# JPCERT/CC インターネット定点観測レポート

## 2023 年 7 月 1 日 ～ 2023 年 9 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2023 年 10 月 31 日

JPCERT CC®

# 目次

## 1. 概況

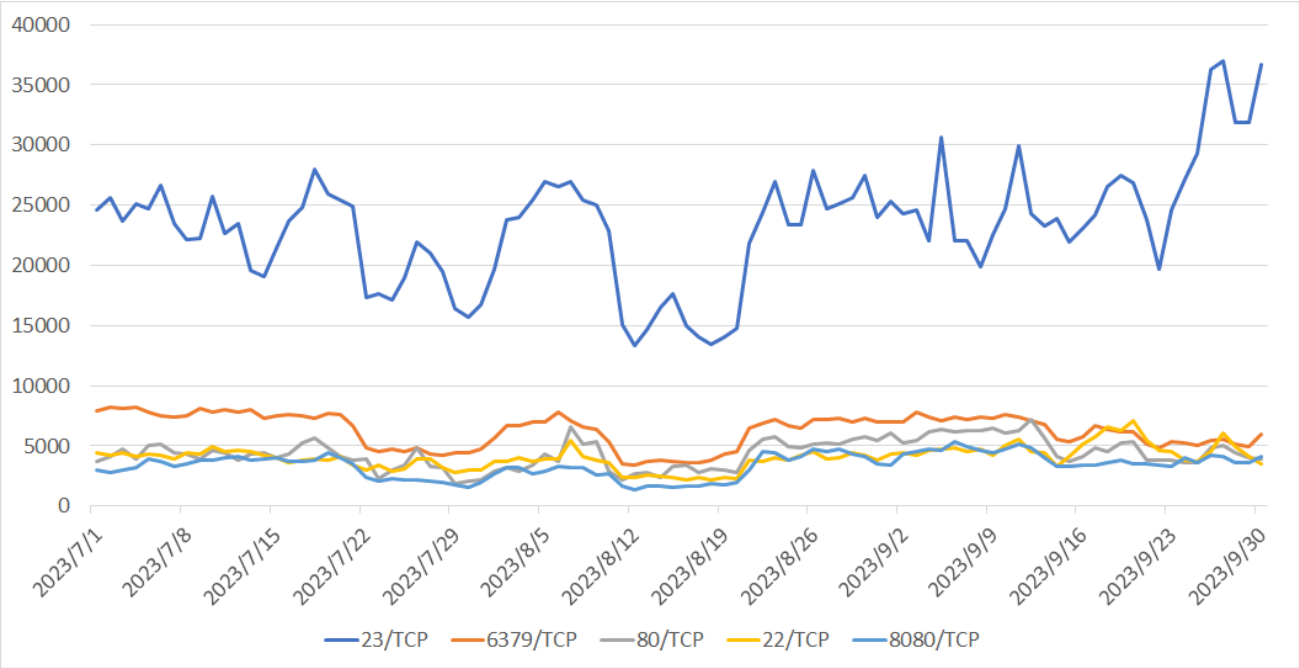
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、一定の IP アドレス帯に向けて網羅的に発信されるパケットを観測しています。こうしたパケットの発信は特定の機器や特定のサービス機能を探索するために行われていると考えられます。JPCERT/CC では、センサーで観測されたパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。センサーから収集したデータを分析し、問題が見つかれば、解決できる可能性がある関係者に情報を提供し、対処を依頼しています。
本レポートでは、本四半期に TSUBAME（インターネット定点観測システム）が観測した結果とその分析の概要を述べます。
本四半期に探索された国内のサービスのトップ 5 は［表 1］に示すとおりでした。

［表 1：頻繁に探索された国内のサービスのトップ 5］

| 順位 | 宛先ポート番号 | 前四半期の順位 |
|---|---|---|
| 1 | telnet（23/TCP） | 1 |
| 2 | redis（6379/TCP） | 2 |
| 3 | http（80/TCP） | 5 |
| 4 | ssh（22/TCP） | 3 |
| 5 | http-alt（8080/TCP） | 10 |

※ポート番号とサービスの対応の詳細は、IANA の文書 (1) を参照してください。
なお、サービス名は IANA の情報をもとに記載していますが、必ずしも
各サービスプロトコルにのっとった形式のパケットが受信されているとは限りません。

