NICTER 観測レポート 2020

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

1. はじめに

本レポートは，サイバーセキュリティ研究室が実施している NICTER プロジェクト*1において，ダークネット観測*2 と各種ハニーポット*3が捉えた 2020 年のサイバー攻撃の状況についてまとめたものです．

例年同様，様々な事象が NICTER の各種センサで観測されましたが，本レポートで説明する 2020 年の主な観測結果をまとめると次のようになります．

- **ダークネット観測統計（2 章）**：海外組織による調査目的とみられる探索（スキャン）活動がさらに増加した結果，ダークネット観測における 1 IP アドレスあたりの年間総観測パケット数が 182 万パケットに達しました．これは，2019 年の観測結果の約 1.5 倍にあたります．また，調査目的とみられるスキャンパケットを除去した観測結果からは，攻撃者による攻撃の対象が多様化する様子が確認されました．
- **IoT ボットの活動と感染機器の実態（3 章）**： Mirai 亜種をはじめとする IoT ボットの活動が依然として観測され，特に，Mozi と呼ばれるボットの活動が顕著でした．また，Mirai 亜種に感染した機器の実態を調査した結果，既知の脆弱性を持つ機器が依然として使用され続けている状況がわかりました．
- **DRDoS 攻撃の観測状況（4 章）**： DDoS 攻撃*4の一種である DRDoS 攻撃の観測結果から，DRDoS 攻撃の長時間化や攻撃に悪用されるサービスの多様化といった事象が確認されました．

2. ダークネット観測統計

2.1. 年間観測パケット数

NICTER プロジェクトのダークネット観測で確認された過去 10 年間の「年間総観測パケット数」「観測 IP アドレス数（ダークネット観測の規模）」「1 IP アドレスあたりの年間総観測パケット数」を表 1 に示します*5．年間総観測パケット数は観測 IP アドレス数に影響されるため，表の右端にある「1 IP アドレスあたりの年間総観測パケット数」をインターネットにおけるサイバー攻撃関連活動の活発さを表す指標として考えます．

この数値に着目すると，2020 年は 1 IP アドレスあたりで約 182 万パケットが観測されたことがわかります．これは，2019 年の約 119 万パケットの約 1.5 倍であり，ダークネットで観測されるパケット数は増加傾向にあることがわかります．

パケット数増加の原因の一つは，2018 年から活発化している，海外組織による調査目的とみられる大規模なスキャンです．この調査目的のスキャンは，攻撃の傾向を分

*1. プロジェクト公式サイト（https://www.nicter.jp/）

*2. インターネット上で到達可能かつ未使用の IP アドレス宛に届くパケットを収集する手法．未使用の IP アドレスであるため本来はパケットが観測されないはずですが，実際にはサイバー攻撃に関連する探索活動（スキャン）や送信元 IP アドレスを詐称した DDoS 攻撃の跳ね返り（バックスキャッタ）等が多く観測されます．このパケットを分析することにより，インターネット上で発生しているサイバー攻撃の兆候や傾向等を把握することができます．

*3. サイバー攻撃を観測・分析するための囮（おとり）システム．欠陥（脆弱性）を意図的に残したシステムあるいはその脆弱性を模擬するプログラムを使用することにより，攻撃者の活動を把握することができます．

*4. 分散型サービス妨害攻撃（Distributed Denial-of-Service Attack）．サーバやネットワーク等のリソースに意図的に過剰な負荷をかけることにより正常なサービスを妨害するサイバー攻撃．

*5. 2019 年の年間総観測パケット数は，NICTER 観測レポート 2019 の発行後に判明した重複カウントを排除して再集計した値を用いています．合わせて NICTER 観測レポート 2019 も修正版を発行しています．

表1: 年間総観測パケット数の統計（過去 10 年間）

年	年間総観測パケット数	観測 IP アドレス数	1 IP アドレスあたりの年間総観測パケット数
2011	約 45.4 億	約 12 万	40,654
2012	約 77.8 億	約 19 万	53,085
2013	約 128.8 億	約 21 万	63,655
2014	約 256.6 億	約 24 万	115,323
2015	約 545.1 億	約 28 万	213,523
2016	約 1,281 億	約 30 万	469,104
2017	約 1,504 億	約 30 万	559,125
2018	約 2,121 億	約 30 万	789,876
2019	約 3,220 億	約 30 万	1,187,935
2020	約 5,001 億	約 30 万	1,820,722

析する際のノイズとなるため，昨年と同様に，一定の判定ルール*6を設けて調査目的のスキャンの判定と除去を行いました．その結果，2020 年は 3,676 個の IP アドレスからの約 2,685 億パケットが調査目的のスキャンとして判定されました．これは 2020 年に観測された全パケットの約 54% にあたります．

2.2. 日ごとの観測パケット数の推移

ダークネットにおける日ごとの観測パケット数の推移を，「調査目的のスキャンパケット」と「それ以外（総観測パケットから調査目的のスキャンパケットを除いたパケット）」に分けて表した積み上げグラフを図 1 に示します．パケット数が急増する箇所に着目すると，この急増の多くが調査目的のスキャンパケットによるものだということがわかります．また，それ以外の急増は，大規模なバックスキャッタが原因でした．3 月から 4 月にかけてのこの事象は 3.5 節で説明します．これらの増加を除くと，2020 年の調査目的のスキャンを除いた観測パケット数は緩やかな増加傾向で推移しました．

2.3. 宛先ポート番号別のパケット数

1 年間にダークネット観測で確認された TCP と UDP のパケットについて，パケット数を宛先ポート番号別に集計し，そのパケット数の多い上位 10 種類のポート番号とその他の割合をまとめたグラフを図 2 に示します．図の左側が調査目的のパケットを含んだグラフ，図の右側が調査目的のパケットを除いたグラフです．また，青色は IoT 機器等，橙色は Windows，緑色は仮想通貨サービスで主に利用されているポート番号をそれぞれ示しています．これらのポート番号に対応するサービスが，NICTER のダークネット観測が捉えた 2020 年の主な攻撃対象であるといえます．

調査目的のスキャンでは広範囲のポート番号に対してスキャンが実施されるため，図 2 の左側のグラフでは上位のポート番号の割合が小さくなり攻撃傾向を把握しづらくなっていますが，それらのノイズを除いた右側の図では攻撃の傾向がわかりやすくなっています．しかしながら，上位 10 種類に含まれない「その他のポート（Other Ports）」の割合は年々高くなってきており，その割合は 2020 年は 62.9%（前年 48.6%）へと増加しました．これは，攻撃が多様化し，多くのポート番号を攻撃の対象とするボットネット等が継続的に活動したためです（3.2 節）．

