモジュールが存在する．また，Shodan [59] が提供している Honeyscore [58] では，IP アドレス情報からハニーポットである可能性をレートとして算出している．一方で，ZMap [33] のような広域ネットワークスキャンツールを用いてハニーポットを検知する研究が行われている．論文 [66] では，9 種類のハニーポットについて，システマチックにフィンガープリントして，インターネット空間をスキャンする研究が行われている．論文 [41] では，IPv4 空間で公開されている産業制御システムを調査した研究が行われている．

ハニーポット検知の回避：ハニーポットの検知が進んでいる一方で，ステルスなハニーポットの研究開発が行われている．論文 [14] では，Honeyd [45] のコードの一部を改変し，OS に適切にパッチを当ててフィンガープリントを防ぐ研究が行われている．論文 [57] では，攻撃通信をハニーポットにリダイレクトし，攻撃でない通信と検知を試みる通信を通常のサーバにリダイレクトする研究が行われている．また，論文 [2] では，ハニーポットと実際のボットの違いを示す方法を提案し，ボットネットに加わる可能性を高める研究が，論文 [11] では，ボットネットに対してインテリジェントな応答を返すことで，より良くボットに模擬する研究が行われている．

同様に，ハニーポットの運用設定が，攻撃者の振舞いにどのような影響を与えるか調査した研究が行われている．論文 [8] では，性質の異なるハニーポットを実装することで，論文 [54] では，数学的モデルを用いてコンピュータシステムを偽のハニーポットであるかのように見せかけることで，ハニーポットに侵入してきた攻撃者の分析を行っている．

このように，ハニーポットの検知を目的とした研究が行われている．しかし，本研究では，ハニーポットの検知性能の向上を目的としておらず，ハニーポットを隠すための最小限の労力さえ費やしていない運用者がどこで，なぜそうするかを調べることを目的としている．そのため，本研究では，広域ネットワークスキャンツールを用いるとともに，インターネット空間を定期的にスキャンしたデータを公開している Censys データ [12] を用いて，シンプルかつ軽量な手法で，変更が可能なバナー等の応答をカスタマイズしていないまま運用されているオープンソースハニーポットの検知を行う．

3. ハニーポットの特徴的な応答に基づく検知

本章では，オープンソースハニーポットを対象に，広域ネットワークスキャンによってインターネット上に設置されているオープンソースハニーポットの調査を行う．はじめに，3.1 節ではハニーポットを検知するためのシグネチャの作成方法を説明する．3.2 節では作成したシグネチャの精度評価を行い，インターネット上で運用されているハニーポットの実態調査を行う．3.3 節ではハニーポットの運用組織に連絡をとり，運用者からのフィードバックについて説明する．そして，3.4 節ではハニーポットの実態調査の結果について考察する．

3.1 ハニーポットの検知に有効なシグネチャの作成

本節では，表 1 に示す 14 のオープンソースハニーポットを検知する手法を説明する．ZMap [33] のような広域ネットワークスキャンツールに実装するために，1 つのパケットで検知可能なハニーポットの特徴的な応答に着目して，ハニーポット検知用のシグネチャを作成した．

Nepenthes（FTP），Dionaea（FTP，HTTP）の 2 種類のオープンソースハニーポットを検知する 3 つのシグネチャについては，Nmap に実装されている既存のものを使用した．残りのハニーポットについては，それぞれローカル環境で実行し，スキャンすることで特徴的な応答を収集した．その結果，5 種類のハニーポットから 8 つのシグネチャを作成することができた．それ以外の 7 種類のハニーポットについては，特徴的な応答を見つけることができなかったため，ハニーポットのソースコードを調査して，9 つのシグネチャを作成した．合計で 12 種類のハニーポットから 17 つのシグネチャを作成した．既存の Nmap のシグネチャを足し合わせ，本研究では 14 種類のオープンソースハニーポットを検知する 20 のシグネチャを使用した．**表 2** にシグネチャの内容を示す．

表 2 オープンソースハニーポットのシグネチャカテゴリ
Table 2 Signature category of open-source honeypots.

Honeypot	Signature Category
Nepenthes (21/TCP, FTP)	*Banner
Dionaea (21/TCP, FTP)	*Banner
Amun (21/TCP, FTP)	Banner
Kippo (22/TCP, SSH)	Error response
Cowrie (22/TCP, SSH)	Error response
Cowrie (23/TCP, Telnet)	Banner
telnetlogger (23/TCP, Telnet)	Banner
MTPot (23/TCP, Telnet)	Banner
Telnet IoT honeypot (23/TCP, Telnet)	Banner
HoneyPy (23/TCP, Telnet)	Banner
Amun (25/TCP, SMTP)	Banner
Glastopf (80/TCP, HTTP)	HTTP response
Shockpot (80/TCP, HTTP)	HTTP response
Wordpot (80/TCP, HTTP)	HTTP response
HoneyThing (80/TCP, HTTP)	HTTP response
Conpot (80/TCP, HTTP)	HTTP response
Dionaea (80/TCP, HTTP)	*HTTP response
Amun (80/TCP, HTTP)	HTTP response
HoneyPy (80/TCP, HTTP)	HTTP response
Amun (143/TCP, IMAP)	Banner

アスタリスク（*）の付いたシグネチャは *nmap-service-probe* に登録されている既存のシグネチャを示している．

Banner：バナーはサービス接続時に表示される文字列であり，FTP，SSH，Telnet 等のサービスでバナーが表示される．Telnet サービスは多くの場合，バナーの文字列の前にネゴシエーションオプションの情報を送ってくる．簡単のため，ここではオプションの情報もバナーの一部として扱う．我々は，デフォルトのハニーポットのバナーはシグネチャとして使えるくらいユニークであることを確認した．FTP と Telnet のハニーポットのバナーを，nmap-service-probe に登録されている 694 の FTP バナーと 1,056 の Telnet バナーと比較し，いずれも一致しないことを確認した．補足すると，オープンソースであることから，検知を回避するためにハニーポットのバナーを変えることは容易である．さらに，多くの場合，設定ファイルからバナーを変更することができるため，ソースコードを変える必要すらない．

HTTP response：HTTP サービスが動いているハニーポットでは，デフォルトの HTTP レスポンスから検知するためのシグネチャを作成することができる．実際に，HTTP サービスが動いている全 8 種類のオープンソースハニーポットからユニークな応答を発見した（HTTP ヘッダのタイムスタンプ，ユニークな HTML コンテンツ，任意のリクエストに対する同一の応答）．そしてバナーと同様に，HTTP レスポンスは検知を回避するために容易に変更することができる．

Error response：あえてエラーを引き起こすリクエストを送った際に，いくつかのハニーポットはうまく対処できず，ユニークな応答を返してしまうことを確認した．たとえば，SSH の通信で実際には存在しない SSH バージョンを送った際に，いくつかのハニーポットはユニークなエラーメッセージを返してしまう．

作成したシグネチャの詳細を**表 3** に示す．表の 3 列目ではシグネチャによる検知を回避する方法を記載している．多くは設定ファイルや HTML コンテンツをカスタマイズすることにより検知を容易に回避することができる．一部はソースコードを変更する必要がある．この場合，事前にハニーポットがどのような応答を返すのか調査し，応答をカスタマイズするためにソースコードのどの部分を変更すればいいのか調査する必要がある．そのため，設定ファイルや HTML コンテンツをカスタマイズすることに比べて手間がかかる．しかし，今回作成したシグネチャの多くはバナー等のサービス接続時に返される応答に着目しており，応答を調査することは容易である．また，この特徴が表れる応答の内容をハニーポットのソースコード内で文字列検索することで，変更箇所を特定することができ，ソースコードの 1 行を変更するだけで検知を回避することができる．また，我々のシグネチャは，たった 1 つのパケットを送り，それに対する応答からハニーポットを検知することができる．そのため ZMap に実装することができ，インターネット全体を広範囲にスキャンすることができる．しかし，SSH ハニーポットの Kippo [25] と Cowrie [18] は似たようなエラーメッセージを返すため，これらを判別するためにさらなる通信が必要となる．検知の詳細なフローを**図 1** に示す．

3.2 シグネチャを用いたハニーポット検知

本節では，はじめにシグネチャの誤検知率が十分に低いことを示すために，精度評価を行う．そして，Censys [12] のスキャンデータと我々が ZMap [13], [33] で行ったスキャンデータに対してシグネチャをマッチングさせる．また，検知したハニーポットについて設置国・AS，運用期間を調査する．

(1) 精度評価

シグネチャはデフォルト設定のオープンソースハニーポットから作成したため，シグネチャがこれらのハニーポットの特徴的な応答と一致することは確認している．そのため評価が必要なのは，False Negative ではなく False Positive である．評価では，ハニーポットが含まれていないと思われる 4 つの正規サービスのデータセットに対してシグネチャをマッチングさせて評価した．

Alexa ランキング：ハニーポットでない可能性が高い Alexa ランキング [3] の上位 10,000 サイトを評価に使用した．10,000 ドメインに対して正引きを実行し，8,744 のユニークな IP アドレスを取得した．そして，これらの IP アドレスに対してスキャンを実施し，我々が作成した 20 のシグネチャとマッチングさせた．ポートの開閉状況を次に記載する．Alexa ランキングは Web サイトのランキングであるため，ほとんどは HTTP が動いていた（8,581）．また，FTP では 749，SSH では 1,128，Telnet では 53，SMTP

表 3 オープンソースハニーポットのシグネチャ
Table 3 Signatures of open-source honeypots.

