6-2　パスワード設定不備の IoT 機器における悪用リスクの実態解明
6-2　Investigation of Abuse Risk of IoT Devices with Weak Password Settings

笠間 貴弘　村上 洸介
KASAMA Takahiro and MURAKAMI Kosuke

IoT マルウェア Mirai は初期パスワード等の簡単なパスワード設定のまま利用されていた世界中の IoT 機器に感染を広げ、大規模なサイバー攻撃を実行した。Mirai がもたらした被害を契機に、日本国内のパスワード設定不備の機器の対処を目的とした NOTICE プロジェクトが 2019 年に開始され、5 年間にわたる毎月の調査によって最大 1 万台以上のパスワード設定不備の IoT 機器を検知し所有者への注意喚起につなげている。一方、Mirai やその亜種は感染後に Telnet サービスを停止し他のマルウェア等による機器へのアクセスを阻止する機能を持つことから、NOTICE で検知されているパスワード設定不備の IoT 機器はいまだ Mirai に感染していない可能性が高いと言える。なぜこれらの機器は Mirai に感染していないのか、また未感染の機器はサイバー攻撃へ悪用されるリスクが低いのかを明らかにするため、我々は NOTICE 調査とダークネット観測、IoT 機器の実機調査を組み合わせることで、国内に存在するパスワード設定不備の IoT 機器の悪用リスクの実態調査を行った。本稿では、その調査結果を報告する。

IoT malware Mirai spread the infection to IoT devices that were being used with weak password settings, leading to a large-scale cyber-attack. The impact of Mirai led to the launch of the NOTICE project in 2019 to address vulnerable IoT devices in Japan. NOTICE has detected up to 10,000 or more vulnerable IoT devices through monthly surveys over the past five years and alerted their owners. Since Mirai and its variants have a function to stop Telnet service after infection and prevent access by other malware, it is highly likely that vulnerable IoT devices detected by NOTICE are not yet infected with Mirai. To clarify why these vulnerable IoT devices remain uninfected by Mirai and whether uninfected devices pose a low-security risk, we surveyed the abuse risk of IoT devices with weak password settings in Japan by combining NOTICE surveys, darknet observations, and investigation of IoT devices. This paper reports the results of the survey.

1　はじめに

2016 年に登場したマルウェア Mirai が全世界の IoT 機器に感染し数百 Gbps 規模の DDoS 攻撃（分散型サービス妨害攻撃）を実行したことで、IoT 機器のセキュリティリスクが広く一般に認知された [1]。ハッカーフォーラムで公開された Mirai のソースコード [2] を見ると、Mirai はインターネット上の 23/TCP 及び 2323/TCP で Telnet サービスが動作する機器を探索し、応答があった機器に対して内部に保持する ID/Password リストを順に入力することで機器にログインを試み、ログインに成功した機器へ感染する機能を有していることがわかる。更に Mirai やその亜種（以下、単に Mirai と呼ぶ）は感染に成功した機器上で Telnet サービスを停止することで、当該機器への他の Telnet アクセスを禁止し他のマルウェアの侵入等を阻害する機能を持つことが知られている。

一方、2019 年に開始した NOTICE プロジェクト [3] において我々は国内約 1.13 億 IPv4 アドレスを毎月調査し、脆弱（ぜいじゃく）なパスワードが設定されている機器として多い月で Telnet・SSH に関して約 2,000 台、HTTP（S）に関して約 10,000 台以上を検知している。少なくとも Telnet に関して、これらの機器が仮に Mirai に感染していた場合は NOTICE 調査によるアクセスは阻害されるはずであることを考慮すると、NOTICE で検知されたパスワード設定に不備のある IoT 機器はいまだ Mirai に感染していない可能性が高いと言える。しかしながら、なぜこれらの脆弱であるはずの機器が Mirai に感染していないのか、また感染していないということはサイバー攻撃に悪用されるリスクは低いと

言えるのかその実態は明らかではない。そこで我々は、まずこれらの機器の Mirai 等への感染有無についてサイバーセキュリティ研究室で実施しているサイバー攻撃観測システム NICTER のデータと突合することで検証を行った。その上で、NOTICE で検知した機器の実機調査を通じて Mirai の感染に至らない要因を明らかにするとともに、攻撃者の視点から機器へのログイン成功時にサイバー攻撃への悪用が可能か否か調査を行った。

