能動的観測と受動的観測の融合によるサイバーセキュリティ情報の収集と分析

吉岡克成[1,2]，インミンパパ[1]，鈴木将吾[1]，渡邉直紀[1]，中山颯[3]，志村俊也[2,4]，徐浩源[2,4]，
四方順司[1,2]，松本勉[1,2]，中尾康二[2,5,6]，針生剛男[2,7]，岩村誠[2,7]，八木毅[2,7]，秋山満昭[2,7]，
寺田真敏[2,8]，島成佳[2,9]，渡部正文[2,9]，角丸貴洋[2,9]，川北将[9]，山田正弘[2,10]，井上大介[5]

[1]横浜国立大学環境情報研究院，[2]横浜国立大学先端科学高等研究院，[3]横浜国立大学理工学部
[4]横浜国立大学情報基盤センター，[5]情報通信研究機構 [6]KDDI 株式会社，[7]日本電信電話株式会社，
[8]株式会社日立製作所，[9]日本電気株式会社 [10]株式会社富士通研究所

あらまし サイバー攻撃に関連した活動の広域的な把握手段として，国内では一部の例外を除いてハニーポットやダークネット観測といった受動的観測が主流であるが，海外ではグローバルスキャン等により積極的な能動的観測を行い，情報収集分析を行う研究事例が多い．そこで能動的観測と受動的観測の融合により，インターネット上のサイバー攻撃の実態とインターネットからアクセス可能なシステム・デバイスの状況を迅速に把握し，同時にマルウェアなどの脅威や脆弱性の詳細分析を行うことで，サイバーセキュリティ関連情報の統合的な情報収集・分析を行う仕組みを提案する．さらに，能動的観測と受動的観測の融合が有効的に働く例を示す．

Collection and Analysis of Cyber Security Data by Active and Passive Monitoring

Katsunari Yoshioka[1,2], Yinminpapa[1], Shogo Suzuki[1], Naoki Watanabe[1], Sou Nakayama[3], Toshiya Shimura[2,4]
Haoyuan Xu[2,4], Junji Shikata[1,2], Tsutomu Matsumoto[1,2], Koji Nakao[2,5,6], Takeo Hariu[2,7], Makoto Iwamura[2,7]
Takeshi Yagi[2,7], Mitsuaki Akiyama[2,7], Masato Terada[2,8], Shigeyoshi Shima[2,9], Masafumi Watanabe[2,9]
Takahiro Kakumaru[2,9], Masaru Kawakita[9], Masahiro Yamada[2,10], Daisuke Inoue[5]

[1]Graduate School of Environment and Information Sciences, [2]Institute of Advanced Science
[3]College of Engineering Science, [4]Information Technology Service Center, Yokohama National University
[5]National Institute of Information and Communications Technology, [6]KDDI Corporation, [7]NTT Corporation
[8]Hitachi, Ltd, [9]NEC Corporation, [10]FUJITSU LABORATORIES LTD.

Abstract In Japan, passive monitoring such as darknet monitoring and honeypot deployment has been the major approach to monitor and analyze cyber attacks in large-scale although active monitoring such as Internet-wide scan is more widely utilized and enhancing the situation awareness in International research activities. We propose a framework of cyber security data collection and analysis by utilizing active and passive monitoring as well as analysis of related malware and vulnerabilities. Finally, we show a few example cases where such combination of monitoring methodologies provide deeper insights of the situation.

1　はじめに

サイバー攻撃に関連した活動の広域的な把握手段として，国内では一部の例外を除いてハニーポットやダークネット観測といった受動的観測が主流であるが，海外ではグローバルスキャンにより積極的な能動的観測を行い，情報収集と分析を行う研究事例が多い．

そこで本稿では，能動的観測と受動的観測の融合により，インターネット上のサイバー攻撃の実態とインターネットからアクセス可能なシステム・デバイスの状況を迅速に把握し，同時に関連マルウェアなどの脅威や脆弱性の詳細分析を行うことで，サイバーセキュリティ関連情報の統合的な情報収集・分析を行う仕組みを提案する．さらに，インターネット接続されたIoTデバイスと産業制御システムについて，能動的観測と受動的観測の融合が有効的に働く例を示す．