Honeypot	Signature Category	Modified Method	Input Data	Response
Nepenthes (21/TCP, FTP) (Nmap)	Banner	Source Code †	NULL	220 ---freeFTPd 1\.0---warFTPd 1\.65---\r\n
Dionaea (21/TCP, FTP) (Nmap)	Banner	Source Code †	NULL	220 Welcome to the ftp service\r\n
Amun (21/TCP, FTP)	Banner	Setting File	NULL	220 Welcome to my FTP Server\r\n
Cowrie (23/TCP, Telnet)	Banner	Setting File	NULL	\xff\xfd\x1flogin:
telnetlogger (23/TCP, Telnet)	Banner	Source Code †	NULL	\xff\xfb\x03\xff\xfb\x01\xff\xfd\x1f\xff\xfd\x18\r\nlogin:
MTPot (23/TCP, Telnet)	Banner	Source Code †	NULL	\xff\xfb\x01\xff\xfb\x03\xff\xfc'\xff\xfe\x01\xff\xfd\x03\xff\xfe\"\xff\xfd'\xff\xfd\x18\xff\xfe\x1fUsername:
Telnet IoT honeypot (23/TCP, Telnet)	Banner	Source Code †	\r\n\r\n	\xff\xfd\x01Login: Password: \r\nWelcome to EmbyLinux 3\.13\.0-24-generic\r\n #
HoneyPy (23/TCP, Telnet)	Banner	Setting File	NULL	Debian GNU/Linux 7\r\nLogin:
Amun (25/TCP, SMTP)	Banner	Setting File	NULL	220 mail\.example\.com SMTP Mailserver\r\n
Glastopf (80/TCP, HTTP)	HTTP response	HTML Content	GET / HTTP/1.0\r\n\r\n	Blog Comments \n <label for=\"comment\">Please post your comments for the blog</label>\n \n <textarea name=\"comment\" id=\"comment\" rows=\"4\" columns=\"300\"></textarea>\n \n <input type=\"submit\" name=\"submit\" id=\"submit_comment\" value=\"Submit\" />\n
Shockpot (80/TCP, HTTP)	HTTP response	Setting File	GET /nsE/2m9/hK9/fOy HTTP/1.0\r\n\r\n	<html><body> It Works! \n This is the default web page for this server\. \n The web server software is running but no content has been added, yet\. \n</body></html>\n
Wordpot (80/TCP, HTTP)	HTTP response	HTML Content	GET /wp-login.php ?action=lostpassword HTTP/1.1\r\n\r\n	<input type=\"hidden\" name=\"testcookie\" value=\"1\" />\n\t \n</form>\n\n<p id=\"nav\">\nLost your password\?
HoneyThing (80/TCP, HTTP)	HTTP response	HTML Content	GET /Forms/login_security _1.html HTTP/1.0\r\n\r\n	<SCRIPT language=\"JavaScript\">\nif\(document\.Login_Form\.tipsFlag\.value == 1\)\nvar infoStr='Username or Password is incorrect, please try again\.';\ndocument\.getElementById\(\"tr1\"\)\.innerHTML = infoStr;\nelse if\(document\.Login_Form\.tipsFlag\.value == 2\)\ntimelast = document\.Login_Form\.timevalue\.value;\nwindow\.setInterval\(\"IncreaseSec\(\) \", 1000\);\n\n</SCRIPT>\n
Conpot (80/TCP, HTTP)	HTTP response	Setting File	GET /index.html HTTP/1.0\r\n\r\n	Last-Modified: Tue, 19 May 1993 09:00:00 GMT
Dionaea (80/TCP, HTTP) (Nmap)	HTTP response	HTML Content	GET / HTTP/1.0\r\n\r\n	<!DOCTYPE html PUBLIC \"-//W3C//DTD HTML 3\.2 Final//EN\"><html>\n<title> Directory listing for /</title>\n<body>\n Directory listing for / \n
Amun (80/TCP, HTTP)	HTTP response	Setting File	GET / HTTP/1.0\r\n\r\n	<!DOCTYPE HTML PUBLIC \"-//IETF//DTD HTML 2\.0//EN\"><html><head><title>It works!</title></head><html><body> It works! tim\.bohn@gmx\.net johan83@freenet\.de</body></html>\n\n
HoneyPy (80/TCP, HTTP)	HTTP response	Setting File	GET / HTTP/1.0\r\n\r\n	Server: Apache/2\.4\.10 \(Debian\)\nConnection: close\nContent-Type: text/html\n\nOK!\n
Amun (143/TCP, IMAP)	Banner	Setting File	\r\n\r\n	a001 OK LOGIN completed

いくつかのシグネチャは正規のサーバの応答のように見えるが，実際には正規のものではない．たとえば，Debian 7.0 の telnetd のデフォルトのバナーは“`Debian GNU/Linux 7\r\ndebian login:`”だが，HoneyPy の“`Debian GNU/Linux 7\r\nLogin:`”のバナーとは異なる．

† 1 行の修正のみで検知回避可能

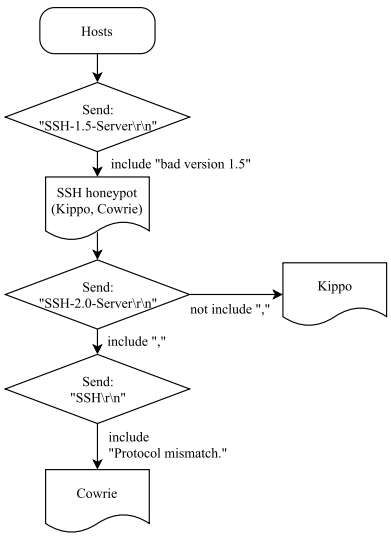


図 1 SSH ハニーポット判別のフロー
Fig. 1 Flow of SSH honeypot distinction.

では 841，IMAP では 557 のポートが開いていた．調査の結果，いずれもシグネチャと一致する応答がなく，False Positive がないことを確認した．

公式の FTP ミラーサーバ：FTP ハニーポットのシグネチャを評価するために，Ubuntu [64]，Apache [61]，CentOS [62] の公式の FTP ミラーサーバを評価に使用した．こちらもハニーポットが含まれていない可能性が高い．299 の Ubuntu のドメイン，119 の Apache のドメイン，258 の CentOS のドメインから，531 のユニークな FTP サーバのドメインを取得し，正引きした結果，457 の IP アドレスを取得した．そして，スキャンを実施し，シグネチャと一致しないことを確認した．また前述のとおり，Nmap に登録されている 694 の FTP サービスのバナーと，ハニーポットの FTP バナーが一致しないことも確認している．

大学の E メールドメイン：SMTP と IMAP のハニーポットのシグネチャを評価するために，大学の E メールドメインを評価に使用した．GitHub リポジトリ [30] から大学のドメインを取得し，正引きから対応する MX レコードを取得した．その結果，SMTP サービスが開いている 6,463 のユニークな IP アドレスと IMAP サービスが開いている 1,683 のユニークな IP アドレスを取得した．そして，スキャンを実施し，どの IP アドレスに対しても False Positive がないことを確認した．

IoT 機器の Telnet サービス：他のサービスとは異なり，Telnet サービスは通常グローバルで使われるサービスではない．しかし，多くの IP カメラやルータのような IoT 機器で Telnet が動いている [5]．調査では，4 種類のルータと 2 種類のネットワークストレージの計 6 種類の IoT 機器の Telnet サービスを調査した．その結果，我々のシグネチャは 6 種類の機器に対して，False Positive が発生しな

表 4 Censys と我々のスキャンデータを用いたハニーポットの検知結果
Table 4 Honeypot detection result using censys and our own scan data.