調査目的のパケットを除いた観測結果を示す図 2 の右側に着目すると，観測パケット数の最も多い宛先ポート番号は，2019 年までに引き続き Telnet サービスで使用される 23/TCP であることがわかります．23/TCP の全体に対する割合は 16.3% であり，2019 年の 24.4% から減少しました．また，Windows 等でファイル共有に使用される Server Message Block（SMB）の 445/TCP が 2 番目

*6. ある 1 日における 1 つの IP アドレスからのパケット（TCP の SYN と UDP パケット）について，

- 宛先ポート番号が 30 種類以上
- 総パケット数が 30 万以上

の条件を共に満たす場合，この IP アドレスからの全パケットを調査目的のスキャンと判定します．詳細は [1, 2] を参照して下さい．

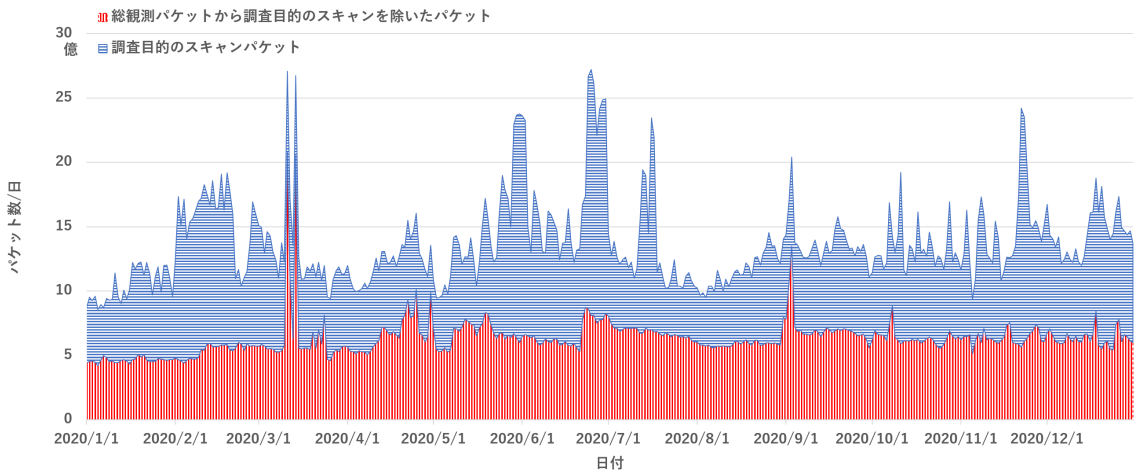
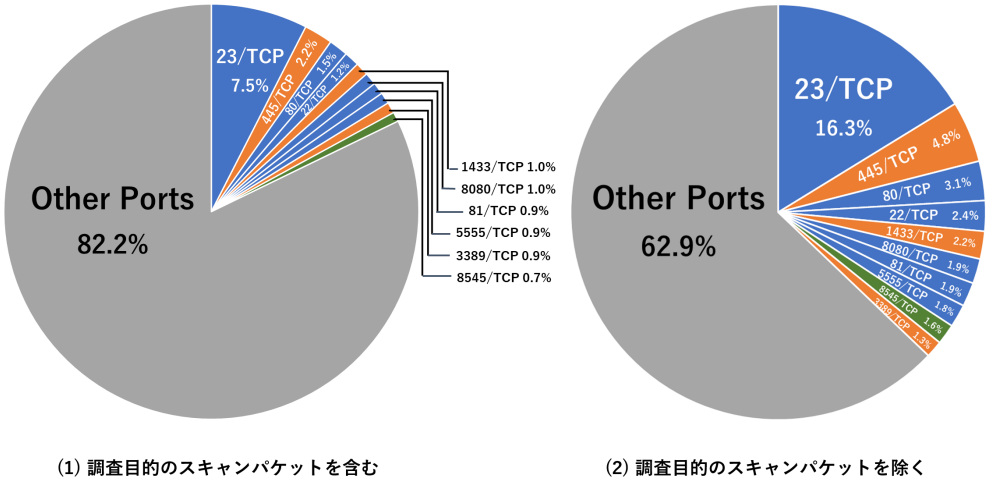


図1: ダークネットにおける日ごとの観測パケット数の推移
（青：調査目的のスキャン，赤：それ以外，積み上げグラフ）



(1) 調査目的のスキャンパケットを含む　　(2) 調査目的のスキャンパケットを除く

図2: 宛先ポート番号別の年間観測パケット数の割合

に多く観測されました．3 番目以降も 2019 年と同様の傾向であり，IoT 機器の Web インターフェイスが動作する 80/TCP，8080/TCP，81/TCP，サーバ等の遠隔操作で使用される SSH（Secure Shell）の 22/TCP，Microsoft SQL Server で使用される 1433/TCP が上位に観測されました．

3. 観測事象の分析

本章では，2020 年にダークネットおよび各種ハニーポットの観測において確認された事象の分析事例として，次の 5 つの事例を説明します．

- Mirai 感染ホスト数の推移（3.1節）
- 宛先ポートセットの分析により確認された感染拡大活動（3.2節）
- ADB が有効な機器の感染事例（3.3節）
- 国内のブロードバンドルータ製品を狙った Mirai 亜種の感染活動（3.4節）
- 大規模なバックスキャッタ（3.5節）

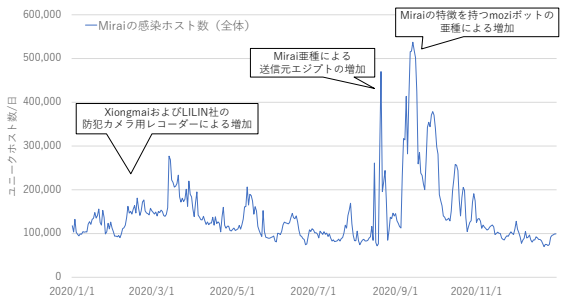


図3: Mirai の感染ホスト数の推移（全体）

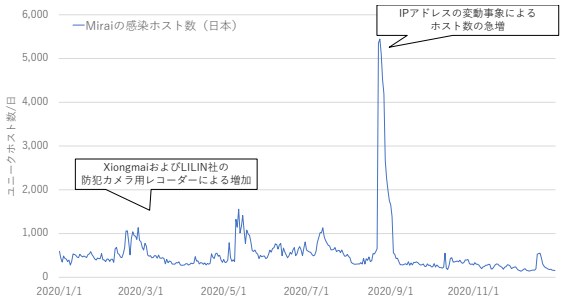


図4: Mirai の感染ホスト数の推移（日本）

3.1. Mirai 感染ホスト数の推移

IoT ボットとして有名な Mirai とその亜種は，スキャン時に生成する TCP の SYN パケットに固有の特徴*7を持っています．そのため，ダークネット観測においてこの特徴を持つパケットの送信元 IP アドレスを集計することにより，Mirai とその亜種に感染したホストの台数を推計することができます．