2　受動的観測

本稿では，観測対象に向けて能動的に行われるサイバー攻撃を観測する手法を受動的観測と呼ぶこととする．一般に受動的観測は，既に構築された実運用中のシステムにおいて攻撃を観測する場合と，観測のためのシステムを構築する場合に分けられる．観測のためのシステムを構築する例として，未使用の IP アドレス帯へ届く通信を観測するダークネット観測が国内外で広く行われている[1-4]．また，これらの IP アドレス帯にセキュリティ上脆弱なシステムや脆弱なシステムを模擬するプログラム(ハニーポット)を囮として動作させることで攻撃を観測する方法が広く採用されている [5-7]．想定する攻撃に応じて，囮として模擬するシステム，サービス，データの種類，規模は大きく異なり，Windows クライアント，Web サーバ・アプリケーション・DB[8, 9], SSH サーバ[10], SIP サーバ[11], DR-DOS に悪用されるサービス[12], 産業制御システム[13, 14], IoT デバイス[15]を模擬するハニーポットが存在する．また，上記のようなシステムやサービスに限らず，不正メール収集用の囮メールアカウント，各種サービスの不正利用等を観測するための囮アカウントやデータ[16, 17]等もサイバー攻撃情報収集に用いられる．

攻撃判別の問題　正規通信と攻撃通信が混在する実運用システムを観測する際は，侵入検知システム等のセキュリティアプライアンスやブラックリストにより攻撃の識別を行った上で分析を行うが未知の攻撃への対応や大量の誤検知の問題がある．ダークネット観測では，従来，観測される通信を異常な通信，主に攻撃と捉えて分析が行われていたが，近年，超高速スキャナ[18]の開発やセキュリティプロジェクト[33]による探索が増加しており[15, 31]，攻撃と調査目的の通信の識別はサイバー攻撃状況把握において重要な課題となっている．

観測効率向上の工夫　受動的観測は，その性質から攻撃を受けなければ観測が行えない．そのため，検索エンジンを使用して目標を探索する攻撃者を観測・誘引する方法[19]，マルウェアを動作させた環境に囮の認証情報[17]や囮メールアカウント情報等を用意しこれを故意に漏洩させる方法，攻撃者が利用することが予想される Web サイトやメーリングリスト等にハニーポットの情報を掲載する方法[14]等がある．また，外部からの攻撃を待つのではなく，保有しているマルウェア検体を解析環境で実行しその挙動を観測する動的解析も広く行われている．

観測能力の向上　攻撃者が囮システムに侵入した後の行動を長期的に観測する場合，囮システムは観測対象のシステムを高い精度で模擬しなければならない．特に標的型攻撃等，人間の攻撃者が深く関わるサイバー攻撃については，囮システムのリアリティが要求される．

3　能動的観測

能動的観測の代表的な手法としてクライアントハニーポットがある．クライアントハニーポットは，脆弱な Web クライアント，または，それを模擬したシステムにより検査対象の Web サイトに

アクセスし，攻撃の発生の有無を確認することで悪性サイトを検知・分析する技術である．また，アクティブプローブにより悪性サーバやマルウェア感染ホストを探索する能動的観測手法が提案されている[20]．

一般的に対象ホストの状態を探索・調査する方法としてネットワークスキャンが広く行われており，代表的なツールとして Nmap[21]がある．近年，全 IPv4 アドレスを 5 分以内でスキャン可能な超高速スキャナとして Zmap[18] や masscan[22]が提案され，その後，ダークネットにおいて観測される Zmap や masscan によるスキャンが増加している[12]．また，近年，インターネットに接続される機会が増加している組み込み機器等の IoT デバイスや制御システム等も検知の対象としてスキャンを行い，その結果を提供する Shodan[23]のようなサービスが注目を集めている．

より積極的な能動的観測手法として、調査対象に規格外のデータを送信することでソフトウェアの不具合を検出するファジングや、擬似的な攻撃を行うことで調査対象のセキュリティ状態を確認するペネトレーションテストが存在する．

上記とは異なる能動的観測として Android アプリのマーケットクローラや特定の Web サービス，特に SNS 等の情報を収集する SNS クローラなどがある．

法と倫理 能動的観測は受動的観測に比べて積極的に観測対象にアクセスし情報収集を行うため，不正アクセス等の法律的，倫理的問題を充分に考慮する必要がある．Zmap の開発元であるミシガン大学は Scanning Best Practice [24]を公開し，研究目的のスキャンを行う場合の注意点を示している．