Honeypot signature	# Honeypots (Censys)	# Honeypots (Censys+Scan)	# Honeypots (Censys+Scan)	Survival Ratio	# Honeypots (Bitter Harvest)
Nepenthes (21/TCP, FTP) (Nmap)	**124**	-	119	96.0%	-
Dionaea (21/TCP, FTP) (Nmap)	**1,751**	-	1,324	75.6%	-
Amun (21/TCP, FTP)	**1,720**	-	745	43.3%	-
Cowrie (23/TCP, Telnet)	**1,796**	-	570	31.7%	938
telnetlogger (23/TCP, Telnet)	**2,984**	-	32	1.1%	-
MTPot (23/TCP, Telnet)	**226**	-	98	43.4%	216
HoneyPy (23/TCP, Telnet)	**2**	-	1	50.0%	-
Amun (25/TCP, SMTP)	**1,608**	-	430	26.7%	-
Glastopf (80/TCP, HTTP)	**2,487**	-	1,154	46.4%	3,371
Conpot (80/TCP, HTTP)	**89**	-	51	57.3%	87
Dionaea (80/TCP, HTTP) (Nmap)	**2,220**	-	569	25.6%	202
Amun (80/TCP, HTTP)	**944**	-	544	57.6%	-
HoneyPy (80/TCP, HTTP)	**19**	-	10	52.6%	-
Amun (143/TCP, IMAP)	**1,728**	-	686	39.7%	-
Kippo (22/TCP, SSH)	-	**505**	-	-	758
Cowrie (22/TCP, SSH)	-	**998**	-	-	2,021
Telnet IoT honeypot (23/TCP, Telnet)	-	**0**	-	-	11
Shockpot (80/TCP, HTTP)	-	**1**	-	-	-
Wordpot (80/TCP, HTTP)	-	**6**	-	-	-
HoneyThing (80/TCP, HTTP)	-	**0**	-	-	-
telnet-password-honeypot (23/TCP, Telnet)	-	-	-	-	1
Total	**17,698**	**1,510**	6,333	35.8%	7,605

かった．そして，Nmap に登録されている 1,056 の Telnet サービスのバナーと，ハニーポットの Telnet バナーが一致しないことも確認している．

(2) 実態調査

続いて，全 IPv4 空間のスキャンデータを用いて，変更が可能なバナー等の応答をカスタマイズしていないオープンソースハニーポットの実態調査を行った．我々で ZMap を用いて全世界のスキャンを行うことも可能だったが，Censys データを用いることにした．その理由として，Censys は ZMap と ZGrab [32] を用いた過去のスキャン結果を格納しており，我々で自らスキャンする必要がないからである．

調査では，2018 年 4 月 9 日から 2018 年 4 月 15 日の Censys データを用いた．サービスごとに開いているホストの数は次のとおりである．21/tcp（FTP）が 16.2M，23/tcp（Telnet）が 8.4M，25/tcp（SMTP）が 13.6M，80/tcp（HTTP）が 64.6M，143/tcp（IMAP）が 9.1M．作成した 20 シグネチャの内 14 シグネチャは，追加でスキャンする必要がなく，Censys データから直接マッチングさせることができる．残りの 6 シグネチャについては，Censys データから直接マッチングさせることができず，はじめに Censys データからより一般的なシグネチャを作成して候補となるホスト群を抽出し，その候補に対して ZMap を用いてスキャンを行った．我々が行ったスキャンの時期（2018 年 5 月 19 日）が Censys のスキャンの 1 カ月後であるため，一部のハニーポットは IP アドレスの変動によって，検知できなくなっている可能性がある．そのため，時間経過による変動を測るために，すでに 14 シグネチャで検知されたハニーポットについても 1 カ月後にスキャンを行った．

表 4 に検知結果を示す．1 列目がハニーポットのシグネチャ，2 列目が Censys データから検知されたハニーポットの数，3 列目が Censys データから抽出した候補のホスト群に対して我々がスキャンして検知したハニーポットの数，4 列目が Censys スキャンの 1 カ月後に我々がスキャンして検知したハニーポットの数，5 列目が 1 カ月後のハニーポットの生存率を示している．結果，14 シグネチャで Censys データから 17,698 のハニーポットを検知した．多くの検知されたハニーポットは，telnetlogger の 2,984 ホスト，Glastopf の 2,487 ホスト，Dionaea の 2,220 ホストだった．Censys データと我々のスキャン結果で検知した残りの 6 シグネチャについては，1,510 のハニーポットを検知した．多く検知されたのは，Cowrie の 998 ホストと Kippo の 505 ホストだった．合計すると，14 種類のオープンソースハニーポットについて 19,208 のハニーポットを検知した．参考として表 4 に関連研究 [66] で行われたオープンソースハニーポット検知実験の結果を示す．関連研究と本研究では調査期間が 1 カ月以上ずれているうえ，本研究では運用の詳細が明らかでない外部システムである Censys のスキャン結果を用いているため，厳密な比較は難しいが，いずれの結果も一定数のオープンソースハニーポットが実際に運用されていることを示している．

Censys データで検知された 17,698 のハニーポットについて，再スキャンした結果，6,333（35.8%）のハニーポットが 1 カ月後も運用されていた．ほとんどのハニーポットは，1 カ月後でもある程度運用されていたが，例外として，3,000 近く運用されていた telnetlogger ハニーポットのほとんどが 1 カ月後には消滅していた．そのすべてがフランスの研究機関の IP アドレスレンジで運用されていたものだった．

表 5 インターネット上でよく観測された FTP バナー
Table 5 Frequently observed FTP banner on the Internet.

Rank	IP	Ratio	Banner
1	5,436,627	33.5%	-
2	800,771	4.93%	220 Microsoft FTP Service\r\n
3	518,558	3.19%	220 FTP Server ready.\r\n
4	343,316	2.11%	220 (vsFTPd 2.2.2)\r\n
5	216,232	1.33%	220 Ftp firmware update utility
6	205,967	1.27%	220 (vsFTPd 3.0.2)\r\n
7	141,608	0.872%	220 FTP service ready.\r\n
8	119,395	0.736%	220 Serv-U FTP Server v6.4 for WinSock ready... \r\n
9	118,699	0.731%	220-Microsoft FTP Service\r\n
10	85,602	0.527%	220 (vsFTPd 3.0.3)\r\n
⋮	⋮	⋮	⋮
228	1,751	0.0108%	**Dionaea banner**
232	1,720	0.0106%	**Amun banner**
3,358	124	0.0008%	**Nepenthes banner**
Total	16,232,733	100%	

表 6 インターネット上でよく観測された Telnet バナー
Table 6 Frequently observed Telnet banner on the Internet.

Rank	IP	Ratio	Banner
1	4,651,675	28.7%	-
2	176,908	2.09%	{"banner":"\r\n\r\nUser Access Verification\r\n \r\nUsername: ","will":[{"name":"Echo","value" :1},{"name":"Suppress Go Ahead","value":3}],"do" :[{"name":"Terminal Type","value":24},{"name": "Negotiate About Window Size","value":31}]}
3	120,561	1.43%	{"banner":"\r\n%connection closed by remote host !\u0000"}
4	102,623	1.21%	{"banner":"\r\r\n(none) login: ","will":[{"name" :"Echo","value":1},{"name":"Suppress Go Ahead", "value":3}],"do":[{"name":"Echo","value":1},{ "name":"Negotiate About Window Size","value" :31}]}
5	100,768	1.19%	{"banner":"\r\n\r\nUser Access Verification\r\n \r\nPassword: ","will":[{"name":"Echo","value" :1},{"name":"Suppress Go Ahead","value":3}],"do" :[{"name":"Terminal Type","value":24},{"name": "Negotiate About Window Size","value":31}]}
6	86,023	1.02%	{"banner":"\r\nWelcome Visiting Huawei Home Gateway\r\nCopyright by Huawei Technologies Co. , Ltd.\r\n\r\nLogin:","will":[{"name":"Echo", "value":1},{"name":"Suppress Go Ahead","value" :3},{"name":"Terminal Type","value":24}]}
7	64,764	0.767%	{"banner":"\r\r\n(none) login: ","will":[{"name" :"Echo","value":1},{"name":"Suppress Go Ahead", "value":3}],"do":[{"name":"Echo","value":1},{ "name":"Negotiate About Window Size","value":31} ,{"name":"Remote Flow Control","value":33}]}
8	53,498	0.633%	{"banner":"\n\r\n\r\rAccount:","will":[{"name": "Echo","value":1}],"do":[{"name":"Terminal Type" ,"value":24}]}
9	41,949	0.497%	{"banner":"\r\nlogin: ","will":[{"name":"Echo", "value":1},{"name":"Suppress Go Ahead","value" :3}]}
10	39,792	0.245%	{"banner":"\r\nAccount:","will":[{"name":"Echo", "value":1}],"do":[{"name":"Terminal Type","value" :24}]}
⋮	⋮	⋮	⋮
189	2,984	0.0353%	**telnetlogger banner**
261	1,793	0.0212%	**Cowrie banner**
1,080	214	0.00253%	**MTPot banner**
52,984	2	0.0000237%	**HoneyPy banner**
Total	16,232,733	100%	

FTP と Telnet のハニーポットのバナーと Censys で観測された全バナーと比較した．**表 5** と**表 6** に，ハニーポットのバナーがインターネット上であまり利用されていないことを示す．このことから，バナーはハニーポットを検出するためのシグネチャに利用することができる．また，バナーをインターネット上でよく使われるバナーに変えるだけで，簡単な検知回避の方法となりうる．

表 7 ハニーポットの AS，国，ネットワークタイプ
Table 7 AS, country and network type of honeypot population.