［表 1］に示した探索されたサービスのトップ 5 に対するパケット観測数の推移を［図 1］に示します。



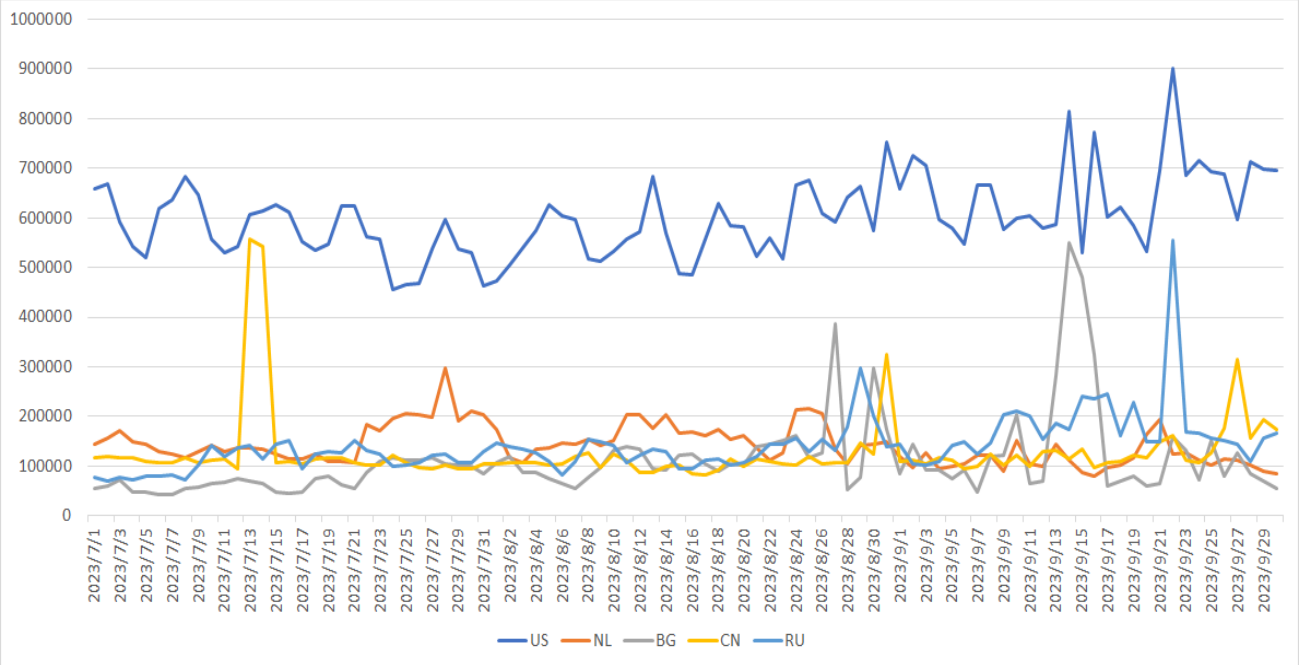

［図 1：2023 年 7～9 月のポート番号宛のパケット観測数トップ 5 の推移］

本四半期に最も頻繁に探索されたサービスは telnet（23/TCP）であり、2 番目は redis（6379/TCP）でした。http（80/TCP）は、期間内で探索される頻度が定常的に高かったために、ssh（22/TCP）と順位が入れ替わりました。次に、本四半期における国内を対象とした探索活動の探索元地域について、活動が活発だった順に並べたトップ 5 を［表 2］に示します。

［表 2：探索元地域トップ 5］

| 順位 | 送信元地域 | 前四半期の順位 |
|---|---|---|
| 1 | 米国 | 1 |
| 2 | オランダ | 3 |
| 3 | ブルガリア | 4 |
| 4 | 中国 | 2 |
| 5 | ロシア | 5 |