2　ダークネット観測結果との突合による Mirai 感染有無の調査

2.1　ダークネットで観測した国内の Mirai 感染ホスト

NICTER [4] はサイバーセキュリティ研究室で研究開発している、未使用の IP アドレス空間（ダークネット）に届くトラフィックを観測することでマルウェア感染機器からのスキャン活動を観測・分析するシステムであり、国内外の組織と連携して約 30 万アドレスの大規模観測網を構築している。Mirai は次の攻撃先を探索するスキャンパケットを raw ソケットで生成し TCP シーケンス番号に宛先 IP アドレスと同じ値を用いることが、公開されたソースコードから知られている。通常のパケットにおいてこの 2 つの値が偶然一致する確率は低いことから、上記の特徴を持つスキャンパケットは Mirai に感染した機器からのスキャンパケットであると判定できる。その判定条件を基に、図 1 に 2021 年 2 月から 5 月にかけての NICTER で観測した日本国内の Mirai 感染ホスト数（IP アドレス数）の推移を示す。日によって増減はあるもののおおむね 1 日辺り平均 500 ホスト前後が国内の Mirai 感染機器として観測されていることがわかる。

2.2　NOTICE で検知した国内のパスワード設定不備機器

NOTICE 調査では、月 1 回の頻度で調査対象の IP アドレスに対してスキャンを行い、ログイン試行が可能である機器に対して約 600 種類の ID/Password リストを用いてログインを試みる。図 2 に Mirai が攻撃対象とする 23/TCP 及び 2323/TCP で稼働する Telnet サービスに対して調査を行い、ログイン及び機種特定に成功した件数を示す。図 2 を見ると、Telnet のパスワード設定不備の機器に関して大半はデフォルトポートである 23/TCP で発見されており、2323/TCP でログイン成功した機器はわずかであることがわかる。なお、23/TCP と 2323/TCP の両方でログイン成功した機器はなかった。

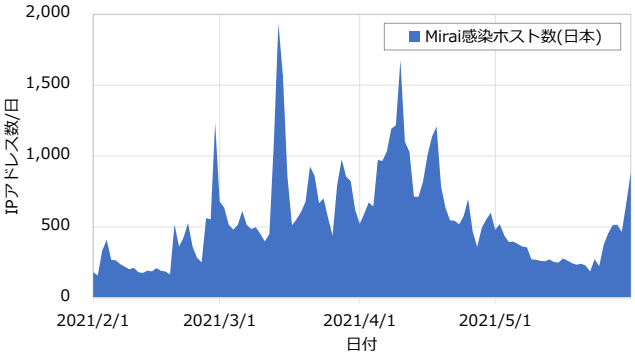

図 1　日本国内の Mirai 感染ホスト数の推移

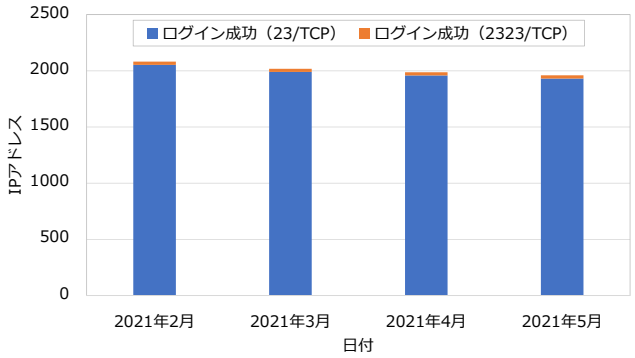

図 2　Telnet のパスワード設定不備機器数（機種特定成功のみ）

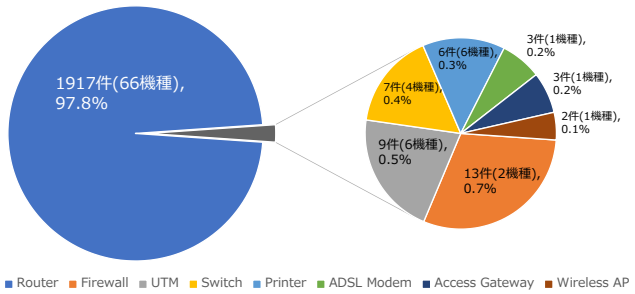

図 3　Telnet ログイン成功機器の機種特定結果

図 3 に 2021 年 5 月調査時にログイン成功した 1,960 アドレスの機器についてカテゴリ別の件数を示す。図 3 を見ると、Telnet でログイン成功した機器の大半（97.8 %）をルータが占めている。ルータ以外としてはわずかにファイアフォール機器、UTM（Unified Threat Management）機器、ネットワークスイッチ、プリンタといった機器が含まれており、全体として 19 ベンダ 87 機種の機器が発見された。