19,208 Honeypots (unique 13,417 IPs)					
IP	**AS Country**	**AS Type**	**IP per /16**	**AS Country**	**AS Type**
2,697	France	*Academic*	390.0	Mexico	*Academic*
783	Mexico	*Academic*	253.1	Taiwan	*ISP*
771	United States	*Hosting*	249.0	Greece	*Academic*
696	Taiwan	*ISP*	203.4	Taiwan	*ISP*
653	Japan	*Academic*	129.6	Japan	*Academic*
606	Taiwan	*ISP*	79.0	Taiwan	*ISP*
510	Italy	*Academic*	77.2	France	*Academic*
464	Taiwan	*ISP*	61.7	Taiwan	*ISP*
450	United States	*Hosting*	56.9	Taiwan	*Academic*
436	Taiwan	*Academic*	45.9	Sweden	*ISP and Hosting*
314	France	*Hosting*	41.1	France	*Academic*
277	Taiwan	*ISP*	21.2	United States	*Hosting*
271	Taiwan	*ISP*	20.0	Taiwan	*Academic*
249	Greece	*Academic*	19.8	Sweden	*Hosting*
247	France	*Academic*	18.8	Taiwan	*Academic*
187	Taiwan	*ISP*	18.4	Taiwan	*ISP*
171	United States	*Hosting*	15.9	Taiwan	*ISP*
154	Romania	*Other*	13.5	Taiwan	*ISP*
149	United States	*Hosting*	13.2	United States	*Hosting*
134	Taiwan	*ISP*	12.6	Taiwan	*ISP*

(3) 設置国・AS

検知されたハニーポットについて，GeoIP2 ISP Database [40] を用いて AS を取得し，ipinfo.io [38] で国情報を取得した．**表 7** に IP アドレスが多かった上位 20 の AS，AS の国名，AS の種類を示す．AS の種類については，手動で 4 種類に分類した．また，それぞれの AS が保有する IP アドレス数に対するハニーポットの割合を計算することで，相対的なハニーポットの密度を調査した．AS ごとに保有 IP アドレス数が異なるため，/16（65,536IP アドレス）あたりのハニーポットの数を計算し，比較した．/16 以下の AS は除外し，表 7 に/16 あたりでハニーポットの数が多かった上位 20 の AS も示す．AS の種類については，大学や研究機関を “*Academic*”，インターネット接続サービスを提供している会社を “*ISP*”，サーバ（共有サーバ，専有サーバ，VPS，クラウドサービス等）の貸し出しを行う会社を “*Hosting*”，それ以外の会社（金融会社，旅行代理店等）を “*Other*” と分類した．結果から，上位のいくつかの AS は大学や研究機関のものであることが判明した．運用されている国・地域については，台湾の AS が多く，上位 20AS のうち 8AS を占めていた．

(4) 運用期間

ハニーポットの運用期間を割り出すために，1 年近くの Censys の過去データ（2017 年 8 月 8 日～2018 年 7 月 17 日）を分析した．**図 2** に，AS ごとに 1 年間検知されたハニーポット数を示す．特定の AS での大きな変動を除き，検知されたハニーポットの数は安定している．たとえば，2017 年 11 月にアイルランドの研究機関のネットワーク（AS1）で 4,383 のハニーポットが運用開始されたが，次の月にそのすべてが運用終了していた．その他の大きな変動として，2017 年 12 月にアメリカの ISP（AS2）で 6,917 のハニーポットが運用終了していた．**図 3** に，2017 年 8 月 8

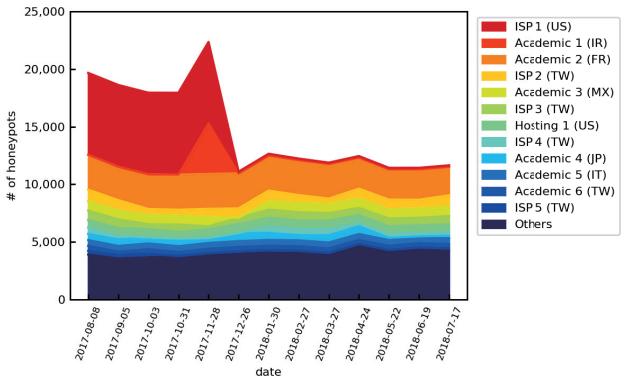


図 2 1 年間のハニーポットの検知数
Fig. 2 # of detected honeypots in one year.

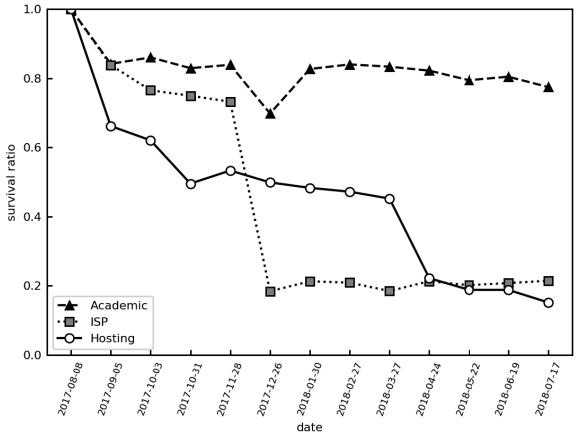


図 3 2017 年 8 月 8 日に検知したハニーポットの生存期間
Fig. 3 Survival time of honeypots detected on August 8, 2017.

日に検知されたハニーポットの生存率を示す．ハニーポットの平均の運用期間は 200.42 日（SD=127.54）だった．運用期間がネットワークの種類ごとに異なるか調査するために，10IP アドレス以上存在した 53 の AS を選定し，手動で *Academic*，*ISP*，*Hosting* に分類した．その結果，2017 年 8 月で *Academic* は 5,553，*ISP* は 11,390，*Hosting* は 1,455 のハニーポットを検知した．特に，研究機関のネットワークのハニーポットの 80%は 1 年後も運用されていた．ISP やホスティングのネットワークのハニーポットは比較的運用期間が短かったが，それでも 20%のハニーポットが 1 年後にも運用されていた．2017 年 12 月に ISP で大きく割合が落ちているのは，アメリカの ISP のハニーポットがいっせいに運用終了したことが原因である．そして，2018 年 4 月にホスティングの割合が落ちているのは，アメリカのホスティングサービスでいっせいに運用終了したことが原因である．

(5) 悪用事例

Springall らによる先行研究 [60] では，アノニマス FTP サーバが攻撃者によってマルウェアのアップロードや配布に悪用されていることが報告されている．本調査でも，21 の FTP ハニーポットが攻撃者によって悪用されていると思われることを発見した．これらのハニーポットにはマルウェアがアップロードされていて，他のホストからダウンロード可能になっていた．VirusTotal を用いてアップロードされていたマルウェアを分類した．54 のマルウェア（17 のユニークなマルウェア）を収集し，内訳は次のとおりだった．12 の CoinMiner，2 の Downloader，2 の Backdoor，1 の Ransomware．これは，攻撃者が侵入したホストにマルウェアをダウンロードさせたい場合に，ダウンロードサーバとして使用されるシナリオに合致する．また，21 の悪用されたハニーポットには似たような名前のファイルがアップロードされており，同一の攻撃者が悪用していた可能性がある．

3.3 運用者からのフィードバック

多数の応答をカスタマイズしていないハニーポットを発見したが，容易に検知可能なハニーポットが運用されていることは望ましくない．このため，ハニーポットが検知された IP アドレスから WHOIS を用いて管理組織名を特定し，その中でハニーポットが集中的に発見された管理組織を対象に，Web サイトに記載されているメールアドレス，または，WHOIS に記載されているメールアドレスに連絡した．また，本来ハニーポットは攻撃を観測するための囮のシステムであるため，運用者はハニーポットの存在を隠そうとすることが考えられる．しかし，一部のハニーポットを運用するプロジェクトでは，ハニーポットで観測された攻撃の情報を共有するために，レポートとして Web 上でハニーポットの運用情報を公開している場合がある．ここでは，検知したハニーポットの種類と Web 上の公開情報に記載されているハニーポットの種類を比較し，管理組織がハニーポットプロジェクトへ参画している可能性があると思われる場合に，該当するプロジェクトの窓口メールアドレスにも連絡した．合計すると 11 組織のハニーポットの運用者に連絡をとり，本研究の概要や意義を説明し，ハニーポット検知の脅威について注意喚起を行い，シグネチャベースの検知を回避するためのカスタマイズを推奨した．また，検知された IP アドレスが実際にハニーポットとして使われているか確認し，容易に検知可能なバナー等の応答をカスタマイズしていないハニーポットを運用した理由を訪ねた．返信がなかった 7 つの組織については，そもそもハニーポットプロジェクトに参加していない可能性や連絡したメールアドレスが誤っていた可能性も考えられるが，今回連絡したメールアドレスからはエラーメールも返ってきていないため，連絡したメールアドレスについては有効である可能性がある．そして，我々が連絡したハニーポットプロジェクトの Web 上の公開情報を確認すると，ハニーポットの運用情報は我々が連絡する数年前に公開されているものであり，ハニーポットが長期間にわたって運用されている可能性がある．さらに，ハニーポットに

は数百ものIPアドレスが割り当てられており，大きなコストをかけて運用されているハニーポットプロジェクトである可能性が高い．それにもかかわらず，ハニーポットが容易に検知される状態で運用されており，また，注意喚起への返信を行わなかったことから，ネットワークやハニーポットの管理に十分な注意が払われていないものと予想される．以降では，返信があった4つの組織について説明する．

ある商用のISPからの返信により，我々が示したIPアドレスが実際にハニーポットとして使われていることが確認できた．そのISPでは，未使用のアドレススペースの一部を世界的に有名なセキュリティ組織の脅威監視センタに一時的にルーティングしていた．そして，そのISPの紹介によりセキュリティセンタの最高技術責任者（Chief Technical Officer）にハニーポットの応答をカスタマイズしないまま運用している理由を訪ねたところ，“攻撃者による検知は大きな問題ではない”という回答が得られた．

