2-2　データ駆動型サイバーセキュリティ技術
2-2　Data-driven Cybersecurity Technology
2-2-1　ダークネット観測システム NICTER の持続的進化と IoT マルウェアの隆盛
2-2-1　Darknet Grows Darker: The Rise of IoT Malware and Beyond

笠間 貴弘　森 好樹　遠藤 由紀子　久保 正樹
KASAMA Takahiro, MORI Yoshiki, ENDO Yukiko, and KUBO Masaki

今から遡ること約 20 年、当時の NICT 情報セキュリティセンター セキュリティ高度化グループにおいて、NICTER プロジェクトは開始された。そして今なお、NICT のサイバーセキュリティ分野における主要な研究開発プロジェクトの一つとして継続されている。NICTER プロジェクトで採用しているダークネット観測は「未使用のグローバル IP アドレス宛の通信を観測することでインターネット上の不正な活動を捉える」というシンプルな観測手法だが、多様化するサイバー攻撃を長年捉え続けている。本稿では、特に 2016 年から 2023 年までの期間におけるサイバー攻撃の変遷について概説する。

About 20 years ago, the NICTER project was launched at NICT. It is still one of NICT's major research and development projects in the field of cybersecurity. Darknet monitoring is a simple method of "detecting malicious activity on the Internet by observing traffic directed towards unused global IP addresses." However, it continues to capture a growing variety of cyber-attacks. This paper outlines the evolution of cyber-attacks observed by NICTER, particularly focusing on the period from 2016 to 2023.

1　はじめに

サイバー攻撃対策の第一歩は実際に発生している攻撃活動を迅速かつ正確に把握することから始まる。我々はインターネット上における大規模かつ無差別なサイバー攻撃に関する大局的な攻撃傾向を把握するために、2005 年から継続してインシデント分析センタ NICTER（Network Incident analysis Center for Tactical Emergency Response）の研究開発を推進し、ダークネット観測・分析を行ってきた [1]。

ダークネットとはインターネット上で到達可能かつ未使用の IP アドレス空間のことを指す。正規のサーバやコンピュータが接続されていないダークネットには本来インターネット側からの通信（パケット）が届くことはないはずだが、実際に観測を行うと大量のパケットがダークネットに届いていることがわかる。これらのパケットは主にマルウェア（不正プログラム）に感染したコンピュータが次の攻撃先を探索する活動（スキャン）や、送信元 IP アドレスを詐称した DDoS 攻撃（分散型サービス妨害攻撃）に対する応答であるバックスキャッタなど、インターネット上における何らかの不正な活動に起因しているため、ダークネット観測を通じてインターネット上で発生しているサイバー攻撃の大局的な傾向を把握することができる。本稿では、我々が 2016 年に公表した研究報告 [2] 以降の約 8 年間におけるダークネット観測結果の推移と特徴的な事例に関する分析結果について紹介する。

2　ダークネット観測統計

2.1　観測パケット数及び送信元アドレス数の推移

まずダークネットトラフィックの量的な変化を明らかにするため、図 1 に 2016 年 1 月 1 日から 2023 年 12 月 31 日までの 8 年間のダークネット観測統計として、TCP SYN パケットの日ごとのパケット数及びユニークな送信元 IPv4 アドレス数（以降、「送信元アドレス数」と書く）を示す。なお長期的な傾向を把握するために、パケット数及び送信元アドレス数は共に前後 3