4 観測の連携

4.1 複数の観測結果の複合的利用

文献[25]では能動的観測と受動的観測を含めた多様な観測結果を多角的に組み合わせたマルチモーダル分析により，異なる種類のサイバー攻撃間の隠れた関連性を明らかにしている．また，上記以外にも多様なデータにもとづき総合的にサイバー攻撃の脅威を分析する手法は多く提案されている[26, 2]．文献[27]では，このように複数の情報源を用いた統合的分析を行う際の注意点として，観測方法の一貫性や観測内容粒度，一定の観測期間が必要であると説明している．

4.2 有機的な連携

独立に収集した観測結果を用いて分析を行うだけでなく，それぞれの観測結果を他の観測結果にフィードバックしたり，互いに連携しつつ観測精度を上げる試みがなされている．文献[17]ではドライブバイダウンロード攻撃によるクライアントマシンへの侵入，クライアントマシンにおけるWebサーバの管理者権限（FTPサーバの認証情報）の探索・取得，Webサーバの改ざん，さらなるWebクライアントへの攻撃，といった攻撃のサイクルに着目し，マルウェア動的解析における囮アカウント情報の漏洩，囮アカウント情報に誘引されたWebサーバハニーポットへの攻撃の観測，Webサーバハニーポットにおいて観測された悪性URLへのクライアントハニーポットによる探索等を行い，攻撃の観測の効率化に成功している．文献[28, 15]ではダークネットやハニーポットに届くパケットの送信元アドレスに対してHTTPやTelnetを用いて接続を行い，得られる情報から当該アドレスで動作するシステムやデバイスを推定している．このように有機的な連携により，より意義のある多角的な情報収集が可能となるといえる．

5　能動的観測と受動的観測の融合による統合的なサイバー攻撃情報収集と分析

本章では，4.2 節で説明した受動的観測，能動的観測の有機的連携をさらに活性化し，統合的なサイバー攻撃情報を収集・分析する仕組みを提案する．収集・蓄積した情報はサイバーセキュリティ研究において利用することや外部へ情報提供することを想定している．

5.1　構成

提案するサイバー攻撃情報収集分析機構の構成図を図 1 に示す．

受動的観測機構　ダークネット観測やハニーポットにより攻撃を観測する機能や既存のネットワークへの攻撃を観測する機能を実現する．特に Windows クライアント，Web サーバ・アプリケーション・DB, SSH サーバ, DR-DOS に悪用されるサービス，産業制御システム，IoT デバイスといった様々な観測対象を模擬するハニーポットを並行運用する．

能動的観測機構　アクセス先の機器やシステム，その構成を推定するスキャナや，悪性サーバやマルウェア感染ホストを検出するアクティブプローブ[20]，クライアントハニーポット機能を実現する．また脆弱性探索が可能なスキャナも適用を検討する．

データ分析・蓄積・制御機構　能動的観測機構，受動的観測機構で観測されたデータの詳細分析，例えば，マルウェア解析などを行い，これらを蓄積・検索する機能を有する．また，外部連携組織への情報提供，外部連携組織からの情報取り込みのインターフェイスとして働く．外部連携組織とのやり取りでは適切なアクセス制御を行う．

機構間の連携　受動的観測機構と能動的観測機構は密接に連携することで有益な情報を効率的に取得する．例えば，ハニーポットやダークネットにおいて攻撃が観測された場合，攻撃元に対して能動的観測を行うことで攻撃ホストに関する付加的な情報を取得できる．また，能動的観測により攻撃元の性質を特定した後，当該ホストからの攻撃に対して受動的観測機構が有する多様なハニーポット群から適切な種別のハニーポットを割り当てることで効率的に攻撃を観測できる可能性がある．また，データ分析・蓄積・制御機構において解析されたマルウェアの接続先（C&C サーバ等）に対して能動的スキャンを行い，当該ホストの情報収集を行うといった連携が考えられる．

外部組織との連携　受動的観測，能動的観測，データ分析・蓄積はいずれも既に多くの研究組織やプロジェクトにおいて実施されている．これらと積極的なデータ共有を進めることで観測範囲を拡大することができる．例えば，NICTER [2], PREDICT [29], Internet Wide Scan Project [33], DNSDB [30], ShadowServer [31], Shodan [23], VirusTotal [32], MWS [34], CAIDA [35]をはじめとする国内外の研究機関・プロジェクト・イベント・サービスとの連携を検討する．