本節では，この特徴に基づいて，世界全体と日本国内における Mirai とその亜種の感染ホスト（以降，「Mirai 感染ホスト」と呼ぶ）を推計し，その推移を分析します．

3.1.1 Mirai 感染ホスト数の推移（全体）

世界全体における Mirai 感染ホスト数の日ごとの推移を図 3 に示します．感染ホスト数は全世界で概ね 10 万から 20 万程度で推移しましたが，2 月〜5 月頃，8 月中旬頃，9 月中旬に一時増加し，最大 50 万ホストが観測されました．

2 月の増加は Xiongmai 社の防犯カメラ用レコーダの脆弱性 [3, 4]，3 月と 5 月の増加は LILIN 社の防犯カメラ用レコーダの脆弱性 [5] を悪用した感染活動がそれぞれ原因でした．

8 月中旬の増加は，主にエジプトで広がった Mirai 亜種の感染活動が原因でした．入手した検体を解析した結果，防犯カメラ用レコーダやルータ製品の脆弱性を悪用した攻撃通信を行うことはわかりましたが，実際にエジプトで感染した機器の特定には至っていません．

9 月中旬からの増加は，主にインドと中国で Mozi ボット [6, 7] への感染が広がったことが原因でした（3.2 節で説明します）．攻撃の送信元で動作している機器を確認した結果，インドの 2 千以上のホストで ZTE 社のルータの管理画面が確認されたことから，この機種のルータに Mozi ボットが感染したと考えられます．中国における感染機器は特定できていません．

3.1.2 Mirai 感染ホスト数の推移（日本国内）

日本国内における Mirai 感染ホスト数の日ごとの推移を図 4 に示します．年間を通してみると感染ホスト数は減少傾向にありました．

2〜5 月におけるホスト数の増加は，世界全体の事象と同じく，Xiongmai 社と LILIN 社の防犯カメラ用レコーダへの感染拡大が原因でした．このことから，これらの機器の利用者が日本にも存在することがわかります．

8 月末には感染ホスト数の急増が観測されましたが，この急増は，ある 10 台程度の感染ホスト群が 1 台あたり数百回にわたり IP アドレスを ISP から再取得したことにより，これらのホスト群が見かけ上数千ホストとして集計されたことが原因でした [8]．

このほかにも，国内のブロードバンドルータ製品への Mirai 亜種の感染拡大が不定期に観測されました．この事象は 3.4 節で説明します．

3.2. 宛先ポートセットの分析により確認された感染拡大活動

3.1 節では Mirai が送信するパケットに固有な特徴を利用して Mirai 感染ホストの分析を行いました．しかし，Mirai 以外のボットや Mirai の中でもその特徴を持たない亜種の分析にはこの特徴を利用できません．そこで，本節では IoT ボットをはじめとするマルウェアが感染拡大

*7. TCP ヘッダのシーケンス番号と宛先 IP アドレスが同じ値になります．ただし，3.2節に示すように，この特徴を持たない Mirai 亜種も観測され始めています．

表2: スキャンポートごとのグループ

グループ	スキャン対象のポートセット	ホスト数増加の観測時期
A	23, 80, 81, 1023, 2323 5555, 7574, 8080, 8443, 37215, 49152, 52869/TCP	2019 年 9 月～
B	80, 1433, 6379, 6380, 7001 7002, 8080, 8088, 9200/TCP	2019 年 3 月～
C	22, 23, 26, 222, 443 444, 666, 830, 2002, 2022, 2222, 2223, 2323, 2382, 3389 4118, 5554, 5555, 6000, 7777 8022, 8888, 9000, 9090, 9999 22222, 50000/TCP	2020 年 9 月～

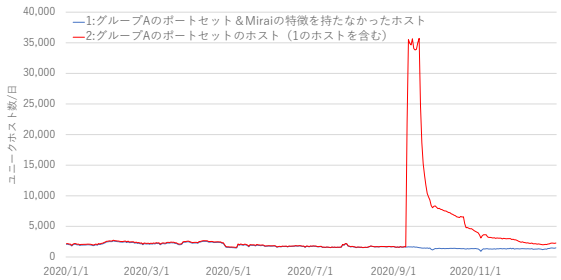


図5: グループ A のホスト数の推移

を目的としたスキャンにおいて使用するポート番号の組み合わせ（ポートセット）に着目して分析を行います．

マルウェアのスキャン時におけるポートセットの種類は多岐にわたりますので，本節では

- 5 種類以上の宛先ポート番号を含む
- スキャンが 1 ヶ月以上継続

の二つの条件を満たすポートセットをスキャンするホスト群（グループ）の傾向を分析します．2020 年にこの条件を満たしたグループは，少なくとも表 2 に示すグループ A～C の 3 種類が存在しました．

3.2.1 グループ A

グループ A は，12 種類のポートをスキャンするホスト群で，2019 年 9 月中旬ごろから活動が継続して観測されています．このグループは，ハニーポットで収集した検体等の情報から Mozi ボットであると推測しています．

グループ A のホスト数の推移を図 5 に示します．ホスト数は 2020 年前半は一日あたり 2 千前後で推移しており，この時期のグループ A のスキャンには 3.1 節の Mirai の特徴は見られませんでした．しかし，9 月中旬にインドと中国でこのポートセットをスキャンするホスト数が急増した後に，Telnet で使用されていると推測されるポート群（23/TCP，1023/TCP，2323/TCP）のグループ A のスキャンには，Mirai の特徴が存在することを確認しました．この時期に Mozi が Telnet のブルートフォースで使用する ID・パスワードを追加したという報告 [7] と合わせると，この時期の更新により Mozi ボットが Mirai のソースコードを流用するようになったと考えられます．