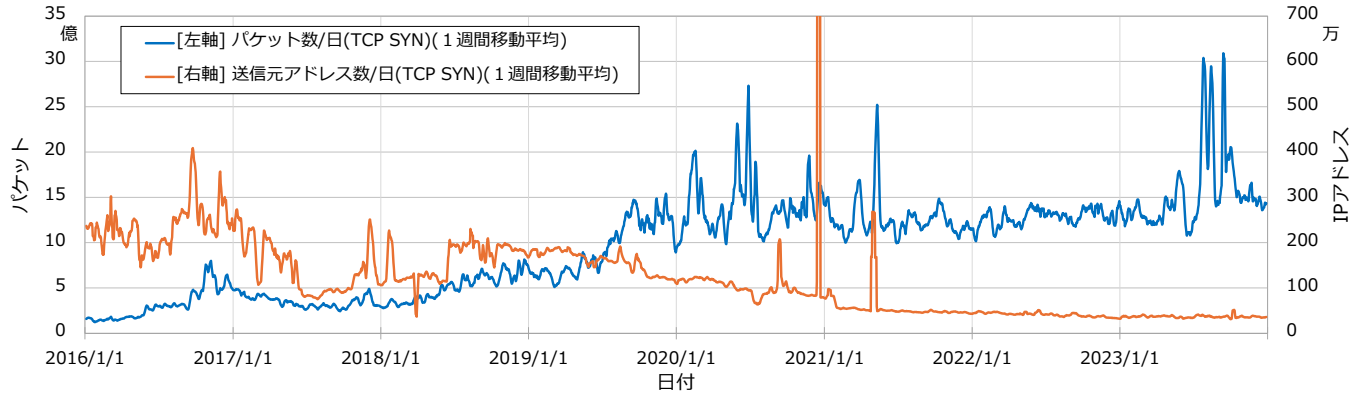

図１　2016 年から 2023 年までのダークネット観測統計

日を含む１週間の移動平均の値を示している。2016 年以降は NICTER の観測対象のダークネットアドレス数は、多少の増減はありつつも約 30 万アドレスを維持している。

図１を見ると、パケット数に関しては 2016 年以降も継続して増加傾向を示しており、2023 年現在においては１日あたり 10 億から 20 億パケットを観測していることがわかる。これは 2016 年と比較して約 10 倍のパケット数に達しており、インターネット空間におけるスキャン活動がこの８年間で一層活発化している様子が明らかとなっている。我々はダークネット観測結果の分析によって、主に２つの要因がこのパケット数の増加をもたらしていることを特定している。１つは 2016 年の研究報告 [2] でも触れていた、ルータや Web カメラ等の IoT 機器に感染するマルウェアの隆盛である。特に 2016 年８月に発見された IoT マルウェア Mirai（ミライ）は、Telnet 及び SSH サービスに対するスキャンと ID・パスワードリストを用いたブルートフォース攻撃によって世界中の数十万台の IoT 機器へ感染を広げ、攻撃者がそれらの感染機器を悪用して 600 Gbps もの大量の通信を発生させる大規模な攻撃を実行したことで話題となった。その後、Mirai のソースコードはインターネット上のハッカーフォーラムで公開され、当該ソースコードを流用した Mirai の亜種が多数登場している。2024 年現在においても IoT 機器を狙うマルウェアとその感染機器が多数存在しており、活発なスキャン活動がダークネット観測で捉えられている。もう一つの要因は攻撃目的ではなく調査目的でインターネットスキャンを実施している調査スキャン組織の増加である。代表的な調査スキャン組織の一つである Shodan [3] はインターネットに接続されている IoT 機器やサービスをインターネットスキャンによって探索し、その結果をデータベース化して検索エンジンとして 2009 年からサービスを提供している。その後、同様のサービスとして Censys [4] や ZoomEye [5] など複数のサービスが登場し、定常的にインターネットスキャンを実施している。これらの商用サービスに加え、特に 2018 年以降において大学や研究機関、匿名の研究者により実施されるインターネットスキャンが増加した結果、ダークネットで観測されるパケット数が増加している。2023 年の我々の調査 [6] ではこのような調査スキャンを実施する組織として 79 組織を特定しており、素性を明らかにしていない未知の調査スキャン組織と合わせると、2023 年の１年間にダークネットで観測したパケット数の約 64 % が調査目的のスキャンによるものであった。

一方、送信元アドレス数に関しては、Mirai による感染拡大が発生した 2016 年後半に１日あたり 300 万アドレスを観測したのをピークに緩やかな減少傾向を示しており、2023 年末の時点では 40 万アドレス程度まで減少している。この減少は、世界中の脆弱（ぜいじゃく）な IoT 機器がマルウェア感染しサイバー攻撃に悪用された結果として IoT 機器のセキュリティ対策の重要性の認識が広まり、一定の対策が進んだことが要因の一つだと考えられる。例えば日本では、IoT 機器を悪用したサイバー攻撃の増加を受けて、IoT 機器の技術基準適合認定の基準にセキュリティ対策を追加する省令が 2020 年４月１日に施行された。その結果、IoT 機器におけるアクセス制御機能、初期設定のパスワードの変更を促す等の機能、ソフトウェアの更新機能などの対策が必須となり、ユーザによる機器の買い替えによってセキュアな IoT 機器への置き換えが一定規模進んでいることが想定される。なお、2020 年 12 月頃の送信元アドレス数の急激な上昇は、送信元アドレスを詐称したスキャンパケットの影響であり実際の感染機器の急増では無いことを確認している。