ある国立研究機関のネットワークの運用者からの返信で，我々がそのネットワークのいくつかのハニーポットを正しく特定できていることが確認できた．そのうちの1つは，研究者によりサイバー攻撃監視を目的に使われていることが分かった．もう1つは，非営利のインターネットセキュリティ組織の脅威監視に使われていた．そのほかについては，大学にアドレススペースが割り当てられているものだった．

他の国立の研究機関のネットワークの運用者からの返信で，我々がそのネットワークのいくつかのハニーポットを正しく特定できていることが確認できた．彼らはハニーポット検知の問題を認識していなかったが，より高度な攻撃を観測するために，他の種類のハニーポット（高対話型ハニーポット）も併用していることに言及した．

台湾の大学の研究者からの返信で，様々な組織でハニーポットの運用を奨励するための政府が支援する一連のサイバーセキュリティプロジェクトが存在し，それが台湾に集中している原因である可能性があることが分かった．

3.4 考察

ハニーポットは本来，通常のサーバのように見せかけているため，これを発見するのは困難であることが予想される．我々の手法で，応答をカスタマイズしていないハニーポットを容易に特定できる場合があることが明らかになったが，適切に設定されており，単純な方法では検知が難しいハニーポットも存在すると思われる．たとえば，我々が調査した14種類のオープンソースハニーポットの中で，Conpotの開発者はカスタマイズの方法を当該ハニーポットの関連ドキュメント内で説明している（HTTPヘッダや応答のレイテンシ等）．応答をカスタマイズしていないConpotを多く発見できなかったのは，これが一因であると思われる．

インターネット上で運用されるハニーポットの設置国やASを調査したところ，研究機関のネットワークで多く運用されていたことから，これらがトレーニング目的や学生の研究プロジェクトによるものである可能性が考えられる．しかし，これらのハニーポットには表7に示したように，何百ものIPアドレスが割り当てられている場合も多い．このことから，学生のプロジェクトというよりも，学術的な調査や実用的な攻撃監視に用いられている可能性が高い．また，調査ではホスティングやISPのような商用の環境で運用されているものも発見しており，台湾の様々なネットワークでも多く発見されている．そのため，これらのハニーポットが運用上の機能や価値があることは明らかである．より正確な知見を得るために，いくつかハニーポット運用者に連絡をとった．11組織に連絡をとったところ，7組織から返信がなかったが，返信がないこと自体が，ネットワークやハニーポットの管理に十分な注意が払われていないことを暗示しているといえる．4組織から返信があり，いずれもハニーポットが実際にサイバー攻撃の観測に用いられていることが確認できた．一部の専門家は，攻撃者によるハニーポットの検知は大きな問題ではないと主張しており，これは，自身のハニーポットが大量のトラフィックを観測できているためだと思われる．しかし，応答をカスタマイズしないままハニーポットを運用している場合には，攻撃者に回避され，本来観測すべきネットワークトラフィックを見逃してしまっている可能性がある．

また，ハニーポットの運用期間を調査したところ，特に，研究機関のネットワークのハニーポットの80%は1年後も同じIPアドレス上で運用されていることが判明し，ISPやホスティングのネットワークのハニーポットは比較的運用期間が短かったが，それでも20%のハニーポットが1年後にも運用されていることが判明した．このことから，これらのハニーポットは検知やブラックリストの対象になる可能性が高い．さらに，ハニーポットが攻撃者によって悪用されていると思われるものを発見していることから，設定が不適切なハニーポットは，ハニーポット自体がセキュリティの脅威になる可能性があることが分かる．

4. ハニーポット検知による観測結果への影響の調査

3章の調査結果から，多数のハニーポットがインターネット上で検知可能な状態で運用されていることが明らかになった．本章では，ハニーポットの検知によって，ハニーポットの観測内容に対してどのような影響を及ぼすのかについて調査する．調査の対象は，後述のとおり，すでに検知ツールが存在するオープンソースハニーポットとした．

表 8 ハニーポットの運用内容
Table 8 Information of honeypots operation.

Honeypot	Customized Point	Period	# Total Packets (96IPs)	# Daily Packets (96IPs)
Kippo (22/TCP, SSH)	Banner (24IPs), Error response (24IPs)	2019/01/26 - 2019/05/17 (98days)	154,634,442	1,577,902
Dionaea (21/TCP, FTP)	Banner	2019/01/26 - 2019/05/17 (98days)	3,186,678	32,517
Dionaea (80/TCP, HTTP)	HTTP header and Top page	2019/01/26 - 2019/05/17 (98days)	35,936,968	366,704
Dionaea (445/TCP, SMB)	SMB negotiate protocol response OemDomainName and ServerName	2019/01/26 - 2019/05/17 (98days)	297,072,159	3,031,349
Dionaea (1433/TCP, MSSQL)	Pre-login TDS package	2019/01/26 - 2019/05/17 (98days)	23,493,927	239,733
Cowrie (23/TCP, Telnet)	Negotiation option	2019/05/03 - 2019/05/17 (15days)	22,231,782	1,482,119
Cowrie (2222/TCP, SSH)	Banner (24IPs), Error response (24IPs)	2019/05/03 - 2019/05/17 (15days)	175,010	11,667

ログが収集できなかった期間：2019/02/07-2019/02/08，2019/02/21-2019/03/04.

表 9 ハニーポット検知ツールのシグネチャ
Table 9 Signatures of honeypot detection tools.

Detection Tool	Service	Honeypot
checkpot, detect-kippo-cowrie honeybee, Metasploit	SSH	Kippo
detect-kippo-cowrie	SSH	Kippo
detect-kippo-cowrie	SSH	Kippo, Cowrie
Nmap	SMB	Dionaea
Nmap	MSSQL	Dionaea

表 10 サービススキャンの送信元 AS
Table 10 Service scan source AS.

# IP	ASN	AS name
108	AS63949	Linode, LLC
8	AS200651	Flokinet Ltd
4	AS32748	Steadfast
4	AS14061	DigitalOcean, LLC
2	AS4808	China Unicom Beijing Province Network
2	AS17621	China Unicom Shanghai network
2	AS16509	Amazon.com, Inc.

4.1 実験内容

ハニーポット検知の影響を調査するために，実験では 2 種類のハニーポットを運用する．具体的には，検知されやすいデフォルト設定のハニーポットと一部の特徴をカスタマイズしたハニーポットを運用し，その観測結果を比較する．実験環境は，大学のアドレスレンジ内で，それぞれ 48 の IP アドレスをハニーポットに割り当て，計 96 の IP アドレスを割り当てた．観測結果の差異がカスタマイズによることを示すために，結果に影響が出る可能性がある他の要因は排除する必要がある．そのため，ハニーポットはすべて同一の/16 のアドレスレンジ内に配置し，IP アドレスはランダムな順番で割り当てた．さらに，検知に影響するカスタマイズした箇所以外の設定については，同一の設定でハニーポットを運用した．

表 8 に本実験のハニーポットの運用内容を示す．1 列目にハニーポットの種類，2 列目にカスタマイズした箇所，3 列目に運用期間，4 列目に全ハニーポットで観測したパケット数，5 列目に 1 日あたりのパケット数を記載した．ハニーポットは，既存の検知ツールで検知可能なハニーポットを使用した．そして，カスタマイズは既存ツールの検知を回避できる最小限のカスタマイズを行った．例外として，Kippo と Cowrie の SSH サービスについては，エラー応答（Error response）とバナーのカスタマイズを行った 2 種類のカスタマイズハニーポットを運用した（それぞれ 24 の IP アドレスを割り当てた）．既存ツールではいずれもエラー応答をもとにハニーポットを検知するが，Kippo と Cowrie で使われているデフォルトのバナーは古く，通常のサーバでよく使われるバナーではないため，バナーをカスタマイズしたハニーポットも運用した．