2.3　調査結果の突合による Mirai 感染有無の検証

2.2 で示した各月の NOTICE 調査で検知された機器が Mirai に感染しているか否かを確認するために、NICTER 観測結果と突合し、各機器の IP アドレスを送信元とした Mirai のスキャンパケットが観測されていたか調査した結果を表 1 に示す。なお、IP アドレス

表 1　NOTICE で検知された機器の Mirai 感染有無

調査月	ログイン成功アドレス (Telnet)	Mirai 感染確認
2021 年 2 月	2,082	0
2021 年 3 月	2,018	1
2021 年 4 月	1,987	0
2021 年 5 月	1,960	0

の付け変わりによる誤判定を避けるため、各機器にログイン成功した日の前後 1 日の期間のダークネット観測結果と突合を行っている。表 1 を見ると、NOTICE 調査によってログイン成功した機器からは 1 アドレスを除いてスキャン活動は観測されていなかった。Mirai が 160 pps という高速なスキャンを行うことと、NICTER ダークネット観測において日々世界中で数万台以上の Mirai に感染した機器が観測されていることを考慮すると、NOTICE で検知されている機器がたまたま Mirai からの攻撃を受けていないとは考えづらく、これらの機器は Mirai の攻撃を受けているにも関わらず何かしらの要因によって感染には至っていないと判断できる。

3　パスワード設定不備の機器が Mirai に感染していない要因の特定

NOTICE で検知している国内約 2,000 台の Telnet のパスワード設定不備の機器がなぜ Mirai に感染していないのかその要因を分析する。公開された Mirai のソースコードの分析によって Mirai の一連の攻撃処理において感染成否に影響を与える可能性のある要因として以下の 3 つの項目を洗い出し、調査を行った。

3.1　調査項目

(1) 機器の Telnet バナー

Telnet は単純なテキストベースの通信プロトコルであり、ID やパスワード入力待ちの状態をクライアント側に伝える制御コード等は存在しない。そのため、Telnet を用いて遠隔の機器へログインする場合、通常クライアントはサーバから受け取ったテキストデータ（例えば「Login:」や「Password:」のようなテキスト）を基にサーバの ID やパスワードの入力待ち状態を判定し適切な入力を行う必要があるが、このログイン手順やテキストメッセージは機器によって異なる。実際の Mirai の攻撃手順では、まず ID 入力待ちのバナー情報に含まれる可能性の高い「:」(0x3a)、「>」(0x3e)「$」(0x24)、「#」(0x23)、「%」(0x25) のいずれかの文字か、もしくは「ogin」(login と Login の両方にマッチさせるため L を除外) か「enter」をバナー情報から見つけた場合に ID 入力を行っている。ID 入力後は、ID 入力待ち判定から「%」(0x25) を除いた残りの 4 文字を見つけるか、「assword」(同様に password と Password にマッチさせるため P を除外) を見つけた場合に、パスワード入力待ち状態と判定してパスワードを入力する。同様にパスワード入力後はバナー情報から認証成功を判定し、更にいくつかのコマンドが機器上に存在することを確認した後に感染のためのコマンド実行処理に移る。この Telnet ログイン時の各判定基準に合致しない機器の場合、Mirai は ID 入力やパスワード入力を行わないため感染には至らない。そこで、各機器の Telnet バナーを調査し、Mirai の判定基準に合致しているかを調査した。

(2) ID/Password リストのカバレッジ

当然だが、Mirai が用いる ID/Password リストに機器に設定されている ID/Password が含まれない場合はログインに成功せず感染には至らない。Mirai はソースコード内に 62 組の ID/Password リストを内包しているため、NOTICE で発見された機器においてこれらの ID/Password が設定されていなければログインは成功しないと判断できる。そこで、各機器について NOTICE 調査時でログイン成功した際の ID/Password が Mirai の ID/Password リストに含まれるかを調査した。なお、一部の Mirai 亜種はオリジナルの Mirai が用いる ID/Password リストから一部を追加・削除した異なる ID/Password リストを感染拡大に用いていることが知られているが、今回の分析ではそれらは対象とせずにオリジナルの ID/Password リストのみを用いた。