2.2　攻撃対象サービスの変化

ダークネットトラフィックで観測される攻撃活動の変化を把握するために、表１に 2016 年から 2023 年ま

表 1　宛先ポート・プロトコル別観測パケット数

2016 年		2017 年		2018 年		2019 年		2020 年		2021 年		2022 年		2023 年	
Port	%	Port	%	Port	%	Port	%	Port	%	Port	%	Port	%	Port	%
23/TCP	53	23/TCP	39	23/TCP	14	23/TCP	11	23/TCP	7.5	23/TCP	5.1	23/TCP	10	23/TCP	9.7
53413/UDP	7.4	22/TCP	6.1	445/TCP	3.1	445/TCP	2.5	445/TCP	2.2	22/TCP	1.9	22/TCP	2.3	22/TCP	1.6
445/TCP	3.8	445/TCP	5.0	80/TCP	2.6	22/TCP	1.7	80/TCP	1.5	445/TCP	1.4	80/TCP	1.6	80/TCP	1.5
2323/TCP	3.1	2323/TCP	3.1	22/TCP	2.5	80/TCP	1.6	22/TCP	1.2	80/TCP	1.4	5555/TCP	1.1	8080/TCP	1.1
1433/TCP	2.3	5358/TCP	2.8	52869/TCP	1.8	8080/TCP	1.2	1433/TCP	1.0	6379/TCP	1.1	6379/TCP	1.0	3389/TCP	1.0
22/TCP	1.8	7547/TCP	2.2	8080/TCP	1.5	52869/TCP	1.2	8080/TCP	1.0	443/TCP	1.0	443/TCP	1.0	443/TCP	0.9
80/TCP	1.3	1900/UDP	2.0	81/TCP	1.5	81/TCP	1.1	81/TCP	0.9	81/TCP	0.8	3389/TCP	0.9	5555/TCP	0.7
5060/UDP	1.3	1433/TCP	1.7	8545/TCP	1.4	8545/TCP	1.1	5555/TCP	0.9	123/UDP	0.8	8080/TCP	0.9	37215/TCP	0.6
53/UDP	1.2	443/TCP	1.7	3389/TCP	1.2	3389/TCP	1.1	3389/TCP	0.9	8080/TCP	0.8	2375/TCP	0.8	5060/UDP	0.6
3389/TCP	1.1	80/TCP	1.3	2323/TCP	1.1	5555/TCP	1.1	8545/TCP	0.7	5060/UDP	0.8	81/TCP	0.8	6379/TCP	0.6
Others	24	Others	36	Others	70	Others	76	Others	82	Others	85	Others	79	Others	84

での各年について、ダークネット観測パケット数を宛先ポート番号･プロトコルごとに集計した上位 10 位と総観測パケット数に対する割合を示す。

2016 年では 23/TCP に対するパケットがダークネットトラフィックの半数以上を占めているが、これは上で述べた Mirai の登場と感染拡大による影響である。23/TCP に関しては 2016 年から 2023 年に至るまで継続して最も多くのパケットを観測しており、Mirai やその後登場した多数の IoT マルウェアによって Telnet サービスを狙う攻撃活動が継続している様子がわかる。23/TCP のように毎年継続して多くのスキャンパケットを観測しているポート・プロトコルがある一方で、特定の期間において集中したスキャンパケットを観測したポート・プロトコルも存在する。このような特定の期間に集中して観測される攻撃活動は、Telnet や SSH のように汎用的なプロトコルに対する攻撃活動では無く、特定の機器に存在する脆弱性を悪用する攻撃活動であることが多い。例えば、2016 年の 53413/UDP は Netcore 製のルータの脆弱性を狙ったスキャンであり、2018 年や 2019 年の 52869/TCP はロジテック製ルータに存在する Realtek SDK の脆弱性を狙ったスキャン、2023 年の 37215/TCP は HUAWEI 製のルータの Web インタフェースの脆弱性を狙ったスキャンに関連している。このような特定の機器の脆弱性に関しては、当該脆弱性を狙う攻撃コードがマルウェアに組み込まれたタイミングにダークネットで観測されるスキャンが急増する事例を多数確認している。