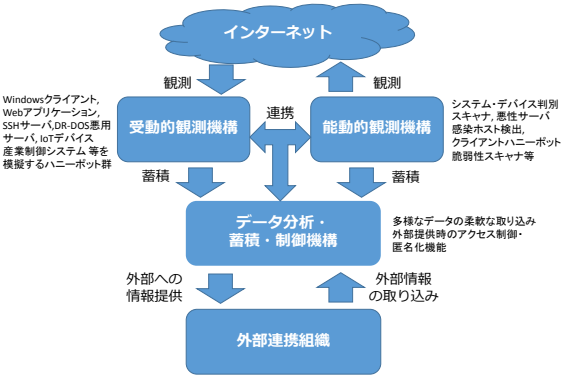

図 1. 能動的観測と受動的観測の融合による統合的サイバー攻撃情報収集分析機構

5.2　課題

提案内容には，多くの技術的，法的，倫理的課題が存在する．まず受動的観測についてはこれまで多くの研究が進められているが，多様化する脅威を観測するためにはこれに合った観

測技術を継続的に検討する必要がある．例えば，産業制御システムやIoTデバイスを模擬するハニーポット技術は発展途上にあり，観測可能な攻撃は限定的といえる．能動的観測については，受動的観測に比べて研究は進展しておらず，特にネットワーク越しに相手のホストの状態や種別を把握するためには，様々な知見と技術の蓄積が必要になると思われる．攻撃が行われるプラットフォームが多様になっていることから，取得したマルウェア等を解析するための環境もマルチプラットフォーム化が必要と思われる．

複数の観測の連携の観点では，有機的な連携による観測効率の向上といった利点だけでなく，他の観測システムとの連動による観測結果への影響とシステムの複雑化にも充分に考慮する必要がある．観測システムは各組織で独自に開発・運用している場合が多く，また長期的に同様の条件で観測を続けることが統計的に重要となり得る．例えば，ダークネットに届くパケットの送信元にリアルタイムに能動的観測を行うことで，送信元に観測機構の存在が露見し，ダークネットの観測結果にも影響する可能性がある．

加えて，能動的観測，受動的観測共に適用可能範囲を法的倫理的に議論する必要がある．特に脆弱性判定技術は擬似的な攻撃を行う必要がある場合が多く，適用には充分な検討が必要である．例えば，観測行為により観測対象や第三者に対して悪影響を及ぼしうる恐れや，データの収集によるプライバシ侵害の問題が考えられる．

5.3　能動的観測と受動的観測の連携試行

本節では，能動的観測と受動的観測が連携することでどのように有益な情報が得られるかを検証するためにいくつかの試行を行った結果を説明する．

IoT デバイス向けハニーポット[15]に対して攻撃を行ってきたホスト群の 23/TCP，80/TCP に対して能動的に接続し，当該攻撃ホスト群に関する情報を収集した．実験期間は 2015 年 4 月 1 日～6 月 20 日の 81 日間である．この期間中，連続する 148IP アドレスに対してハニーポットを設置し，23/TCP に対する攻撃を観測した結果，81 日間で 180,581IP アドレスからの通信を観測し，そのうち 130,314 アドレスについては，ハニーポットに対して辞書攻撃により侵入を行い，マルウェアのダウンロードを試みていた．これらのアドレスに対して上記の通り，23/TCP，80/TCP に接続し，得られた応答から攻撃ホスト群の識別を行った．その結果，表 1 に示すとおり，攻撃元として 58 種類の組み込み機器，システムが確認され，この中には DVR，IP カメラ，ルータとったように近年マルウェア感染の事実が多く報告されている機器に加えて，Heat Pump や Security Appliance といった機器やシステムと推定される応答が確認された．これらの機器・システムがインターネットから接続可能であるだけでなく，既にマルウェアに感染している可能性があることを示唆する結果といえる．

上記と同様のコンセプトに基づき，マルウェア感染が疑われるホストのうち，重要システムの有無を確認した．具体的には Shodan により，2015 年 6 月 1 日～6 月 9 日の間産業制御システムが動作していると判別された IP アドレス群のうち，同時期にダークネットに対して攻撃を行っている IP アドレスの有無を確認した．なお、分析に使用したダークネットは/24 ネットワーク 11 個、/25 ネットワーク 2 個、/32 ネットワーク 1 個である。また、Shodan による誤判断を減らすため、Shodan の検索結果に表示されている当該ホストからの応答を手動で確認し、ICS からの応答と推測されるものに絞込を行った。さらにこれらのホストに対して Nmap により能動的スキャンを行い，対象ホストのポート待ち受け状態等を確認し，Shodan の観測結果との比較により，産業制御システムが動作しているかどうかのチェックを行った．その結果，24 IP アドレスについて産業制御システムと判定されるホストが能動スキャン時にも動作中であり、さらに、マルウェア感染している疑いがあることが確認