［表 2］に掲げた送信元地域からのパケット観測数の推移を［図 2］に示します。

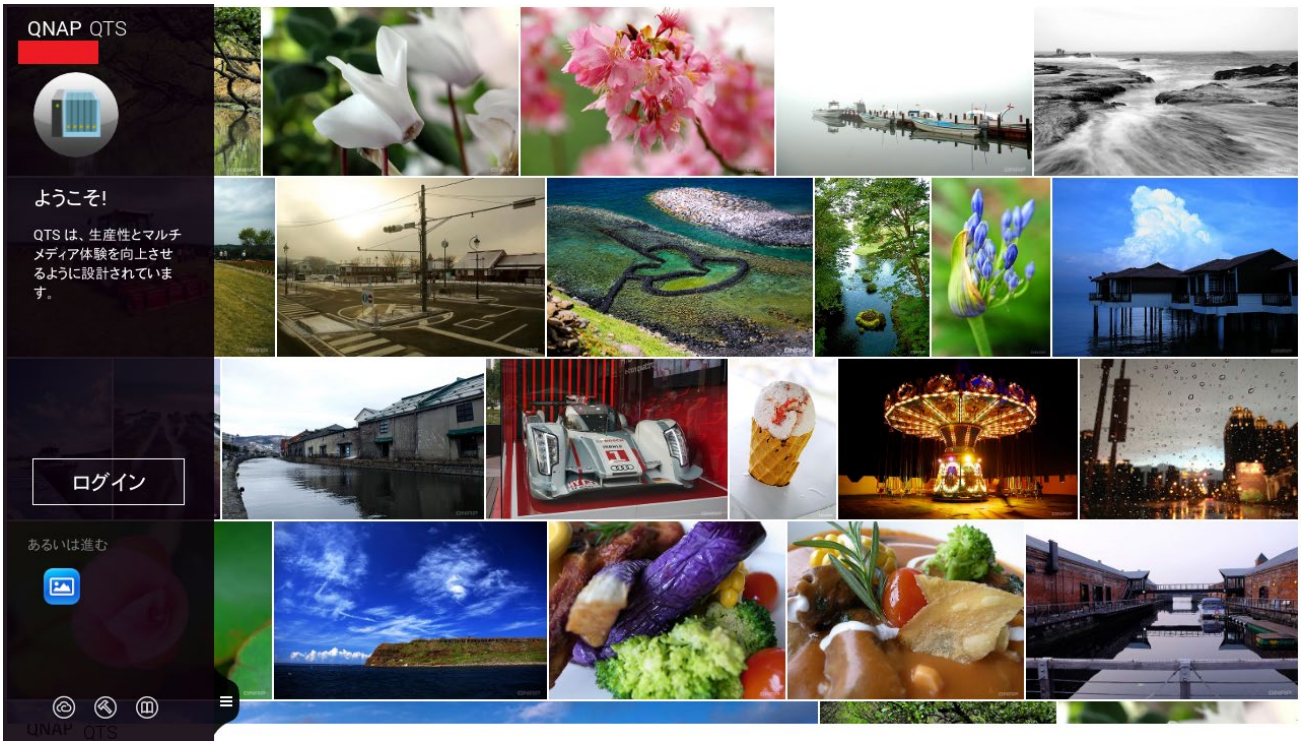



［図 2：2023 年 7～9 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

ブルガリアを送信元とするパケットが、9 月 8 日から 11 日にかけて、および、13 日から 16 日にかけて一時的に増加しました。それ以外の地域は前四半期と同様でした。なお、TSUBAME では RIR（Regional Internet Registry）による割り当て情報を用いて個々の IP アドレスの地域を判断しています。