また全体的な傾向として、2016 年以降は 80/TCP や 8080/TCP、81/TCP など HTTP 関連のポートに対するスキャンが増加している。これは上で述べた調査スキャン組織が HTTP 関連のポートをスキャン対象にしていることに加え、IoT 機器への攻撃活動として Web インタフェースの脆弱性を狙う攻撃活動が活発化していることが要因として挙げられる。特に IoT 機器の中には Well-known ポートではないハイポートで Web インタフェースが稼働している機器も存在しており、そのような機器を探索するスキャン活動が多数観測されている。なお、2018 年以降は後述する調査スキャン組織の増加によって広範囲のポート・プロトコルに対する定常的なスキャンを観測しており、その結果として観測パケット数上位のポート・プロトコルであっても総観測パケット数に対する割合は低い割合となっている。

3　ケーススタディ

本節では、この 8 年間において NICTER システムで観測した特徴的な事象について述べる。

3.1　Mirai 及び亜種の隆盛

2012 年に登場した Carna ボットネット、2014 年に登場した BASHLITE など、IoT 機器に感染するマルウェアは以前から存在していたが、2016 年の IoT マルウェア Mirai の感染爆発は IoT 機器のセキュリティに関する一つのターニングポイントとなった。公開されたソースコードの情報から、Mirai はスキャンパケットを raw ソケットで生成し TCP のシーケンス番号として宛先 IP アドレスの値を用いることが明らかになっている。一方、通常の SYN パケットでは TCP シーケンス番号はランダムな値が割り当てられ宛先 IP アドレスと偶然同じ値となる確率は低いことから、TCP シーケンス番号と宛先 IP アドレスの値が一致するか確認することで、Mirai もしくは Mirai のソースコードを流用した亜種によるスキャンパケットを判定できる。我々はこのような特徴的なスキャンパケットやスキャン対象ポートの組合せなどから、類似する攻

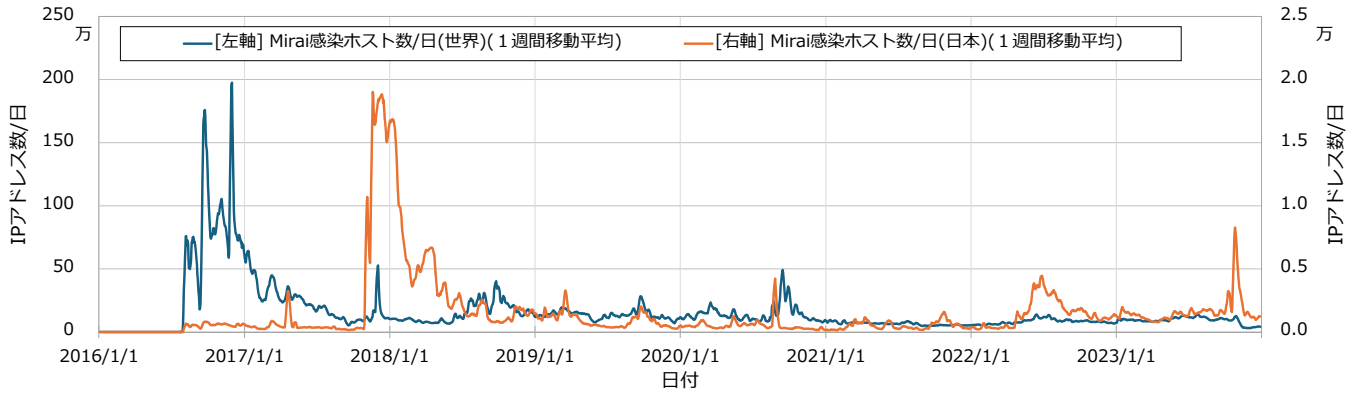

図２　2016 年から 2023 年までの Mirai 感染ホスト数の推移

撃活動を分類する仕組みを構築している。図２に世界全体及び日本国内の Mirai とその亜種に感染していると推測した送信元アドレス数（以降「Mirai 感染ホスト数」と呼ぶ）の推移を示す。

図２を見ると、2016 年８月に Mirai 感染ホストが急増し、わずか１日足らずで数十万台規模へ感染を広げる様子が NICTER で観測されている。ピーク時には１週間の移動平均で約 200 万もの感染機器が観測されており、被害の大きさを確認することができる。2017 年以降は、感染機器の対処や Mirai 亜種の登場などの様々な影響を受け、観測される感染台数は１日あたり数万から 10 万台程度で推移を続けている。一方、国内の Mirai 感染ホストに着目すると Mirai 登場時期においては１日平均 500 台しか観測されておらず、当初の国内の IoT 機器への Mirai 感染は限定的であったことがわかる。しかし、2017 年末から 2018 年にかけて国内で２万大規模の Mirai 感染ホストが観測されている。これは NICTER 観測レポート 2017 [7] で報告した日本国内で流通するブロードバンドルータに残存する Realtek SDK の脆弱性を悪用して感染を広げる Mirai 亜種が登場したことが原因である。その後も世界全体の観測数とは平均的には２桁近く少ないものの、主に Mirai 亜種の登場によって国内でも数千台規模の感染ホストが観測されており、Mirai の影響は登場から８年近く経過した今でも残存していることがわかる。