図6: グループ B とグループ C のホスト数の推移

3.2.2 グループ B

グループ B は，9 種類のポートをスキャンするホスト群で，2019 年 3 月末ごろから観測されています．このグループは，PHP の Web フレームワーク，Hadoop，WebLogic，MSSQL，Redis，Elasticsearch 等，主に Linux サーバで動作するミドルウェアの脆弱性を標的とします．このグループのマルウェアに感染すると，ファイアウォールの無効化やサーバのログ削除，仮想通貨の採掘等が行われます．

グループ B のホスト数の推移を図 6 の青線で示します．年間を通して穏やかな減少傾向にはありますが，一日あたり 1 千台程度が観測されました．送信元の IP アドレスに着目すると，感染ホストには地理的な偏りが見られ，12 月 1 日に確認された 552 ホストのうち，75% 以上が中国のホストで，AS 別にみると 52% を占める 290 ホストが中国の大手 IT 企業が提供するホスティングサービス上で動作していました．

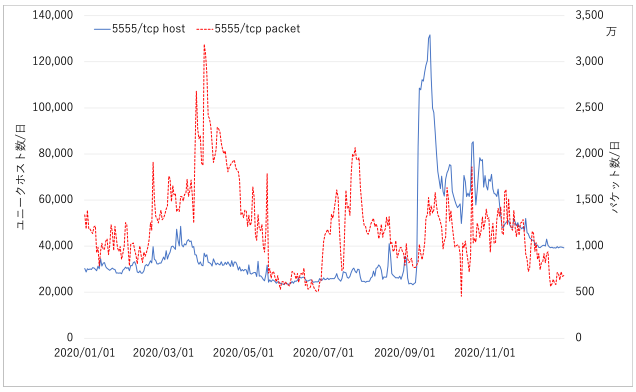


図7: 5555/TCP 宛の攻撃件数，攻撃ホスト数の推移（全体）

3.2.3 グループ C

グループ C は，27 種類のポートをスキャンするホスト群で，2020 年 9 月から活動が観測されはじめました．このグループは，SSH や Telnet が動作していると推測されるポート群のほかに，サービス不明のゾロ目のポート（例えば 666/TCP や 7777/TCP）をスキャンしています．

グループ C のホスト数の推移を図 6 の赤線で示します．2020 年 9 月に初めて確認されてから，その後は減少傾向にあるものの，12 月 2 日に急増し最大 6,433 ホストが確認されました．感染ホストに地理的な偏りは見られませんでしたが，12 月 2 日の急増時には，送信元の 91% 以上がクラウドサービスの EU リージョンの IP アドレスでした．このことから，感染ホストの多くは IoT 機器ではなく，クラウドサービスやレンタルサーバ等の Linux サーバであると考えられます．

また，このグループのホストは，TCP のポート以外にも，UDP の様々なポートに対してプロトコルに則っていないバイト列を送付していることが確認されています．このグループから観測された UDP のポート番号の例としては，1900，4000，5060，5353，6881，8000，8080，8081，8082，8083，11211，30301 が挙げられます．攻撃者が何の目的でこのようなパケットを送付しているのかはわかっていませんが，今後もこのグループの動向を注視する必要があると考えています．

3.3. ADB が有効な機器の感染事例

Android Debug Bridge（ADB）が使用する 5555/TCP を狙った攻撃は，2018 年 2 月から観測されはじめ [9]，2020 年も攻撃数は高い水準で推移しました（図 7）．9 月 11 日から主にインドで，9 月 19 日からは主に中国でホスト数が増加し（この増加は 3.2 節のグループ A によるものです．），ピーク時には世界全体で 13 万ホストに達しました．

ADB で感染拡大を試みるボットが動作する機器では ADB が動作していることが予想されます．そこで，我々は Mirai の特徴を持つパケットで ADB をスキャンする全世界のホストに対して，ADB で接続してその応答を収集し，どのような機器が Mirai 亜種に感染しているのかの実態を調査しました．

- **期間：** 2020 年 10 月 5 日から 11 月 4 日（31 日間）
- **調査対象：** Mirai の特徴をもつパケットで 5555/TCP をスキャンするホスト
- **調査方法：** Mirai の特徴を持つ 5555/TCP のスキャンパケットの送信元に対し，5555/TCP で接続して adb connect のペイロードを送信し，応答を収集．

取得した応答には Android の build property とよばれる機器に関する情報が含まれます．build property の ro.product.name には機器のチップセット名が，ro.product.model には機種名が含まれるケースが大半ですが，これらのパラメータにどのような文字列を設定するかは開発者次第であるため，表記には様々な組み合わせが見られました．

応答を取得できたホストは重複を排除すると 9,161 件，1 日あたり 200〜400 件程度でした．ホストの国別の分布（図 8）を見ると韓国が最も多く全体の 17% となる約 1500 ホストを占め，中国，香港がそれに続きました．日本は 34 番目に多い 27 ホストでした．ホストのインターネット接続回線を種別を見ると，94% がケーブル/DSL，携帯電話網はわずか 4% でした．

取得した応答に含まれる ro.product.name は 363 種類/9,067 件でした．件数の多い順に上位 10 件を表 3 に示します．取得した ro.product.name にはチップセットごとに特徴的な文字列がみられました．最も多かった製品群は，HiSilicon 社の SoC を搭載した機器（ro.product.name

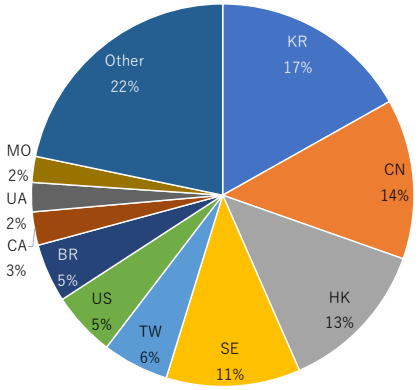


図8: 国別のホスト数（adb）

表3: ro.product.name（上位 10 件）

ro.product.name	件数
Hi3798MV100	1,329
dolphin_fvd_p	825
rk322x_box	695
p281	617
Hi3718CV100	573
etrel_p1	408
mtk_mt5882	271
A95X_R1_SSV6051P	163
rk3288	155
rk3328	132

が Hi の文字からはじまる）で全体の 1/4 を占めました．そのほかにも，ロックチップ社の SoC を搭載する機器や Allwinner 社の SoC を搭載した Android TV Box 製品が多数見られました．搭載されている SoC の特徴や build property 等の情報から，感染した機器の多くは，Android OS を搭載し HDMI 出力を有するメディアプレーヤー端末であり，そのほかにもスマートフォンやタブレット，ドライブレコーダー等の機器が存在することがわかりました．