表 1. 能動的観測により特定されたマルウェア感染疑いのある組み込みデバイス群

デバイス分類	デバイスモデル数	攻撃ホスト数
DVR	56	3,771
Surveillance Device	8	1,102
Web Camera	2	614
CPE	1	184
Broadband Access CPE	1	138
Set Top Box	4	137
Router	26	126
Wireless Router	57	136
Digital TV Receiver	1	115
ADSL Router	7	67
ADSL Gateway	1	64
IP Camera	10	31
Router	26	21
Heat Pump	1	16
Digital Video Scaler	1	12
Environment Monitoring Unit	1	10
NAS	3	9
Network Video Recorder	3	7
Digital Attached Storage	1	6
Optical Imaging Facility of The Canada-France-Hawaii Telescope	1	5
ADSL Modem	1	5
Security Appliance	5	4
Metrological Satellite	1	4
VoIP Gateway	1	3
Video Encoder/Decoder	1	3
FTTH Home Gateway	3	3
Wireless Bridge	1	2
VoIP Router	1	2
Music Player	1	2
IP Phone	1	2
GSM Router	1	2
Disk Recording System	1	2
Digital Video Broadcaster	1	2
Wireless Gateway	1	1
WiMAX MIMO Outdoor CPE	1	1
Wifi Audio Receiver	1	1
Web Point of Sale Device	1	1
VoIP Telephony System	1	1
VoIP Gateway		1
Telephony Modem	1	1
Telephone Gateway	1	1
Solid State Recorder	1	1
Smart Box	1	1
Security Appliance	5	1
Parking Management System	1	1
OfficeServ Devie Manager System	1	1
Network Video Server	1	1
Multiplexer Scrambler	1	1
LED display control system	1	1
iPad	1	1
Internet communication Module	1	1
Home Automation Gateway	1	1
Fire Alarm System	1	1
DVR Card	1	1
DSL Router	1	1
Data Acquision Server (ICS)	1	1
Black Box Media Player	1	1
Analog Phone Adapter	1	1

表 2. Shodan により産業制御システムと判定された IP アドレスがマルウェア感染していると推測される事例

IP アドレス(CC)	待受ポート(応答パケット TTL) *太字は ICS プロトコル	ICS プロトコル	ダークネットへの攻撃パケット宛先ポート(TTL)
A(TW)	23, **47808**/UDP (111)	BACnet	445/TCP(104)
B(BR)	13,21,22,80,81,**502** /TCP(50)	Modbus	23/TCP(51)
C(VE)	**502**, 8080/TCP(45) 3389/TCP(109)	Modbus	445/TCP(110)
D(AU)	80, **1911**/TCP(117)	Tridium	445/TCP (118)
E(US)	1911,3389/TCP (114)	Tridium	3389/TCP (116)
F(TR)	23/TCP(50), 80/TCP(80), **102**/TCP(15)	Siemens S7	445/TCP (117)

された. その結果の一部を表 2 に示す. IP アドレス A は 23/TCP, 47808/TCP で待ち受けており、後者はビル制御プロトコルである BACnet のデフォルトポートである. TTL 値よりこれらのサービスが起動しているホストは Windows ホストであることが予想される. 一方, ダークネットで観測された攻撃の宛先も Windows マシンの脆弱性を狙うものであり, 感染疑いホストも同様に Windows マシンであることが予想される. アドレス C は 502, 8080, 3389/TCP で待ち受けを行うサービスが起動しているが, TTL 値から実際には 2 台以上の異なるホストが提供するサービスであることが推測される. これはゲートウェイマシンからポートフォーワーディング等により特定ポートへの通信のみ他ホストに転送している場合に見られる典型的な状況であり, リモート制御を行う産業制御システムにおいて想定されるネットワーク構成といえる.

このように能動的観測と受動的観測が連携して動作することで観測対象ホストの詳細を把握しつつ, それらのホストからの攻撃を観測することで新たな知見が得られたといえる.