3.2　日本国内のマルウェア感染事例

ここでは、NICTER システムで観測した日本国内の特徴的なマルウェア感染事例について述べる。

3.2.1　古い国内ブロードバンドルータの感染

前節で述べた通り、2017 年以降 NICTER システムではロジテック製ブロードバンドルータに存在する Realtek SDK の脆弱性を狙った 52869/TCP 宛のスキャンパケットを継続的に観測しており、当該脆弱性を悪用した Mirai 亜種の感染も確認していた。一部のロジテック製ブロードバンドルータでは 52881/TCP で稼働する UPnP（Universal Plug and Play）サービスに対してリクエストを送信することで機器の Description ファイルを取得できる機器が存在し、Description ファイルには当該機器の情報として製品型番、シリアル番号、UDN（Unique Device Name）などが記載されている。この UDN に含まれる UUID（Universally Unique Identifier）には MAC アドレス、乱数、またはハッシュ値ベースの値が使用されているため、機器のグローバル IP アドレスが変更されても同一機器の特定が可能になる。そこで 2021 年１月１月から 2021 年４月 31 日までの期間において、観測した日本国内の Mirai の特徴を持つスキャンパケットの送信元アドレスに対して Description ファイルの収集を行い、国内の Mirai 感染ホストに対するロジテック製ブロードバンドルータの割合を調査した結果を図３に示す。

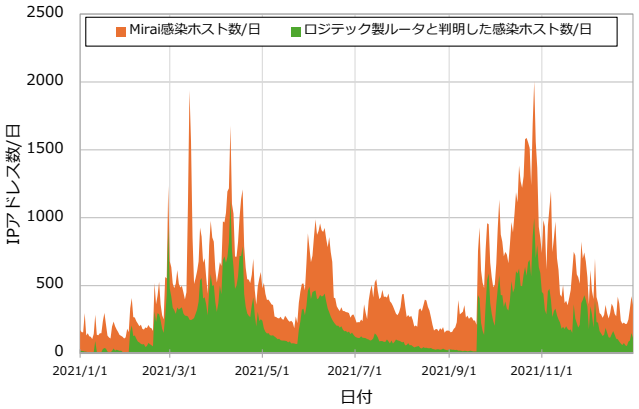

図３　国内の Mirai 感染ホスト数とロジテック製ルータの割合

図３を見ると、NICTER で観測される国内の Mirai 感染ホストのうち平均で約 40 %、多い時で 80 % 近くがロジテック製ルータであることが確認できている。我々が特定した該当のロジテック製ブロードバンドルータは当時の時点で 10 年以上前に販売された機器であり、既にベンダによるサポートも終了している EoL（End of Life）製品であったが継続して利用し続け

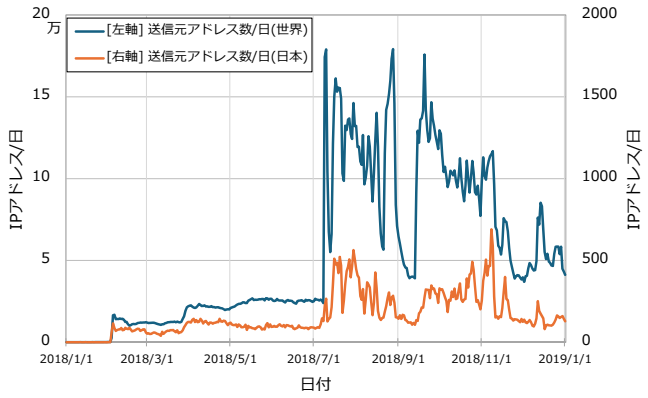

図 4　スキャンの送信元アドレス数の推移 (5555/TCP)

図 5　国内で感染していた Android OS 搭載機器例

ているユーザが一定数存在し、数百台規模でマルウェア感染をしている状況が明らかとなった。総務省の調査 [8] においても、1 割以上のユーザが自宅の無線 LAN ルータを 10 年以上継続して利用しており、6 割以上のユーザはサポート期間を認識しておらず、ファームウェア更新を着実に実施しているユーザは 2 割にしか満たないことが報告されている。本事例は、IoT 機器が普及する一方で長年放置され稼働し続けている日本国内の古い IoT 機器がマルウェアに感染した特徴的な事例の一つである。