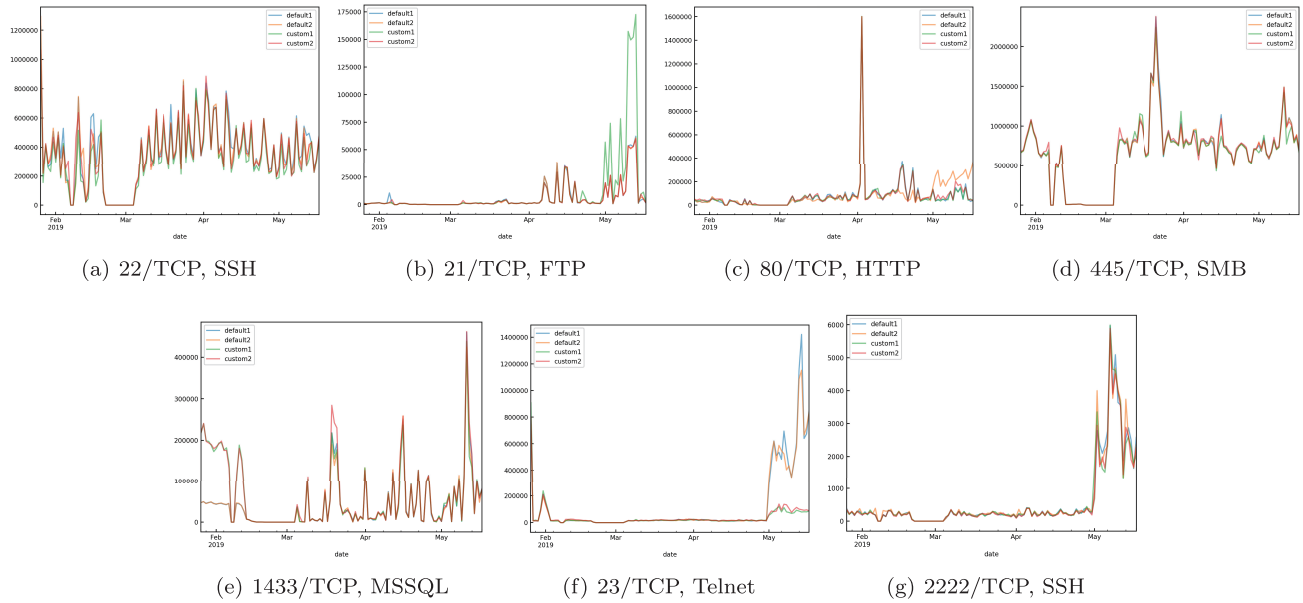
4.2 事前実験

デフォルト設定のハニーポットとカスタマイズしたハニーポットの観測結果を比較する前に，既存ツールを用いたハニーポット検知が行われているか調査した．調査方法としては，ハニーポット検知ツールの通信を事前に調査して，ツールを特定するためのシグネチャを作成する．そして，ハニーポットで観測した通信に対してシグネチャをマッチングさせることで，検知ツールの通信が存在したかどうか調査する．**表 9** に作成した検知ツールのシグネチャを示す．checkpot [16], detect-kippo-cowrie [19], honeybee [22], Kippo SSH Honeypot Detector（Metasploit）[50]，Nmap Service Scan [46] の 5 種類の検知ツールを特定する 5 種類のシグネチャを作成した．

検知ツールを特定するシグネチャとハニーポットの通信を比較した結果，SSH ハニーポットを検知するツールの通信（checkpot, detect-kippo-cowrie, honeybee, Metasploit）は観測されなかった．しかし，Nmap の SMB サービスと一致する通信は全運用期間で 1,134 パケット観測し，Nmap の MSSQL サービスと一致する通信は 967 パケット観測した．いずれも Dionaea を検知する Nmap のサービススキャンの通信だった．観測した計 2,101 パケットは 144 のユニークな IP アドレスからの通信であり，このサービススキャンを行ってきた AS を調査した．上位の AS を**表 10** に示す．表からも分かるように，サービススキャンを行ってきた大多数がアメリカの VPS を提供する Linode からの通信であることを確認した．

4.3 実験結果

本節では，デフォルト設定のハニーポット（48IP）で観



(a) 22/TCP, SSH (b) 21/TCP, FTP (c) 80/TCP, HTTP (d) 445/TCP, SMB

(e) 1433/TCP, MSSQL (f) 23/TCP, Telnet (g) 2222/TCP, SSH

図 4 パケット数
Fig. 4 # of packets.

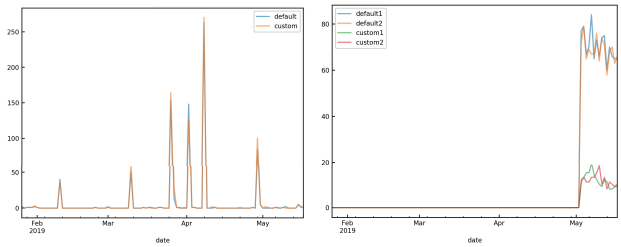
測した攻撃の通信とカスタマイズしたハニーポット（48IP）で観測した攻撃の通信を比較する．それぞれさらに 2 つのグループに分割し，*default1*・*default2*・*custom1*・*custom2* の 4 グループ（各 24IP）で観測した結果を比較した．SSH サービスについては，バナーとエラー応答の 2 種類のカスタマイズを行っており，*custom1* がバナーをカスタマイズしたハニーポット，*custom2* がエラー応答をカスタマイズしたハニーポットに対応している．

(1) パケット数

図 4 に各サービスごとの総パケット数の推移を記載する．図 4 (b)（FTP サービス）では，5 月に *custom1* のパケット数が多く観測されているが，特定の IP アドレスに集中して大量のパケットが送られてきていたことが原因で，設定の差異によるものではなかった．図 4 (c)（HTTP サービス）の 5 月の *default2* もパケット数が多くなっているが，同様の原因だった．

図 4 (e)（MSSQL サービス）から，運用開始後から 2 月上旬の期間で，パケット数に差が出ていることが分かる．通信の内容を見ると，pre-login TDS package の値（カスタマイズした箇所）を取得した後に通信内容が変化する攻撃が存在することが原因だった．具体的には，値をカスタマイズした場合には値の取得後に接続が切れ，その後同じ攻撃者から何度も同様の通信が行われた（15 回程度）．そのため，カスタマイズしたハニーポットの方がパケット数が多くなっていた．

図 4 (f)（Telnet サービス）では，5 月の運用開始後から，カスタマイズしたハニーポットの方が受信パケット数が少ない．カスタマイズしたハニーポットでは検知されないようにネゴシエーションオプションを削除しており，オプションを設定しないとその後の挙動を観測できない攻撃が存在することが原因だった（2019 年 1 月 27 日以降の公式の Cowrie（`commit cdc8038529c43e7dc673812e1f1e1e864ae1236b`）では，Nmap による検知を回避するために，ネゴシエーションオプションを削除している）．



(a) Dionaea (b) Cowrie

図 5 マルウェア数
Fig. 5 # of malwares.

(2) マルウェア数

図 5 に Dionaea と Cowrie の収集マルウェア数の推移を記載する．Kippo ではマルウェアを収集することができなかった．その原因としては，Kippo に実装されているコマンドが少なく，パイプやリダイレクトも使用できないことが原因だと思われる．

図からも分かるように，Dionaea ではパケット数と同様にデフォルト設定のハニーポットとカスタマイズしたハニーポットとで収集マルウェア数に明確な差は確認できなかった．Cowrie ではカスタマイズしたハニーポットの方が収集マルウェア数が少なく，同様にオプションを設定していないことが原因である．

4.4 考察

前述の調査では，はじめに，攻撃者が既存の検知ツールを用いてハニーポットの検知を試みているか調査した．その結果，Nmap のサービススキャンのシグネチャと一致する通信を複数観測した．しかし，Nmap のサービススキャンは本来ホストのサービスを特定するためのスキャンであるため，今回の結果だけでは，攻撃者が意図してハニーポットの検知を試みようとしたのか，単にサービスを特定しようとしたのか不明である．しかし，サービススキャンは比較的実行に時間がかかるスキャンであるため，少なくとも，コストをかけて攻撃先のホストのサービスの種類を特定しようとする攻撃者が存在することは明らかになった．そして，このサービススキャンを実行した攻撃者には，デフォルト設定のハニーポットはハニーポットであると露見してしまう．

次に，デフォルト設定のハニーポットとカスタマイズしたハニーポットの観測結果を比較した．その結果，一部のサービスでは攻撃に違いが現れ，Dionaea の MSSQL サービスでは，パラメータの違いによって，攻撃が変化することがあった．また，Cowrie の Telnet サービスでは，ハニーポットの特徴を消したカスタマイズしたハニーポットの方でパケット数・収集マルウェア数が激減した．その原因は，Telnet サービスに対する攻撃の大多数を占める Mirai の挙動が原因であることが判明した．Mirai のソースコードを確認したところ，サーバ側にオプションが設定されていない場合に，その時点で攻撃が停止することが分かった．そのため，オプションの設定を削除したカスタマイズしたハニーポットでは，攻撃が減少した．当初は，検知されにくくするためにカスタマイズすることによって攻撃の観測数が向上すると想定していたが，ほとんどのサービスで大きな違いは見られなかった．このことから，今回着目したハニーポットの特徴については，観測結果に明確な差が現れるほど大規模なハニーポットの検知は行われていないと予想される．3 章で示したように，高速な広域ネットワークスキャンにより応答をカスタマイズしていないハニーポットは容易に検知されてしまうものである．しかし，現状そのような検知やハニーポット回避が広く攻撃者によって行われている状況ではないことが明らかになった．

5. 研究倫理

ハニーポットの実態を明らかにするという点で，我々の研究は攻撃的な研究という一面を持ち，本論文を公表することにより攻撃者がハニーポット検知の可能性を認識する恐れがある．しかし，既存研究においてハニーポット検知に関する研究が取り組まれており，また，実際にハニーポットを検知するツールやサービスが公開されているため，本論文の公開の悪影響は限定的と考える．そして，ハニーポットのバナー等の応答を調査したり，その特徴からシンプルなシグネチャを作成することは高い技術力を必要とせずに実施できることであり，当然，攻撃者にも実施可能である．そのため，この問題を広く研究者に周知し，検知対策を促進することの意義は，前述の悪影響よりも十分に大きいと考え本論文で調査結果を公開することとした．ただし，研究倫理的な理由から，個別のハニーポットを言及する際に，AS 名と IP アドレスを記載しなかった．