(3) 機器上の BusyBox の有無

Telnet でのログインに成功した後、Mirai は BusyBox [5] を用いて wget や tftp、echo コマンドを使用して Mirai 本体のバイナリファイルをダウンロード・実行させることで感染する。BusyBox は標準 UNIX コマンドとして提供される様々なプログラムを単一の実行ファイルとして提供するプログラムであり、多数の組み込みシステムや IoT 機器などで用いられている。Mirai がログインに成功しても当該機器上に BusyBox が存在しない場合は感染には至らないため、各機器内に BusyBox と Mirai が感染に用いるコマンドが用意されているかを調査した。

3.2　調査結果

2021 年 5 月の NOTICE 調査で発見した 1,960 台の機器について、上記の 3 つの要因の影響を調査し 4 つのパターンに分類した結果を 2 に示す。まず、Mirai による Telnet のバナー判定条件に合致しない機器（パターン 1）は存在せず、全ての機器で Mirai による ID/

表 2　Mirai の感染処理の失敗パターン

	Telnet バナー	ID/Password 設定	BusyBox の有無	IPs
パターン 1	Fail	–	–	0
パターン 2	Pass	Fail	–	158
パターン 3	Pass	Pass	Fail	266
パターン 3*	Pass*	Pass*	Fail	1,536

Password の入力とログイン成功判定が行われる。次に、機器に設定されていた ID/Password が Mirai の ID/Password リストに含まれていなかった機器（パターン 2）は全体のわずか 8 % の 158 アドレスに留まっており、9 割以上の 1,802 台の機器は Mirai が用いる ID/Password リストで認証を突破されてしまうことが明らかとなった。最後に、Mirai によって認証が突破される機器について BusyBox の有無について検証した結果、全ての機器で BusyBox が存在していなかった（パターン 3、パターン 3*）。すなわち、NOTICE で Telnet のパスワード設定不備が検知された機器は、大半が Mirai の攻撃によって認証が突破され機器内に侵入されてはいるものの、Mirai がマルウェアのダウンロード・実行のために利用するコマンドが機器に存在しなかったことが要因で感染まで至っていなかったと判断できる。

ここで、表 2 におけるパターン 3 とパターン 3* の違いについて説明する。パターン 3* には、Telnet アクセス時に ID の入力が不要でパスワード入力のみが求められる機器が該当していた。前述したとおり、Mirai によるログイン試行は ID 入力、パスワード入力、ログイン判定の順に進むため、ID 入力が不要な機器では本来適切なログイン処理は行えない。しかし、パターン 3* に該当する機器が返すパスワード入力待ち状態のバナー情報は Mirai の ID 入力待ち判定条件にマッチするため、Mirai は ID 入力待ち状態と誤判定し ID 入力を行う。その後、ID 入力を受け取った機器は認証失敗のメッセージと再度パスワード入力待ちを示すバナー情報を返すが、このバナー情報が今度は Mirai のパスワード入力待ち判定条件にマッチすることでパスワードが入力され、パスワードが一致した場合は認証に成功する。すなわち、パターン 3* の機器は Mirai の Telnet バナーの誤判定によって偶然ログインに成功している機器と言える。

4　実機を用いたログイン成功後の悪用リスクの検証

3 の調査によって、NOTICE で検知されている Telnet のパスワード設定不備の機器は、主に Mirai が感染時に使用するコマンドが機器上にないことが要因で感染に至っていないことが明らかとなった。しかしながら、この調査結果からはあくまでも Mirai が用いる感染手順が失敗することを示しただけであり、ログイン成功後に当該機器がサイバー攻撃に悪用される可能性は否定できない。そこで実機を用いて各プロトコルでログインした後に利用できるコマンドや機能を調査し、それらを用いた悪用リスクの調査を実施した。