3.2.2　Android OS を搭載した IoT 機器の感染

2018 年 2 月 4 日から 5555/TCP に対するスキャンの送信元アドレス数が増加し、2018 年 7 月 9 日に急増した結果、ピーク時には世界中で約 18 万アドレス、日本で約 500 アドレスからのスキャンを観測した (図 4)。

このような特定の宛先ポートに対する送信元アドレス数の急増は、新たな脆弱性や機器を狙うマルウェアが登場し感染拡大をしている際に典型的に観測される傾向であるため、我々は攻撃対象となっている脆弱性及び機器について分析を行い、以下の実態を特定した。

- 5555/TCP 宛のスキャンは、ネットワーク経由の ADB (Android Debug Bridge) が有効かつ Secure モードが無効化されていて認証無しのコマンド実行が可能な Android OS 搭載機器を狙った攻撃活動であった。
- 5555/TCP で稼働する ADB サービスへのアクセスによって感染を拡げる 2 種類の攻撃活動が存在し、一方の攻撃活動では仮想通貨 Monero のマイニング用 Android APK ファイルを感染機器にインストールし仮想通貨のマイニングを試みる挙動が見られた。また、もう一方の攻撃活動では他方のマルウェアを機器上から削除しようとする (機器を占有しようとする) 挙動が見られた。
- 当該攻撃によってマルウェア感染した機器は、日本国内では感染機器の過半数をケーブルテレビ向けセットトップボックスと Android エミュレータが占めていた。一方、世界全体ではデジタルサイネージやドライブレコーダ、SIM フリーのスマートフォンなど多様な機器が感染していた。

日本国内においても数百台規模の感染が観測されていたことから、我々は実際に国内で感染している機器の販売元を特定し、連絡を取ることで機器の利用実態について調査を実施した。図 5 は調査の結果特定した、工事現場で利用されていた実際の感染機器例 (デジタルサイネージ機器) である。当該機器の販売元にヒアリングを行った結果、当該機器は別の業者から Android OS が搭載された機材を購入しその上に独自のサイネージ用アプリをインストールして販売していることが判明した。この機材は工場出荷時もしくは OS のインストール時の時点でネットワーク経由の ADB が有効になっており、その後グローバル IP アドレスが直接割り当てられる環境で使用されていたことで攻撃を受けマルウェアに感染していたことを特定した。本事例は、従来はスタンドアローンで動作していた機器に汎用 OS が搭載されてインターネットに接続されるようになった結果、不適切な設定のまま運用されていることでマルウェア感染につながった特徴的な事例の一つである。

3.2.3　InfectedSlurs ボットの感染拡大

InfectedSlurs ボット [9] は 2022 年から観測されている IoT 機器を感染対象とするマルウェアであり、Mirai の特徴を持つスキャンパケットを送信する。我々の調査の結果、日本国内で InfectedSlurs への感染が確認された主な IoT 機器は、モバイル回線に接続された防犯カメラ、コンセント埋め込み型の Wi-Fi ルータ、DVR/NVR (Degital Video Recorder/Network Video Recorder) の 3 種類であることを特定した。特に図 2 において 2023 年 10 月から 11 月にかけての日本国内における Mirai 感染ホスト数増加の原因は、InfectedSlurs に感染した DVR が原因であり、実際

に 2023 年 10 月 24 日に確認された Mirai 感染ホスト 8,445 アドレスにアクセスした結果、1,003 アドレスで図 6 に示すような DVR 機器の Web 管理画面が確認できている。また、我々が運用しているハニーポットで観測した InfectedSlurs の攻撃ペイロードを分析した結果、観測された攻撃ペイロードはいずれも Web 管理画面から初期設定の ID・パスワードを用いてログインを試みるものであり、ダークネットで観測された DVR 機器はいずれも Web 管理画面から侵入された結果 InfectedSlurs に感染したと考えられる。我々は、InfectedSlurs への感染が確認できた機器について、それぞれ開発ベンダや販売代理店を特定してコンタクトを取り、対策済みファームウェアの公開や代理店による初期パスワードの変更などの対処が実施されている。