また本論文の開示に先立ち，可能な限りハニーポット運用者であると想定される主体に通知を行うとともに，Github に連絡先が記載されていた 6 のハニーポット開発者（Conpot，Glastopf，Cowrie，MTPot，Shockpot，telnetlogger）に連絡をとり，彼らに我々の結果の概要と手法の詳細を伝えた．その後，Conpot と Glastopf に関わる 2 人の開発者から返信を受け取った．そのうちの 1 人（Lukas Rist）は両方のハニーポットに関わっており，我々の開示を考慮して，Glastopf のリポジトリにハニーポット設定のカスタマイズに関する記述を追加した．Conpot については，すでにドキュメント内にカスタマイズに関するセクション [43] がある．当該開発者は，検知可能性は低対話型ハニーポット固有のものだが，デフォルト設定のハニーポットは攻撃者がさらに容易に検知可能であるとも述べた．そのため，彼らはハニーポットを配置する際に，カスタマイズを推奨している．また，攻撃者がリアルかエミュレートか判別するタイミングを特定することで，運用者がハニーポット検知に対処できるようになると言及している．

また，攻撃者に悪用されていたハニーポットを運用していたネットワークの運用者にも連絡をとり，その結果，ハニーポット内にホスティングされていたマルウェアファイルはいずれも削除されている．具体的には，3 種類の異なる方法（Web サイトに記載されているメールアドレス，Web サイトにある連絡フォーム，WHOIS に記載されているメールアドレス）でそれぞれの運用者に連絡をとり，彼らのハニーポットによって引き起こされる潜在的な脅威と検知されにくくなる方法について提案した．

関連研究ではすでに，適切にハニーポットを設定する方法について提案されている [9]．ここでは，さらにオープンソースハニーポットの運用者に対する運用上の推奨を補足する．

(1) FTP，Telnet，SMTP，IMAP サービスが動いているオープンソースハニーポットについては，デフォルトのバナーが一般のバナーと異なることがある．検知を回避するには，バナーをインターネット上で実際によく使われているバナーに変更することが有効だと考えられる．上位 10 の FTP と Telnet のバナーを表 5 と表 6 に示している．他のサービスについても，同様に Censys データから調査することができる．そして，ほとんどのハニーポットはバナーを設定ファイルから変更することができる．

(2) HTTP サービスが動いているオープンソースハニーポットについては，デフォルトの Web コンテンツがユニークであることがあり，ハニーポット検知に利用できる可能性がある（HTTP ヘッダのタイムスタンプ，ユニークな HTML コンテンツ，任意のリクエストに対する同一の応答）．ほとんどのハニーポットは HTML ファイルが規定のディレクトリに格納されており，Web コンテンツを変更可能である．

(3) SSH サービスが動いているオープンソースハニーポットについては，あえてエラーを引き起こすリクエストをうまく対処できていないことがある．これについては，ソースコードを修正する必要があり，他の場合に比べて修正することが難しい可能性がある．

6. まとめ

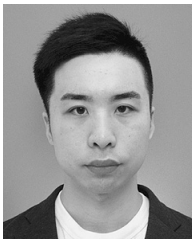
本研究では，単純なシグネチャによりインターネット上で運用される 19,000 以上の変更が可能なバナー等の応答をカスタマイズしていないハニーポットを発見した．その多くが研究機関のネットワークで運用されていたが，企業やクラウドのネットワークでも運用されていた．運用されている国については，台湾のネットワークで多く発見された．11 組織のハニーポット運用者に連絡をとったが，4 つの組織からしか返答をもらうことができず，ネットワークやハニーポットの管理に十分な注意が払われていない可能性がある．実際に，一部のハニーポット運用者はハニーポット検知の問題を認識していなかったことが明らかになった．また，検知されたハニーポットの一部には，攻撃者によってマルウェアの配布悪用されているものが存在した．

謝辞 本研究成果の一部は，国立研究開発法人情報通信研究機構（NICT）の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」の支援により得られた．

参考文献

[1] Aguirre-Anaya, E., Gallegos-Garcia, G., Solano Luna, N. and Villa Vargas, L.A.: A New Procedure to Detect Low Interaction Honeypots, *International Journal of Electrical and Computer Engineering*, pp.848–857 (2014).
[2] Al-Hakbani, M.M. and Dahshan, M.H.: Avoiding honeypot detection in peer-to-peer botnets, *IEEE International Conference on Engineering and Technology*, *ICETECH'15* (2015).
[3] Alexa: Alexa, available from ⟨https://www.alexa.com/⟩.
[4] Anagnostakis, K.G., Sidiroglou, S., Akritidis, P., Xinidis, K., Markatos, E. and Keromytis, A.D.: Detecting Targeted Attacks Using Shadow Honeypots, *Proc. 14th USENIX Security Symposium*, *SSYM'05* (2005).
[5] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al.: Understanding the mirai botnet, *USENIX Security Symposium* (2017).
[6] Baecher, P., Koetter, M., Holz, T., Dornseif, M. and Freiling, F.: The nepenthes platform: An efficient approach to collect malware, *International Workshop on Recent Advances in Intrusion Detection*, Springer, pp.165–184 (2006).
[7] Bar, A., Shapira, B., Rokach, L. and Unger, M.: Identifying Attack Propagation Patterns in Honeypots using Markov Chains Modeling and Complex Networks Analysis, *IEEE International Conference on Software Science, Technology and Engineering*, *SWSTE'16* (2016).
[8] Barron, T. and Nikiforakis, N.: Picky Attackers: Quantifying the Role of System Properties on Intruder Behavior, *Proc. 33rd Annual Computer Security Applications Conference*, *ACSAC'17* (2017).
[9] Blackhat: Breaking Honeypots for Fun and Profit, available from ⟨https://www.blackhat.com/us-15/briefing.html#breaking-honeypots-for-fun-and-profit⟩.
[10] Chamotra, S., Sehgal, R.K. and Misra, R.S.: Honeypot Baselining for Zero Day Attack Detection, *International Journal of Information Security and Privacy*, pp.63–74 (2017).
[11] Costarella, C., Chung, S., Endicott-Popovsky, B. and Dittrich, D.: Hardening honeynets against honeypot-aware botnet attacks, *International Conference on Cloud Security and Management*, *ICCSM'15* (2015).
[12] Durumeric, Z., Adrian, D., Mirian, A., Bailey, M. and Halderman, J.A.: A Search Engine Backed by Internet-Wide Scanning, *Proc. 22nd ACM SIGSAC Conference on Computer and Communications Security*, *CCS'15* (2015).
[13] Durumeric, Z., Wustrow, E. and Halderman, J.A.: ZMap: Fast Internet-wide Scanning and Its Security Applications, *Proc. 22nd USENIX Security Symposium*, *USENIX'13* (2013).
[14] Fu, X., Yu, W., Cheng, D., Tan, X., Streff, K. and Graham, S.: On recognizing virtual honeypots and countermeasures, *Proc. 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, *DASC'06* (2006).
[15] GitHub: Amun, available from ⟨https://github.com/zeroq/amun⟩.
[16] GitHub: checkpot, available from ⟨https://github.com/vladalexgit/checkpot⟩.
[17] GitHub: Conpot, available from ⟨https://github.com/mushorg/conpot⟩.
[18] GitHub: Cowrie, available from ⟨https://github.com/micheloosterhof/cowrie⟩.
[19] GitHub: detect-kippo-cowrie, available from ⟨https://github.com/blazeinfosec/detect-kippo-cowrie⟩.
[20] GitHub: Dionaea, available from ⟨https://github.com/rep/dionaea⟩.
[21] GitHub: Glastopf, available from ⟨https://github.com/mushorg/glastopf⟩.
[22] GitHub: honeybee, available from ⟨https://github.com/mohitrajain/honeybee⟩.
[23] GitHub: HoneyPy, available from ⟨https://github.com/foospidy/HoneyPy⟩.
[24] GitHub: HoneyThing, available from ⟨https://github.com/omererdem/honeything⟩.
[25] GitHub: Kippo, available from ⟨https://github.com/desaster/kippo⟩.
[26] GitHub: MTPot, available from ⟨https://github.com/Cymmetria/MTPot⟩.
[27] Github: Shockpot, available from ⟨https://github.com/threatstream/shockpot⟩.
[28] GitHub: Telnet IoT honeypot, available from ⟨https://github.com/Phype/telnet-iot-honeypot⟩.
[29] GitHub: telnetlogger, available from ⟨https://github.