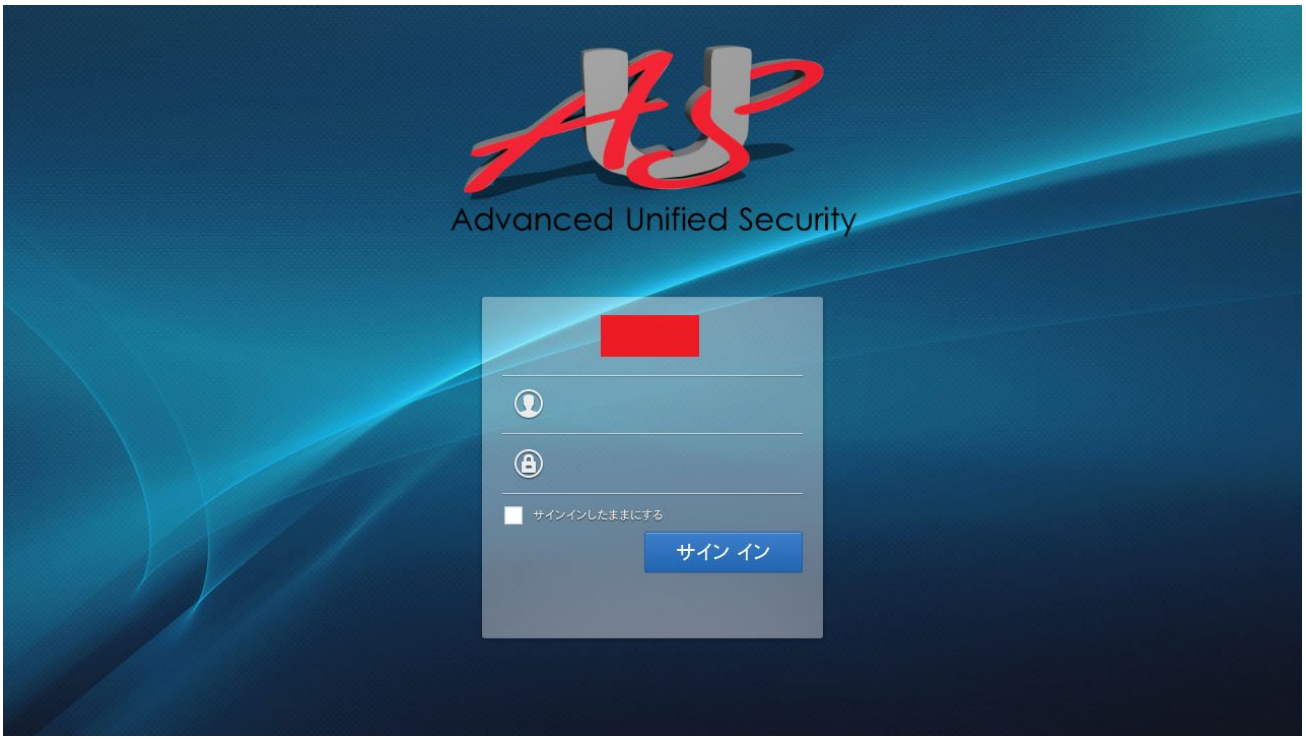
## 2. 台湾製の NAS や無線 LAN ルーター等からの不審なパケットの観測について

NAS や無線 LAN ルーター、DVR などが送信元となっている探索活動の多くが、Mirai の感染活動との関連性が推測される特徴を持っていますが、少数ながら Mirai の特徴を持たない探索活動も観測されています。前者を Mirai 型探索、後者を非 Mirai 型探索と記します。ここでは、非 Mirai 型探索に注目した分析について述べます。探索するサービスが双方の探索で大きく異なっていました。非 Mirai 型探索対象サービスでは、ftp や http、https、mongodb、ms-sql-s、pptp、sip、ssc-agent、imap 等に加えて、Well-known のポート以外も対象となっており、広範囲にわたっています。
探索対象サービスから、非 Mirai 型探索が探し出そうとしている製品を特定することは困難でした。そこで、探索元の機器情報を Shodan.io などの情報から調べてみたところ、台湾のメーカーが提供する NAS や無線 LAN ルーターなどであることがわかりました。さらに、それらの機器は、インターネットに複数のポートが開放されていたり、ファームウェアが古かったりすることが確認できました。インターネット経由で侵害を受け、何らかのマルウェアが機器上で動作していると推測し、継続して調査を行っています。探索元の機器に Web ブラウザーでアクセスすると表示されるページのサンプルを［図 3-1～9］に示します。