ADB が出荷時の状態で有効なのか，それともユーザが設定を変更して有効な状態になっているのかについては，観測データからはわかりませんが，ADB を可能な限り無効化しておくとともに，ADB を有効にする場合でもインターネットから接続できないようにする必要があるといえます．

3.4. 国内ブロードバンドルータ製品を狙った Mirai 亜種の感染活動

2017 年 11 月に日本国内で Mirai 亜種の大規模感染が発生しました [10, 11]．この感染拡大は，ロジテック社のブロードバンドルータ製品の内部で動作している UPnP サービスに存在した脆弱性（CVE-2014-8361 [12]）が原因でした [13]．この UPnP サービスは 52869/TCP で動作しており，このポートを狙った攻撃は 2017 年以降継続して観測されています [1, 14, 15]．

そこで，国内で動作している該当製品の実態を把握するため，国内の Mirai 感染ホストに対して 52881/TCP[*8]に接続を行い，感染機器の情報を収集しました．

- **期間：** 2020 年 8 月 27 日から 12 月 31 日（127 日間）
- **調査対象：** Mirai の特徴をもつパケットの送信元 IP アドレス（日本のみ）
- **調査方法：** Mirai 感染ホストの 52881/TCP に HTTP プロトコルでアクセスし，UPnP Description ファイルを収集

取得した UPnP Description ファイルには UPnP 対応デバイスの機器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ます．この UDN に記載されている UUID（Universally Unique Identifier）の下 12 桁には 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 [16]，機器のグローバル IP アドレスが変わったとしてもこの値から同じ機器と特定することができると考えられます．

この UUID を用いて感染ホストを集計した結果，4 ヶ月間で 1,173 件，1 日あたり 10〜450 件程度の感染ホストを確認しました（図 9）．また，IP アドレスを元に集計した感染ホスト数は 2,753 件だったため，UUID を用いて集計することにより機器の IP アドレスの変更の影響を受けず，実態に近い値が得られたといえます．

該当のブロードバンドルータ製品は 10 年以上前に発売された機器で，すでにサポートを終了しており使用は推奨されませんが，2020 年においてもこの機器を使用し続けているユーザが一定数いることがわかります．この機

*8. ロジテック社のブロードバンドルータ製品の一部では，UPnP サービスの Description ファイルが 52881/TCP の特定のパスに外部からアクセス可能な状態で公開されていることがあります．

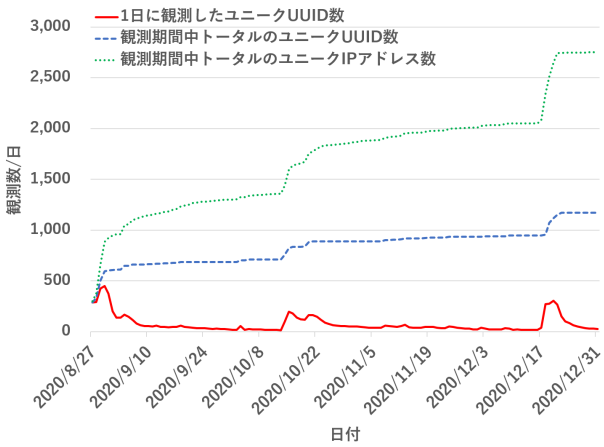


図9: UPnP Description ファイルの UUID の件数

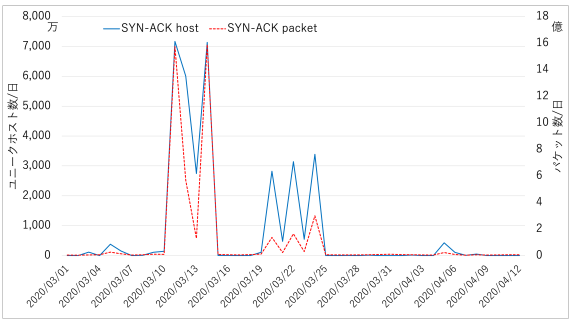


図10: SYN-ACK パケット数とその送信元 IP アドレス数の推移

器だけにかかわらず，今一度ご自身の利用する機器はすでにサポートが終了していないか，最新のファームウェアを使用しているかの確認をお願いします．

3.5. 大規模なバックスキャッタ

ダークネットでは，TCP の SYN パケットに対する SYN-ACK パケットが大量に観測されることがあります．この事象の多くは，攻撃者が送信元を不特定多数の IP アドレスに詐称して SYN パケットを送信する SYN Flood 攻撃と呼ばれる DDoS 攻撃に起因し，このような SYN-ACK パケットはバックスキャッタと呼ばれます．しかし，2020 年 3 月にダークネットで観測された大規模なバックスキャッタは，SYN Flood 攻撃の特徴とは異なる事象が観測されました．本節ではこの事象について説明します．

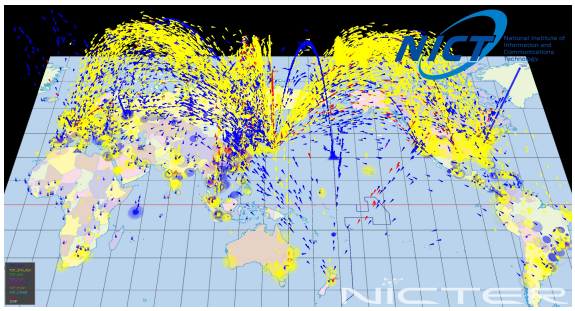


図11: ATLAS による大規模バックスキャッタの可視化

NICTER のダークネット観測網で観測された SYN-ACK パケット数およびその送信元 IP アドレス数の日ごとの推移を図 10 に示します．3 月の初旬に日本を含む全世界からの SYN-ACK パケット数は増加し，3 月 11 日と 14 日には 1 日に観測された SYN-ACK パケット数は 15 億，送信元 IP アドレス数は 7 千万に達しました．この時期のダークネット観測の状況を，NICTER のダークネット可視化システム ATLAS で可視化した画像を図 11 に示します．黄色の点が SYN-ACK パケットを表しており，世界中から SYN-ACK パケットが大量に届いている様子が確認できます．