6 おわりに

本稿では, 能動的観測と受動的観測の融合によりサイバー攻撃の観測を有効に行う仕組みを提案した. 今後, この機構の実現に向けて

さらに検討・実証を進める予定である.

参考文献

[1] The UCSD Network Telescope, https://www.caida.org/projects/network_telescope/

[2] サイバー攻撃観測・分析・対策システム NICTER, http://nict.go.jp/nsri/cyber/research.html

[3] 警察庁 インターネット定点観測, https://www.npa.go.jp/cyberpolice/detect/observation.html

[4] TSUBAME (インターネット定点観測システム), https://www.jpcert.or.jp/tsubame/

[5] Honeynet, http://www.honeynet.org/

[6] What is a Honeypot?, SANS Institute, http://www.sans.org/security-resources/idfaq/honeypot3.php

[7] 伊藤光恭, 針生剛男, 谷本直人, 岩村誠, 八木毅, 川古谷裕平, 青木一史, 秋山満昭, 中山心太, "マルウェア対策技術," NTT 技術ジャーナル, 2010.

[8] 八木毅, 針生剛男, ハイブリッド型 Web ハニーポット Web Phantom の実装と評価, 電子情報通信学会技術研究報告. ICSS, 情報通信システムセキュリティ 113(502), 65-70, 2014.

[9] Glastoph Project, http://glastopf.org/

[10] Kippo – SSH Honeypot, https://www.honeynet.org/project/Kippo

[11] Project 11 - VoIP low interaction server honeypots, https://www.honeynet.org/gsoc2011/slot11

[12] Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS," RAID2015, 2015.

[13] CONPOT ICS/SCADA Honeypot, http://www.conpot.org/

[14] SCADA HoneyNet Project: Building Honeypots for Industrial Networks, http://scadahoneynet.sourceforge.net/

[15] Yinminpapa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analyzing the Rise of IoT Compromises," USENIX/WOOT'15, 2015.

[16] L. Spitzner, "Honey tokens: The other honeypot," Security Focus, vol. 21, 2003.

[17] Mitsuaki Akiyama, Takeshi Yagi, Kazufumi Aoki, Takeo Hariu, Youki Kadobayashi, "Active Credential Leakage for Observing Web-Based Attack Cycle," RAID2013, pp. 223-243, 2013.

[18] Zmap: The Internet Scanner, https://zmap.io/

[19] GHH - The "Google Hack" Honeypot, http://ghh.sourceforge.net/

[20] A Nappa, Z Xu, MZ Rafique, J Caballero, G Gu, "Cyberprobe: Towards internet-scale active detection of malicious servers," NDSS2014, 2014.

[21] Nmap: the Network Mapper - Free Security Scanner, https://nmap.org/

[22] masscan | Penetration Testing Tools, http://tools.kali.org/information-gathering/masscan

[23] SHODAN - Computer Search Engine, www.shodanhq.com/

[24] Scanning Best Practices, https://zmap.io/documentation.html#bestpractices

[25] 笠間貴弘,中里純二, 鈴木未央, 衛藤将史, 井上大介, 中尾康二, 秋山満昭, 青木一史, 岩村誠, 八木毅, 斉藤典明, 針生剛男, "多様なセンサの観測情報を用いたマルチモーダル分析," 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) 2012.

[26] Brett Stone-Gross, Andreas Moser, Kevin Almeroth, Christopher Kruegel, and Engin Kirda, "FIRE: FInding Rogue nEtworks," ACSAC2009, 2009.

[27] H Asghari, M van Eeten, M Mueller,

"Internet Measurements and Public Policy: Mind the Gap," USENIX/CSET 2013, 2013.
[28] 笠間貴弘,島村隼平, 井上大介, "マルチモーダル分析による組込みシステムからの攻撃活動状況の把握," CSS2014.
[29] PREDICT, https://www.predict.org/default.aspx?cs_Category=2
[30] DNSDB, https://www.dnsdb.info/
[31] Shadowserver Foundation, https://www.shadowserver.org/
[32] VirusTotal, https://www.virustotal.com/
[33] Internet-Wide Scan Data Repository, https://scans.io/
[34] マルウェア対策研究人材育成ワークショップ 2015, www.iwsec.org/mws/2015/
[35] CAIDA Data, www.caida.org/data/