4.1　Telnet ログイン後の悪用リスクの調査項目

NOTICE 調査で Telnet サービスに対するログインに成功した機器のうち、16 ベンダ 35 機種を調査対象機器として選定した。図 3 で示したとおり NOTICE で発見した機器の多くがルータであることからルータから最も多い 28 機種を選定し、残りはスイッチを 2 機種、NAS（Network Attached Storage）を 1 機種、UTM（Unified Threat Management）機器を 2 機種、AP（アクセスポイント）機器を 1 機種、リモートアクセス装置を 1 機種選定した。これらの機器に対してログイン後の機能等を調査し、以下に示す操作が実行可能か検証した。

(1) 任意プログラムの実行

ログイン後に攻撃者が用意する任意のプログラムを当該機器上で実行させることが可能かを検証する。なお、プログラムは実行可能ファイルのみではなく、スクリプトファイルやバッチファイルも調査対象とした。加えて、任意のリモートホストからプログラムファイルを取得可能かについても検証する。Mirai も感染時にはリモートホストからマルウェア本体を取得・実行することで、機器の環境に合わせたマルウェアの配布などを実現している。

(2) プログラムの永続化

任意プログラムの実行が可能な場合に、当該プログラムの永続化（再起動後に自動実行されるようにすること）が可能かを検証する。例えば、IoT 機器で読み取り専用のファイルシステムが用いられている場合などでは、仮に侵入できた場合でもマルウェアを不揮発領域に書き込むことができずに機器の再起動時に感染前の状態に戻ってしまう。プログラムの永続化の可否は攻撃者が当該機器を継続的に悪用できるかに大きく影響する要素である。

(3) 機器設定情報の操作

ログインに成功した機器に保存されている重要な設定情報が取得･変更できるかを検証する。例えば、ルータの場合では機器内に PPPoE の認証情報や VPN の認証情報が設定・保存されているケースがあり、仮にこれらの情報を攻撃者が取得できた場合は利用者になりすました回線の利用や VPN 経由での攻撃活動が可能になるなど大きなリスクにつながることから、これら 2 つの設定情報が取得・変更できるかを確認した。

表 3　実機を用いた悪用可能性の検証結果 (Telnet)

大項目	小項目	実行可能	管理者権限でのみ実行可能	実行不可
任意プログラムの実行	任意プログラムの実行	6	11	18
	リモートホストからのファイル取得	8	9	18
プログラムの永続化	プログラムの永続化	3	11	21
機器設定情報の操作	機器設定情報の取得	18	7	10
	機器設定情報の変更	9	16	10
外部への攻撃通信	任意のリモートホストへの接続	12	9	14
	任意のペイロードの送信	3	6	26
	送信元詐称パケットの送信	3	2	30

(4) 外部への攻撃通信

ログイン後に任意のリモートホストへの攻撃通信が可能かを検証する。具体的には Telnet や SSH クライアントを利用したリモートホストへの接続が可能かを確認することで、Mirai のような Telnet/SSH を経由した他の IoT 機器への感染拡大が可能か検証する。

また、ネットワークプログラミングのできる任意プログラム実行が可能な場合には、任意のペイロードを付加したパケットの送信可否や送信元アドレスを詐称したパケットの送信可否についても検証する。任意ペイロードのパケット送信が可能な場合は脆弱性を悪用する攻撃通信等が可能になり、送信元アドレスの詐称が可能な場合はリフレクション攻撃[*1]に用いることができる。さらに任意ペイロードのパケットが送信可能な機器については、DoS 攻撃の能力を検証するためにパケットサイズを 60 byte 及び 1,500 byte パケットに設定した UDP パケットを連続送信することで送信可能な最大通信速度の測定を行う。

4.2　Telnet ログイン後の悪用リスク調査結果

表 3 に上記で示した各操作が可能であった機種数を示す。なお、一部の機器においては管理者権限でのみ実行可能な操作が存在したため表中では分けて集計している。6 機種についてはマニュアル調査や実機調査を行ったもののログイン後に実行可能なコマンドに関する情報が得られず一般的な UNIX コマンド等も存在しなかったことから、今回の調査では全ての項目について実行不可に分類した。

まず、任意プログラム実行に関しては 35 機種中 17 機種で実行可能であったが、11 機種については管理者権限のみで実行可能でありログイン成功したアカウントがユーザ権限の場合には権限昇格が必要になる。実行可能なプログラムファイルについては、17 機種中 7 機種ではバッチファイルのみが実行可能でありバッチ処理で実行できる機能は各機器に用意されているコマンドに依存している。残りの 10 機種では実行可能ファイルやスクリプトファイルの実行が可能であった。これらの 17 機種では管理者権限が求められる機種も含め全機種でリモートホストからのファイル取得が可能であり、侵入後に外部からプログラムファイルをダウンロード・実行することができた。さらにプログラムの永続化に関しては、任意プログラムの実行が可能な 17 機種中 14 機種で実行可能であることがわかった。つまり 35 機種中約半数の機種では現時点で Mirai には感染していないものの、ログイン成功後にマルウェア感染と同等の操作が可能であることが明らかとなった。