また、InfectedSlurs の検体を追跡調査した結果、2023 年 11 月以降の検体ではスキャン機能の更新が行われ、Mirai の特徴を持たないスキャンパケットを送信するように変更されていた。その影響を受けて図 2 では 2023 年 11 月以降の日本国内の Mirai 感染ホスト数は見かけ上減少したように見えるが、実際には Mirai の特徴を持たない InectedSlurs に感染した多数の機器が継続して存在している。本事例は、Telnet や SSH といった従来の IoT マルウェアの主要な感染経路では無く、Web 管理画面のパスワード設定不備を悪用されてマルウェア感染に至った特徴的な事例である。

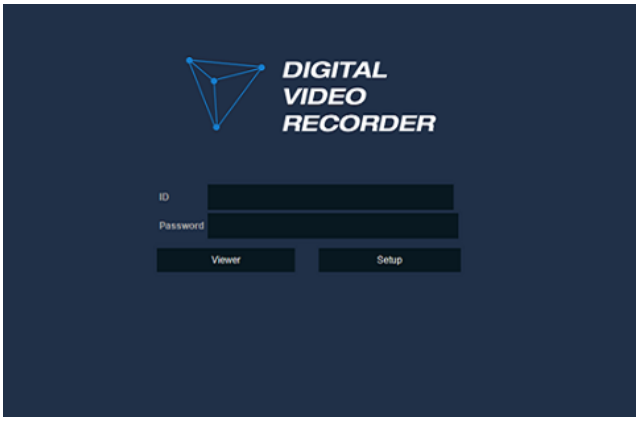

図 6　InfectedSlurs に感染した DVR のログイン画面例

3.3　調査スキャン組織の増加と定常的なスキャン活動

2018 年以降に調査スキャン組織が増加した結果、2023 年には調査スキャン組織によるものと推測されるパケットが全体の約 64 % を占めており、ダークネット観測における大きなノイズとなっている。そこで我々は 2018 年から独自の基準 [10] と GreyNoise [11] や SANS [12] などの外部インテリジェンスを組合せることで調査目的のスキャンパケットを判定し、調査スキャン組織の特定や当該スキャンパケットを除外した分析を行っている。

2023 年の 1 年間では合計 17,187 個の送信元アドレスを調査目的のスキャンに関連したものと判定し、そのうち 11,186 アドレスに関連する調査スキャン組織として 79 組織を特定した。表 2 に 2023 年の 1 年間で特定した調査スキャン組織のうち、観測パケット数の多い上位 10 組織について示す。種別については各組織の Web サイトを参照し、スキャン結果をどのようなサービスや目的で利用しているかが確認できたものについて記載しているが、目的が記載されていても活動実態が確認できなかった場合には不明としている。

表 2 を見ると、最も活発な調査スキャンを実施している組織は Censys であり、年間で約 456 億パケットを観測している。Censys は全 TCP ポートと UDP ポートに対する定常的かつ広範囲のスキャン活動を行っており、スキャン結果を脅威情報提供サービスとしてユーザに提供している。このように調査スキャンの結果を脅威情報提供サービスとして利用している調査スキャン組織は多く、上位 10 組織中少なくとも 6 組織は同様のサービス提供を行っている。一方、2 番目に活発な調査スキャンを行っている Recyber [13] は Web

表 2　調査スキャン組織 (2023 年の観測パケット数上位 10 組織

組織名	種別	パケット数	送信元アドレス数	宛先ポート数 (TCP/UDP)	観測日数
Censys	脅威情報提供サービス	約 456 億	375	65,535 / 65,535	365
The Recyber Project	不明	約 340 億	281	65,536 / 5	365
CriminalIP	脅威情報提供サービス	約 307 億	3,264	28,864 / 1,955	365
Palo Alto Networks (Cortex-Xpanse)	脅威情報提供サービス	約 245 億	47	1,498 / 23	365
Shadowserver	脅威情報提供サービス	約 110 億	529	310 / 40	365
Academy for internet research	不明	約 84 億	30	1,479 / 1	339
driftnet (internet-measurement.com)	脅威情報提供サービス	約 57 億	514	65,535 / 2	365
Shodan	脅威情報提供サービス	約 39 億	84	1,252 / 86	365
internettl	不明	約 28 億	150	257 / 121	262