この大規模バックスキャッタの調査を進めた結果，次の事実がわかりました．

1. SYN-ACK パケットの宛先 IP アドレスには，ネットワーク的な偏りがあること．
2. NICTER で運用している全ポート応答型のハニーポット [17] に，送信元 IP アドレスを NICTER のダークネットの IP アドレスに詐称した SYN パケットが多数届いていたこと．

これらの観測結果から，この事象は SYN Flood 攻撃ではなく SYN-ACK パケットの再送による通信の輻輳を狙った DRDoS 攻撃であり，特定のホストを狙った DDoS 攻撃ではなくネットワークや AS を狙った絨毯爆撃（Carpet Bombing）型の DDoS 攻撃であった可能性が高いと考えられます．

4. DRDoS 攻撃の観測状況

DRDoS（Distributed Reflection Denial-of-Service）攻撃とは，インターネット上の DNS や NTP 等のサーバを

通信の増幅器として悪用し，攻撃対象に大量のパケットを送付する DDoS 攻撃の一種です．我々は横浜国立大学吉岡研究室と共同で，DRDoS 攻撃を観測するハニーポットである AmpPot[18, 19] の研究開発を進めています．本章では，NICTER プロジェクトで運用中の AmpPot が 2020 年に観測した DRDoS 攻撃の傾向について報告します．

本章で分析に使用するデータの観測期間および観測規模は次のとおりです．

- 観測期間：2020 年 1 月 1 日〜12 月 31 日
- 観測規模：AmpPot 9 台（Proxied モード 7 台，Agnostic モード 2 台[*9]）

DRDoS 攻撃では攻撃者から大量のパケットが送信されるため，攻撃を観測する AmpPot でも大量のパケットが観測されます．そこで AmpPot では，攻撃件数や規模を把握しやすいように，AmpPot ごとに同一の攻撃対象（IP アドレス）に対する連続したパケット群をまとめて 1 件の攻撃として集計しています．本章で記述する攻撃件数とはこの集計に基づく件数で，特に断らない限り，上記の 9 台の AmpPot の観測結果を合計したものです．

4.1. DRDoS 攻撃の観測結果

4.1.1 攻撃件数の推移

2020 年に AmpPot が観測した DRDoS 攻撃件数の日ごとの推移を図 12 に示します．2020 年の 1 年間に，AmpPot は累計で約 3,120 万件（前年約 1,917 万件），1 日平均で 8.5 万件（前年約 5.3 万件）の攻撃を観測しました．そのうち，日本宛の攻撃は，累計で約 24 万件（前年約 8 万件），1 日平均で約 666 件（前年約 232 件）でした．

このことから，DRDoS 攻撃の発生件数は増加傾向にあることがわかります．ただし，日本宛の攻撃件数の増加は，不定期に発生する攻撃件数の急増によるもので，これらの急増の多くは特定のクラウドサービスを狙った絨毯爆撃（Carpet Bombing）攻撃[*10]でした．これらの攻撃を除外すれば，2020 年の日本宛の攻撃件数は 2019 年と同等です．

4.1.2 国・地域別の被攻撃件数

国・地域別の被攻撃件数の割合を図 13 に示します[*11]．全攻撃の 1/3 以上がアメリカに割り当てられている IP アドレス宛の攻撃で，2 番目に多い中国を合わせると全攻撃の半数以上，さらに上位 5 カ国で全攻撃件数の約 2/3 を占めているという傾向は 2019 年と変わりません．

表4: DRDoS 攻撃に悪用されるサービス（攻撃件数の多い上位 10 種類）

ポート番号	サービス名	攻撃件数
123/UDP	NTP	15,607,719
389/UDP	CLDAP*	3,751,164
11211/UDP	Memcached	3,475,883
19/UDP	CharGen	1,737,124
53/UDP	DNS	1,359,967
1900/UDP	SSDP	884,793
161/UDP	SNMP	705,861
3702/UDP	WSD*	666,971
1194/UDP	OpenVPN*	477,384
3283/UDP	ARMS*	379,123

4.1.3 攻撃の継続時間

AmpPot が観測した DRDoS 攻撃の継続時間の分布を図 14 に示します．これまでの傾向と同じく全体的に短時間の攻撃が多く，約 27% が 1 分未満（前年約 38%），約 82% が 10 分未満（前年約 87%）の攻撃でした．一方で，1 時間以上の比較的長時間にわたって観測された攻撃は，全体の約 4.3%（前年 2.6%）でした．このことから，2020 年は攻撃の継続時間の分布が 2019 年と比較して僅かではありますが長くなっていることがわかります．

4.1.4 攻撃に悪用されるサービス

AmpPot が観測した攻撃のうち，攻撃に悪用された件数の多い上位 10 種類のサービスを表 4 に示します[*12]．DRDoS 攻撃に悪用される主要なサービスは，昨年から大きな変化はありませんでした．

*9. Proxied モードとは，実際のサーバプログラムをハニーポットとして用いる AmpPot のモードです．Agnostic モードとは，受信パケットに対して（そのサービスのプロトコルを無視して）大きな応答を返す AmpPot のモードです．詳細は [18, 20] を参照して下さい．

*10. ネットワークや AS を攻撃対象として，それらに属する多数の IP アドレスに対して実行される DDoS 攻撃．AmpPot は IP アドレスごとに攻撃件数を集計するため，絨毯爆撃攻撃が発生すると攻撃件数が急増するように見える．