機器設定情報(PPPoE や VPN の認証情報)の操作に関しては、25 機種で設定情報の取得が可能であった。これらの設定情報が取得可能な機種のうち 18 機種は権限昇格無しに情報が取得可能であったことから、設定情報の取得は任意プログラム実行や外部通信等の操作よりも容易に実行可能だと言える。一方、設定変更については上記 25 機種全てで実行できたものの 16 機種では管理者権限が必要であった。

外部への攻撃通信に関しては、任意ホストへの Telnet もしくは SSH による接続は 21 機種で可能であり、そのうち 12 機種では管理者権限無しに実行が可能であった。これは当該機種を踏み台として他のホストに対する感染拡大が可能となることを示している。一方で、任意ペイロードのパケット送信と送信元詐称パケットの送信が可能な機種についてはそれぞれ 10 機種、6 機種に限定されており、任意ペイロードのパケット送信が可能である 10 機種の内 4 機種は対象機種上で利用できるスクリプト言語を通じて当該機能を実現できるがペイロードに指定できるデータ形式は文字列型

*1　リフレクション攻撃とは、送信元の IP アドレスを攻撃対象の IP アドレスに偽装したパケットを特定のサービス (DNS 等) に対して送信することによって、サービスからの増幅された応答を攻撃対象に送り付ける攻撃のこと。

に限定されていた。任意ペイロードの送信が可能なこれらの計10機種では、侵入後にリモートホストへのエクスプロイトコード送信などに悪用される可能性がある。

任意ペイロードのパケット送信が可能な機器において、外部に対する DoS 攻撃に悪用した場合の攻撃能力（通信速度）を調査した結果、ショートパケット（60 byte）の送信では最大で 63.7 Mbps（99.4 kpps）、ロングパケット（1,500 byte）の送信では最大で 880.7 Mbps（75.8 kpps）でデータ送信可能な機器が確認された。実際には機器が接続される回線品質を含めた諸条件により通信速度は調査値より下がる可能性があるが、1 台の機器であっても数十 Mbps から最大で 1 Gbps 弱の大量通信を発生させることができ、通常のサーバや PC 環境と比べて遜色のない攻撃能力を持つことが明らかとなった。

4.3　WebUI ログイン後の悪用リスク調査結果

NOTICE 調査では、HTTP(S) の Basic/Digest 認証に対するログイン試行を 2022 年 6 月に開始し、2022 年 12 月までの調査を通じて HTTP(S) のパスワード設定不備の機器として 82 ベンダ 422 機種を発見している。図 4 に 2022 年 12 月時の NOTICE 調査にて Basic/Digest 認証に対するログインに成功した機器についてカテゴリ別の分布を示す。図 4 を見ると、Telnet と同様にルータが最も多く検知されているが、Telnet と異なる点として WebUI を備えたネットワークカメラが約 20 % を占めている。HTTP(S) による WebUI へのログイン成功時の悪用リスクを明らかにするため、Telnet と同様に NOTICE 調査でログイン成功した機器から 16 ベンダ 62 機種を調査対象として選定し、**4.1** で調査した同様の操作が WebUI に用意された機能を通じて実行可能か調査を実施した結果を表 4 に示す。なお、HTTP(S) 独自の調査として WebUI を起点とした CLI（Command Line Interface）からの再侵入のリスクを検証するために、WebUI から Telnet 及び SSH サービスの CLI サービスを起動可能であるかも調査した。

まず、任意プログラムの実行や永続化については Telnet ログイン成功後と比較して実行可能な機種は限定されており、特定のベンダの製品 6 機種のみが実行可能であった。