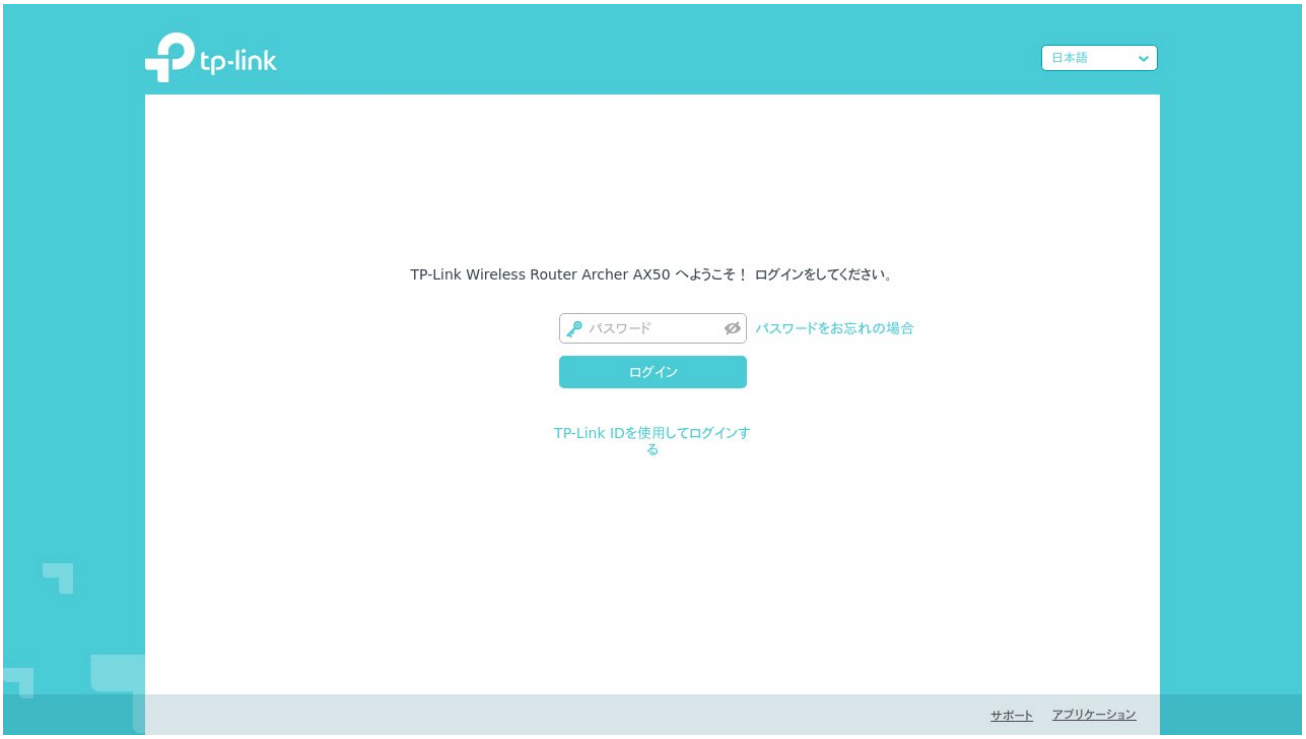

［図 3-1：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例（1）］


［図 3-2：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例 (2)］

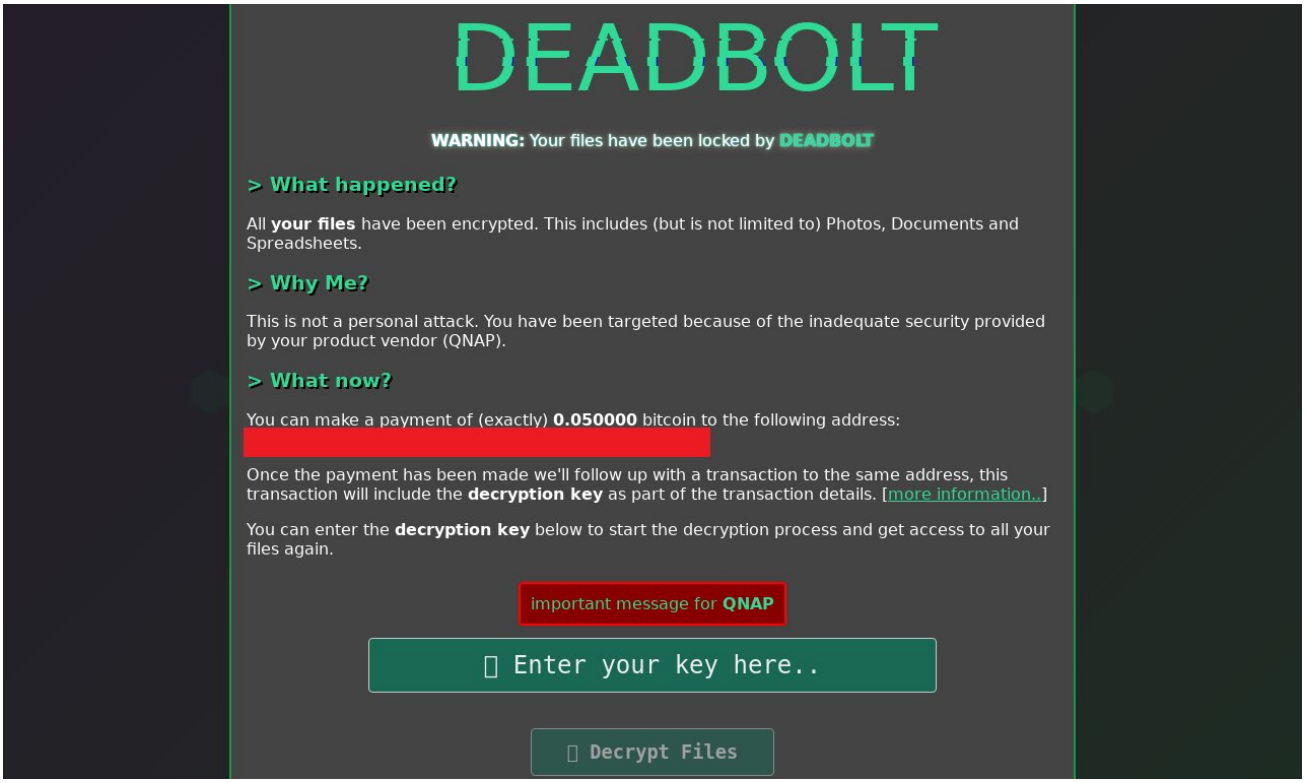