サイト上では「研究者、大学、その他の教育機関を支援するプロジェクトである」という説明が記載されているものの、その運営組織や実際にスキャン結果が誰に提供されどのように活用されているのかといった情報は明らかにされておらず、実質的には情報は得られない。これらの組織名が特定できた調査スキャン組織以外にも未知組織による調査スキャンを多数判定しており、それらの未知組織による調査スキャンとして 79 組織による調査スキャンと同等程度のパケット数を観測している。未知組織による調査スキャンでは海外のホスティングサービスやクラウドサービスをインフラとして用いる傾向があり、その中にはいわゆる防弾ホスティングと呼ばれる Abuse 対応に適切に対応しないサービスも多く含まれる。

我々は 2016 年の研究報告 [2] で調査スキャンの増加を報告していたが、それから 8 年が経過し、よりインターネットスキャンが一般のセキュリティ研究者や企業に普及したことで、マルウェアによるスキャンパケットを上回る規模の調査スキャンパケットを観測している状況が明らかになった。我々は独自の基準も組み合わせることで調査目的のスキャンを判定し、より効果的なダークネット観測データの分析を実現しようとしているが、未知組織の調査スキャンの判別方法にはまだ課題が存在しており今後も検討を進めて行く。

4　おわりに

本稿では、2016 年から 2023 年にかけて NICTER プロジェクトで観測したダークネットトラフィックの推移と特徴的な観測事象について示した。NICT では 2005 年から継続したダークネット観測を行っているが、この約 20 年間、Web を介したドライブ・バイ・ダウンロード攻撃や特定の組織を狙う標的型攻撃、フィッシング、スマートフォンの不正アプリ、ビジネスメール詐欺等々、サイバー攻撃は多様化してきた。こうした状況の変化の中でサイバーセキュリティの専門家からも、ダークネット観測のような外部からのスキャンを待ち受ける受動的な攻撃観測手法は時代遅れでありもはや効果がない、という主張を少なからず耳にしてきた。しかしそのような根拠のない主張とは裏腹に、我々は継続したダークネット観測によって毎年のように新たに登場する攻撃事象を捉えており、IoT マルウェアの隆盛や調査スキャン組織の登場も背景にインターネット上のスキャン活動はかつてないほどに活発化している。我々は今後も NICTER による継続的なサイバー攻撃観測と分析、その知見を活かした対策手法の研究開発を進めていき、NICTERWEB [14] 等を通じた成果の一般公開も継続していく。

【参考文献】

1 D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, “nicter: An incident analysis system toward binding network monitoring with malware analysis,” Proceedings of the 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp.58–66, 2008.
2 笠間 貴弘, “NICTER のダークネット長期分析,” 情報通信研究機構研究報告, vol.62, no.2, pp.17–23, 2016.
3 Shodan. https://www.shodan.io/
4 Censys, “Censys Search”. https://search.censys.io/
5 Knownsec, “ZoomEye”. https://www.zoomeye.org/
6 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュティネクサス, “NICTER 観測レポート 2023,” https://csl.nict.go.jp/nicter-report.html
7 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティ研究室, “NICTER 観測レポート 2017,” https://csl.nict.go.jp/report/NICTER_report_2017.pdf
8 総務省, “無線 lan セキュリティに関する調査,” https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
9 Akamai, “InfectedSlurs ボットネットがゼロデイで Mirai を拡散,” https://www.akamai.com/ja/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days
10 遠藤 由紀子, 森 好樹, 島村 隼平, 久保 正樹, “ダークネット観測における大規模スキャナの判定指標の提案,” 電子情報通信学会 信学技報, ICSS2019-80, pp.73–78, 2020.
11 GreyNoise, “Greynoise is the source for understanding internet noise,” https://www.greynoise.io/
12 SANS, “Internet Storm Center/DShield API,” https://isc.sans.edu/api/threatcategory/
13 Recyber, “The Recyber Project,” https://www.recyber.net/
14 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティ研究室, “NICTERWEB,” https://www.nicter.jp/

笠間 貴弘（かさま たかひろ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
室長
博士 (工学)
サイバーセキュリティ
【受賞歴】
2022 年　電子情報通信学会 ICSS 2022 年度研究賞
2019 年　NDSS2019 Distinguished Paper Award
2011 年　情報処理学会 2011 年度山下記念研究賞

森 好樹（もり よしき）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究技術員
サイバーセキュリティ

遠藤 由紀子　（えんどう ゆきこ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究技術員
サイバーセキュリティ

久保 正樹　（くぼ まさき）
サイバーセキュリティ研究所
サイバーセキュリティ研究室／
サイバーセキュリティネクサス
上席研究技術員
脆弱性、サイバー攻撃観測・分析、IoT セキュリティ、セキュアコーディング