これらの機種では WebUI 上で CLI コマンドやスクリプトを入力できる機能が用意されており、リモートホストからのファイル取得・実行も可能であるため、任意のサーバ上からの任意のプログラムファイルの取得・実行が可能であった。一方、機器設定情報の操作に関しては大半の機器で実行可能であり、51 機種において PPPoE もしくは VPN の設定情報の取得・変更が可能であることが分かった。なお、残りの 11 機種はいずれも機種のカテゴリがルータ以外であり、機器設定情報の操作ができないのではなく、そもそも機種に PPPoE 及び VPN 接続の機能が備わっていなかったため実行不可となっている。

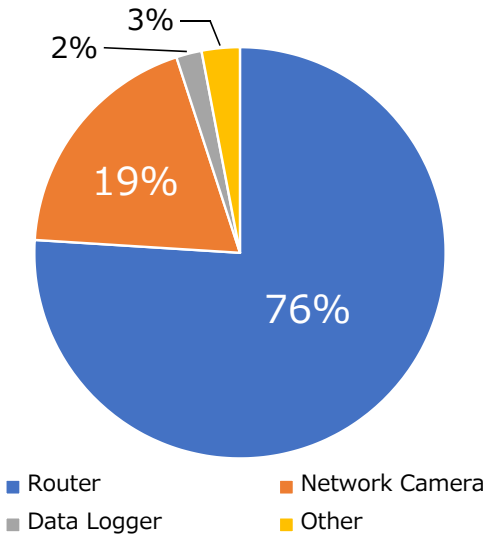

図 4　HTTP(S) ログイン成功機器の機種特定結果

外部への攻撃通信に関しては、任意のプログラムの実行が可能であった 6 機種では Telnet や SSH クライアントの利用は禁止されていたが、スクリプトファイルからソケット通信ライブラリを用いることでリモートホストへの接続が行えた。ただし、送信可能なデータについては文字列型に制限されていることを確認したため、リモートエクスプロイト攻撃の実行には制限がある。当該 6 機種について UDP パケットを連続送信するスクリプトを作成して通信速度を測定した結果、ショートパケット（60 byte）では最大 38.4 Mbps（82 kpps）、ロングパケット（1,500 byte）では最大 326.9 Mbps（27.9 kpps）の速度でデータ送信可能な機種を確認した。この数値は Telnet に関する調査結果よりは小さい値となっているが、WebUI 経由の侵入であっても Telnet 侵入時と遜色ない DoS 攻撃が実現可能な機器が存在することを示している。

追加のサービス起動に関しては、WebUI から Telnet サービスを起動可能な機種は 19 機種、SSH サービスを起動可能な機種は 12 機種存在した。これらの機器に関しては、WebUI へ侵入できた攻撃者が上記サービスを起動し、CLI から再侵入されるリスクが想定される。

4.4　侵入されるサービスによる悪用リスクの差異

我々が実施した調査結果から、Telnet へのログイン成功時には半数以上の機種が任意プログラムの実行や外部への攻撃通信が可能である一方、HTTP(S) を用

表 4　実機を用いた悪用可能性の検証結果 (HTTP(S))

大項目	小項目	実行可能	実行不可
任意プログラムの実行	任意プログラムの実行	6	56
	リモートホストからのファイル取得	14	48
プログラムの永続化	プログラムの永続化	6	56
機器設定情報の操作	機器設定情報の取得	51	11
	機器設定情報の変更	51	11
外部への攻撃通信	任意のリモートホストへの接続	6	56
	任意のペイロードの送信	6	56
	送信元詐称パケットの送信	0	62
サービス起動	Telnet	19	43
	SSH	12	50

いた WebUI へのログイン成功時にはこれらの操作が実行できる機種は限定的であることが明らかとなった。これは Telnet や SSH などの CLI サービスは通常エンジニアや ICT 技術に詳しいユーザがアクセスするものであることから自由度の高い操作が可能な機器が多い一方、WebUI などの GUI(Graphical User Interface)は一般ユーザも多くアクセスすることから機器の設定確認や変更といった機器に応じた特定の操作を行うための専用画面が用意されており操作の自由度が限定されることが影響していると考えられる。すなわち、CLI と GUI のサービスを比較した場合には一般的には CLI サービスに対する不正アクセスの方がマルウェア感染につながるリスクが高いと言える。一方で、機器設定情報の取得・変更については WebUI へのログイン成功時に多くの機器で実行可能であった。これらの操作だけでは Mirai のような直接的なマルウェア感染にはつながらないものの、PPPoE の認証情報や VPN 設定情報の取得が可能であり、サイバー攻撃の踏み台として悪用される可能性がある。