com/robertdavidgraham/telnetlogger⟩.
[30] Github: University Domains and Names Data List & API, available from ⟨https://github.com/Hipo/university-domains-list⟩.
[31] GitHub: Wordpot, available from ⟨https://github.com/gbrindisi/wordpot⟩.
[32] Github: ZGrab, available from ⟨https://github.com/zmap/zgrab⟩.
[33] Github: ZMap, available from ⟨https://github.com/zmap/zmap⟩.
[34] Goseva-Popstojanova, K., Anastasovski, G., Dimitrijevikj, A., Pantev, R. and Miller, B.: Characterization and classification of malicious Web traffic, *Computers & Security*, pp.92–115 (2014).
[35] Hayatle, O., Youssef, A. and Otrok, H.: Dempster-shafer evidence combining for (anti)-honeypot technologies, *Information Security Journal: A Global Perspective*, Vol.21, No.6, pp.306–316 (2012).
[36] Holz, T. and Raynal, F.: Detecting honeypots and other suspicious environments, *Proc. 6th IEEE Information Assurance Workshop*, *IAW'05* (2005).
[37] IIJ: Internet Infrastructure Review (IIR) Vol.36, available from ⟨https://www.iij.ad.jp/dev/report/iir/036/02.html⟩.
[38] ipinfo.io: ipinfo.io: IP Address API and Data Solutions - geolocation, company, carrier info, type and more, available from ⟨https://ipinfo.io/⟩.
[39] Kramer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K. and Rossow, C.: AmpPot: Honeypot for Monitoring Amplification DDoS Attack, *Proc. 18th International Symposium on Research in Attacks, Intrusions and Defenses*, *RAID'15* (2015).
[40] MaxMind: GeoIP2 ISP Database, available from ⟨https://www.maxmind.com/en/geoip2-isp-database⟩.
[41] Mirian, A., Ma, Z., Adrian, D., Tischer, M., Chuenchujit, T., Yardley, T., Berthier, R., Mason, J., Durumeric, Z., Halderman, Alex, J. and Bailey, M.: An Internet-wide view of ICS devices, *14th Annual Conference on Privacy, Security and Trust*, *PST'16* (2016).
[42] Morishita, S., Hoizumi, T., Ueno, W., Tanabe, R., Gañán, C., van Eeten, M.J., Yoshioka, K. and Matsumoto, T.: Detect Me If You... Oh Wait. An Internet-Wide View of Self-Revealing Honeypots, *2019 IFIP/IEEE Symposium on Integrated Network and Service Management* (*IM*), pp.134–143, IEEE (2019).
[43] mushorg: Conpot's documentation, available from ⟨https://conpot.readthedocs.io/en/latest/⟩.
[44] NICT: NICTERWEB 2.0, available from ⟨https://www.nicter.jp/⟩.
[45] Niels Provos: Honeyd Virtual Honeypot, available from ⟨http://www.honeyd.org/⟩.
[46] Nmap.Org: Nmap: the Network Mapper - Free Security Scanner, available from ⟨https://nmap.org/⟩.
[47] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, *Proc. 9th USENIX Conference on Offensive Technologies*, *WOOT'15* (2015).
[48] Pastebin: ssh honeypot lists – Pastebin, available from ⟨https://pastebin.com/N2FUYg1x⟩.
[49] Patel, R.R. and Thaker, C.S.: Zero-Day Attack Signatures Detection Using Honeypot, *Proc. International Conference on Computer Communication and Networks*, *COMNET'11* (2011).
[50] Rapid7: Kippo SSH Honeypot Detector, available from ⟨https://www.rapid7.com/db/modules/-auxiliary/scanner/ssh/detect_kippo⟩.
[51] Rapid7: Metasploit: Penetration Testing Software, Pen Testing Security, available from ⟨https://www.metasploit.com/⟩.
[52] Rapid7: Shodan Honeyscore Client, available from ⟨https://www.rapid7.com/db/modules/-auxiliary/gather/shodan_honeyscore⟩.
[53] Roberto Tanara: Dionaea honeypot: from Conficker to WannaCry + SambaCry CVE 2017-7494, available from ⟨https://www.honeynet.org/node/1353⟩.
[54] Rowe, N.C., Duong, B.T. and Custy, E.J.: Fake Honeypots: A Defensive Tactic for Cyberspace, *Proc. 7th IEEE Information Assurance Workshop*, *IAW'06* (2006).
[55] Ryan Barnett: New Bot Malware (BoSSaBoTv2) Attacking Web Servers Discovered, available from ⟨https://www.trustwave.com/Resources/SpiderLabs-Blog/-Honeypot-Alert--New-Bot-Malware-(BoSSaBoTv2)-Attacking-Web-Servers-Discovered/⟩.
[56] Send-Safe: Send-Safe Honeypot Hunter, available from ⟨http://www.send-safe.com/honeypot-hunter.html⟩.
[57] Shiue, L.-M. and Kao, S.-J.: Countermeasure for detection of honeypot deployment, *International Conference on Computer and Communication Engineering*, *ICCCE'08* (2008).
[58] Shodan: Honeyscore, available from ⟨https://honeyscore.shodan.io/⟩.
[59] Shodan: Shodan, available from ⟨https://www.shodan.io/⟩.
[60] Springall, D., Durumeric, Z. and Halderman, J.A.: FTP: The forgotten cloud, *International Conference on 46th Annual IEEE/IFIP Dependable Systems and Networks*, *DSN'16* (2016).
[61] The Apache Software Foundation: The status of all apache mirrors, available from ⟨https://www.apache.org/mirrors/⟩.
[62] The CentOS Project: List of CentOS Mirrors, available from ⟨https://www.centos.org/download/mirrors/⟩.
[63] The Honeynet Project: About The Honeynet Project, available from ⟨https://www.honeynet.org/about⟩.
[64] Ubuntu: Official Archive Mirrors for Ubuntu, available from ⟨https://launchpad.net/ubuntu/+archivemirrors⟩.
[65] Uitto, J., Rauti, S., Laurén, S. and Leppänen, V.: A Survey on Anti-honeypot and Anti-introspection Methods, *World Conference on Information Systems and Technologies*, *WorldCIST'17* (2017).
[66] Vetterl, A. and Clayton, R.: Bitter Harvest: Systematically Fingerprinting Low- and Medium-interaction Honeypots at Internet Scale, *12th USENIX Workshop on Offensive Technologies*, *WOOT'18* (2018).
[67] Wang, P., Wu, L., Cunningham, R. and Zou, C.C.: Honeypot detection in advanced botnet attacks, *International Journal of Information and Computer Security*, pp.30–51 (2010).



森下 瞬

2020 年 3 月横浜国立大学大学院環境情報学府情報環境専攻博士課程前期修了．修士（情報学）．同年 4 月株式会社インターネットイニシアティブ（IIJ）入社．在学中，ネットワークセキュリティに関する研究に従事．

上野 航

2019 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期修了．修士（工学）．同年 4 月 NTT コミュニケーションズ株式会社入社．在学中，情報セキュリティに関する研究に従事．

田辺 瑠偉 （正会員）

2017 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（情報学）．同年 4 月横浜国立大学大学院環境情報研究院で産学官連携研究員．2018 年 4 月より横浜国立大学先端科学高等研究院特任教員（助教）．情報セキュリティ，特にネットワークセキュリティの研究に従事．2017 年情報処理学会山下記念研究賞受賞．

カルロス ガニャン

アーヘンのフィリップス研究室でワイヤレスセンサネットワークの安全性とセキュリティに関する研究に従事し，2008 年に修士号を取得．その後，モバイルアドホックネットワークにおける映像配信の安全性に関する研究に従事，2010 年にテレマティックスの分野で修士号を取得．さらに，2012 年に自動車向けアドホックネットワークに関する研究により博士号を取得．2020 年現在，デルフト工科大学サイバーセキュリティ経済学グループ准教授．IoT，スマートシティのサイバーセキュリティ，データサイエンスの研究に取り組み，特に持続可能な社会を実現するためのコネクテッド製品・サービスのセキュリティ研究に従事．

ミシェル ファン イートゥン

デルフト工科大学教授．サイバーセキュリティを専門とし，特に大規模インターネット調査とインシデントデータ分析により，インターネットサービス業界のセキュリティリスクへの対応を分析する研究に従事．これまで ITU，OECD，欧州委員会，オランダ政府の研究プロジェクトとして，マルウェアの経済学，サイバー犯罪の影響分析，ボットネットと悪質なホスティングサービスを軽減させるための ISP の役割の分析に従事．オランダ政府サイバーセキュリティ評議会会員．

吉岡 克成 （正会員）

2005 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（工学）．同年 4 月独立行政法人情報通信研究機構で研究員として勤務．2007 年 12 月横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011 年 4 月横浜国立大学大学院環境情報研究院准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009 年文部科学大臣表彰・科学技術賞（研究部門），2016 年産学官連携功労者表彰総務大臣賞，2017 年情報セキュリティ文化賞をそれぞれ受賞．

松本 勉 （正会員）

1986 年東京大学大学院工学系研究科電子工学専攻博士課程修了．工学博士．同年横浜国立大学勤務．現在，同大学・環境情報研究院教授および先端科学高等研究院情報・物理セキュリティ研究ユニット主任研究者および産業技術総合研究所サイバーフィジカルセキュリティ研究センター長．CRYPTREC 暗号技術検討会座長，日本学術会議連携会員を兼任．情報・物理セキュリティの研究教育に 1981 年より従事．この間，日本銀行金融研究所客員研究員，独カールスルーエ大学客員教授，日本学術振興会学術システム研究センター専門研究員，国際暗号学会 IACR 理事等を歴任．暗号学国際会議 ASIACRYPT，電子情報通信学会暗号と情報セキュリティシンポジウム SCIS，バイオメトリクス研究専門委員会，ハードウェアセキュリティ研究専門委員会等の創設に貢献．電子情報通信学会業績賞，第 5 回ドコモ・モバイル・サイエンス賞，第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞等受賞．