*11. 国情報の推定には MaxMind 社（https://www.maxmind.com/）の GeoIP データベースを使用しました．

*12. 表中の * の付いたサービスは，Agnostic モードの 2 台の AmpPot のみで観測しています

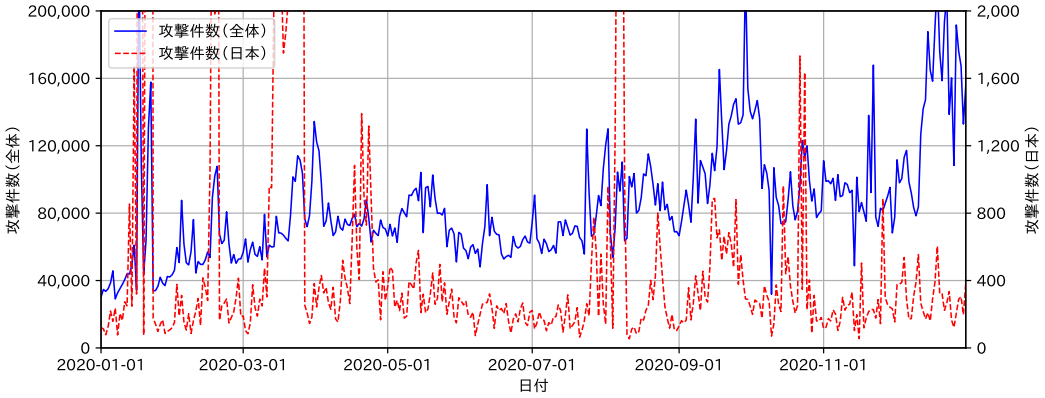


図12: 日ごとの DRDoS 攻撃件数の推移（左軸：全体，右軸：日本宛）

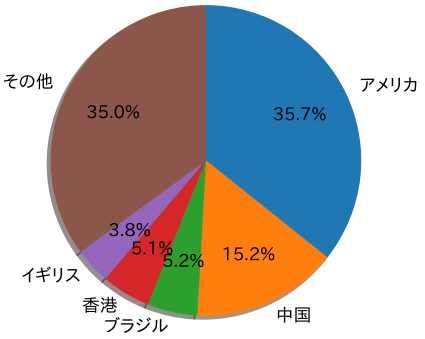


図13: 国・地域別の被攻撃件数

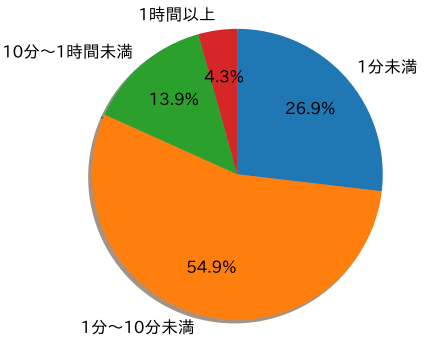


図14: 攻撃継続時間

一方で，2020 年に DRDoS 攻撃に悪用されたサービスの種類は 2019 年と比較して更に多様化したことを確認しました．1 万件以上の攻撃が観測されたサービス数は，

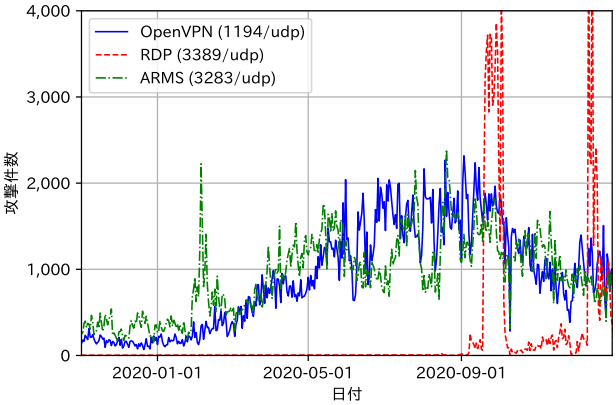


図15: OpenVPN，RDP，ARMS を悪用した攻撃件数の推移

2019 年は 19 種類でしたが，2020 年は 35 種類に増加しました．

4.1.5 マルチベクタ型の攻撃

昨年のレポートで報告した [14]，複数種類の手法を組み合わせたマルチベクタ型の DRDoS 攻撃も 2020 年は微増傾向にあります．2 種類以上の手法を組み合わせた攻撃は，2019 年 12 月は全体の約 14% だったのに対し，2020 年 12 月は全体の約 23% に増加しました．

4.2. その他の観測事象

4.2.1 リモートワークに関連するサービスを悪用した DRDoS 攻撃

2020 年はコロナ禍の中でリモートワークが普及しました．リモートワークに使用される機器がサイバー攻撃の

表5: ランサム DDoS の観測事例

(a) 製造・IT 系

攻撃対象	時刻	悪用されたサービス
A 社	2020/10/07 08:16 - 09:18	CharGen, WSD
B 社	2020/10/08 08:20 - 09:26	CharGen, NTP, WSD
C 社	2020/10/09 08:25 - 09:38	

(b) 通信系

攻撃対象	時刻	悪用されたサービス
E 社	2020/10/13 09:08 - 10:27	CharGen, NTP, ARMS, WSD
F 社	2020/10/13 10:27 - 11:31	
G 社	2020/10/13 11:34 - 12:42	

標的となった事例が報告されています [21] が，それ以外にも，リモートワークで使用されるサービスが DRDoS 攻撃の踏み台として悪用される事例が観測されています [22, 23, 24].

OpenVPN（1194/UDP), RDP（Remote Desktop Protocol; 3389/UDP), ARMS（Apple Remote Management Service; 3283/UDP）のサービスを悪用した DRDoS 攻撃の件数の推移を図 15 に示します．これらのサービスはいずれも遠隔から機器やネットワークを利用するために使用されますが，これらのサービスを悪用した DRDoS 攻撃が 2020 年に増加したことがわかります．

攻撃者がコロナ禍におけるリモートワークに着目してこれらのサービスを悪用しているのかは不明ですが，これらのサービスは DRDoS 攻撃にも悪用される恐れがありますので，不要なサービスをインターネット上に公開しない，アクセス制御を適切に行う等の対策をお願いします．

4.2.2 DDoS 脅迫の観測事例

2020 年 8 月ごろから DDoS 攻撃を示唆して金銭を要求する脅迫行為が国内外で報告されています [25, 26]．我々の AmpPot でもこの事象に関連すると推測される攻撃（ランサム DDoS）が観測されています．

国内の企業を狙った攻撃事例の一部を表 5a と表 5b に示します．表 5a は国内の製造・IT 系の企業を狙った攻撃の事例です．2020 年 10 月 7 日から 9 日にかけて，毎日ほぼ同じ時刻に，同様のサービスを悪用して攻撃が実行されたことがわかります．また，表 5b に示す通信系の企業を狙った攻撃事例では，2020 年 10 月 13 日に 1 時間ずつ次々と攻撃対象を変えながら，攻撃が実行されたことがわかります．

国内外の一連の攻撃事例を分析した結果，攻撃事例の多くは日本時間の午前中に実行され，攻撃の継続時間は 60〜90 分，悪用されたサービスは CharGen，NTP，ARMS，WSD の 4 種類が中心でした．また，観測された国内の事例では，攻撃対象として企業の Web サーバでなく，DNS サーバやそのほかのサーバが狙われる傾向にありました．