ただし、WebUI へログイン成功した際に Telnet や SSH の CLI サービスを新たに起動できる機器も一定割合存在しており、GUI への不正アクセスを起点に CLI サービスからの侵入が行える機種も存在することから注意が必要である。

5　おわりに

2019 年からの NOTICE 調査を通じて、我々は日本国内に存在する多数のパスワード設定不備の機器を検知してきた。そして検知した機器の通知と並行して、他の攻撃観測データとの突合分析や実機を用いた調査によって、パスワード設定不備のある機器の悪用リスクを正確に把握するための検証を行っている。我々は、NICTER ダークネット観測結果との突合によって NOTICE 調査で検知されている機器が IoT マルウェア Mirai に感染していないことを明らかにし、なぜそれらの脆弱であるはずの機器がマルウェア感染に至っていないかの要因を特定することに成功した。また、実機調査を通じてログイン成功後の機器悪用リスクの調査を行い、NOTICE 検知機器の多くで任意プログラムの実行や外部への攻撃通信の送信など攻撃活動につながる操作が実行可能であることを実証した。これらの結果から、NOTICE で検知されている機器の多くはたまたま現時点において Mirai の感染を免れているだけであり、攻撃者が機器に合わせた悪用方法を実行することで直ちにサイバー攻撃に悪用されてしまうリスクがあり、迅速な対処が必要であることが明らかとなった。本稿で紹介した成果を含め、興味のある方は発表済み論文を参照されたい [6]–[11]。我々は NOTICE 調査による注意喚起を通じて、国内のパスワード設定不備の機器の対処を進め、日本国内の IoT 機器のセキュリティ向上に引き続き取り組んでいく。

【参考文献】

1　Krebs on Security, “DDoS on Dyn Impacts Twitter, Spotify, Reddit,” https://krebsonsecurity.com/2016/10/ddoson-dyn-impacts-twitter-spotify-reddit/
2　jgamblin, “Mirai-Source-Code: Leaked Mirai Source Code for Research/IoC Development Purposes,” https://github.com/jgamblin/Mirai-Source-Code
3　NOTICE SUPPORT CENTER, “NOTICE ｜サイバー攻撃に悪用されるおそれのある IoT 機器の調査、注意喚起を行うプロジェクト,” https://notice.go.jp/
4　国立研究開発法人情報通信研究機構, “NICTERWEB,” https://www.nicter.jp/
5　“BusyBox”. https://www.busybox.net/
6　村上 洸介, 笠間 貴弘, 井上 大介, “ID/Password 設定に不備のある IoT 機器におけるマルウェア感染可能性の大規模調査,” 電子情報通信学会 信学技報, vol.121, no.122, pp.147–152, 2021.
7　村上 洸介, 笠間 貴弘, 藤田 彬, 浦川 順平, 井上 大介, “WebUI のコンテンツ情報と画像特徴量を組み合わせた IoT 機器の機種特定手法,” 電子情報通信学会 信学技報, vol.121, no.410, pp.7–12, 2022.

8　村上 洸介, 笠間 貴弘, 井上 大介, “実機を使用した不正ログイン後の IoT 機器悪用可能性の調査,” 電子情報通信学会 信学技報, vol.122, no.86, pp.31–36, 2022.
9　村上 洸介, 笠間 貴弘, 井上 大介, “脆弱な IoT 機器管理用パスワードの設定状況と注意喚起効果の分析,” 電子情報通信学会 信学技報, vol.122, no.244, pp.20–35, 2022.
10　村上 洸介, 笠間 貴弘, 井上 大介, “Web 管理画面への不正ログイン成功時の悪用リスク調査,” 電子情報通信学会 信学技報, vol.122, no.422, pp.91–96, 2023.
11　K. Murakami, T. Kasama, and D. Inoue, “A Large-Scale Investigation into the Possibility of Malware Infection of IoT Devices with Weak Credentials,” IEICE Transactions on Information and Systems, vol.E106.D, no.9, pp.1316–1325, 2023.

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

村上 洸介（むらかみ こうすけ）
株式会社 KDDI 総合研究所
先端技術研究所
セキュリティ部門
サイバーセキュリティグループ
コアリサーチャー
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
2021 年　電子情報通信学会 ICSS 2021 年度研究賞