5. おわりに

2020 年は 2019 年に引き続き，海外組織による大規模調査スキャンが総観測パケットの約半数を占めるという傾向が継続しました．大規模スキャナに判定された IP アドレスは 2019 年の 1.5 倍以上に増え，多数のスキャナによるスキャンパケット数も増大していることから，この傾向は今後も続くと考えられます．大規模スキャナの中にはその運営組織のわからないものも含まれており，これらの組織がスキャンによって得たデータを何の目的でどのように利用しているのかはわかりませんが，今後も調査スキャンの特徴やスキャンの送信元の分析を通して，大規模調査スキャンの実態を分析する予定です．

IoT ボットの活動については依然として Mirai 亜種の活動が活発に観測されるとともに，2020 年は Mozi と呼ばれる IoT ボットの活動が特徴的でした．ボットが送信するスキャンパケットの特徴に基づく従来の分析に加え，スキャンの宛先ポートセットに基づいた分析を日々行うことで，新たなボットの活動も把握できるようになってきました．観測・分析と研究開発のサイクルを回しながら，今後も新たな脅威に追従できるよう，観測データの分析手法の高度化を進めていく予定です．

AmpPot の観測結果からは，2019 年を大きく上回る数の DRDoS 攻撃が日々発生している状況が明らかになり，ランサム DDoS により日本の企業が攻撃を受けている事象も確認されました．また，DRDoS 攻撃に悪用されたサービスもより多様化し，複数種類の手法を組み合わせる攻撃も増加しています．コロナ禍によりリモートワークが増加し，オンラインサービスへの社会的な依存度が高まる今日，DoS 攻撃はますます大きな社会的脅威になっています．引き続き，観測データの分析による DRDoS の

手法の変化と攻撃活動の全容把握を進めていく予定です．

参考文献

[1] サイバーセキュリティ研究室．NICTER 観測レポート 2018. Technical report, 国立研究開発法人情報通信研究機構, 2019.

[2] 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．In 情報通信システムセキュリティ研究会（ICSS）. 電子情報通信学会, 2020.

[3] Vladislav Yarmak. Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras. https://habr.com/en/post/486856/.

[4] NICTER 解析チーム．ビデオレコーダを狙った 9530/tcp 宛通信の増加について．https://blog.nicter.jp/2020/04/nvr-9530/.

[5] Yanlong Ma, Lingming Tu, Genshen Ye and Hongda Liu. Multiple botnets are spreading using LILIN DVR 0-day. https://blog.netlab.360.com/multiple-botnets-are-spreading-using-lilin-dvr-0-day-en/.

[6] ALEX.TURING, HUI WANG. Mozi, Another Botnet Using DHT. https://blog.netlab.360.com/mozi-another-botnet-using-dht/.

[7] Andreas Klopsch , Prof. Dr. Christian Dietrich , Raphael Springer. A detailed look into the Mozi P2P IoT botnet. https://chrisdietri.ch/talk/mozi_iot_botnet_slides_botconf_202012.pdf.

[8] NICTER 解析チーム．日本国内の Mirai の特徴を持つパケットの送信元 IP アドレス数急増について．https://blog.nicter.jp/2020/10/jp_mirai_spike/.

[9] IIJ-SECT．国内 Mirai 亜種感染機器からのスキャン通信が再び増加 (2018 年 2-3 月の観測状況)．https://sect.iij.ad.jp/d/2018/04/057113.html.

[10] サイバーセキュリティ研究室．NICTER 観測レポート：ルータ製品の脆弱性を悪用して感染を広げる Mirai の亜種に関する活動 (2017-12-19)．Technical report, 国立研究開発法人情報通信研究機構, 2017.

[11] JPCERT/CC. Mirai 亜種の感染活動に関する注意喚起．https://www.jpcert.or.jp/at/2017/at170049.html.

[12] IPA JVN iPedia. Realtek SDK の miniigd SOAP サービスにおける任意のコードを実行される脆弱性．https://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-008039.html.

[13] Logitec. ロジテック製 300Mbps 無線 LAN ブロードバンドルータおよびセットモデル（全 11 モデル）に関する重要なお知らせとお願い．https://www.logitec.co.jp/info/2017/1219.html.

[14] 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 2019. Technical report, 国立研究開発法人情報通信研究機構, 2020.

[15] 警察庁 @police．複数の IoT 機器等の脆弱性を標的としたアクセスの増加等について．https://www.npa.go.jp/cyberpolice/detect/pdf/20200130.pdf.

[16] IETF. A Universally Unique IDentifier (UUID) URN Namespace. https://tools.ietf.org/html/rfc4122.

[17] 牧田大佑，島村隼平，久保正樹，井上大介．全ポート待受型の簡易ハニーポットによるサイバー攻撃観測．In 暗号と情報セキュリティシンポジウム (SCIS2019). 電子情報通信学会, 2019.

[18] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow. Amppot: Monitoring and defending against amplification ddos attacks. In International Workshop on Recent Advances in Intrusion Detection, pages 615–636. Springer, 2015.

[19] 横浜国立大学情報・物理セキュリティ研究拠点．AmpPot: Honeypot for Monitoring Amplification DDoS Attack. http://ipsr.ynu.ac.jp/dos/.

[20] 西添友美，牧田大佑，吉岡克成，松本勉．プロトコル非準拠ハニーポットを用いた新種の DRDoS 攻撃の早期検知．In 情報通信システムセキュリティ研究会（ICSS）. 電子情報通信学会, 2017.

[21] JPCERT/CC. JPCERT/CC 活動四半期レポート［2020 年 10 月 1 日～2020 年 12 月 31 日］. https://www.jpcert.or.jp/pr/2021/PR_Report20210121.pdf.

[22] NSFOCUS. What You Should Know about OpenVPN Reflection Attacks. https://nsfocusglobal.com/what-you-should-know-about-openvpn-reflection-attacks/.

[23] NETSCOUT. Microsoft Remote Desktop Protocol (RDP) Reflection/Amplification DDoS Attack Mitigation Recommendations - January 2021. https://www.netscout.com/blog/asert/microsoft-remote-desktop-protocol-rdp-reflectionamplification.

[24] NETSCOUT. A Call to ARMS: Apple Remote Management Service UDP Reflection/Amplification DDoS Attacks. https://www.netscout.com/blog/asert/call-arms-apple-remote-management-service-udp.

[25] Akamai SIRT. RANSOM DEMANDS RETURN: NEW DDOS EXTORTION THREATS FROM OLD ACTORS TARGETING FINANCE AND RETAIL. https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html.

[26] JPCERT/CC. DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について．https://www.jpcert.or.jp/newsflash/2020090701.html.