［図 3-3：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例 (3)］

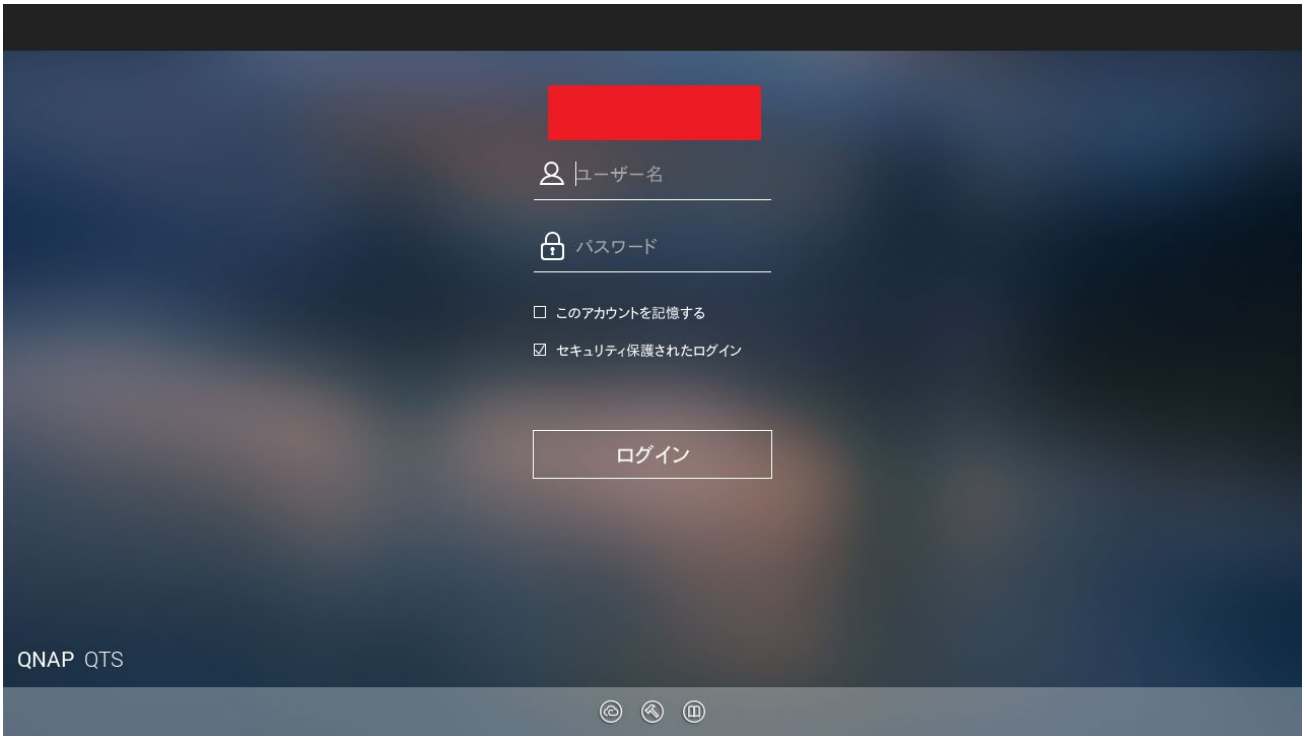

［図 3-4：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例（4）］



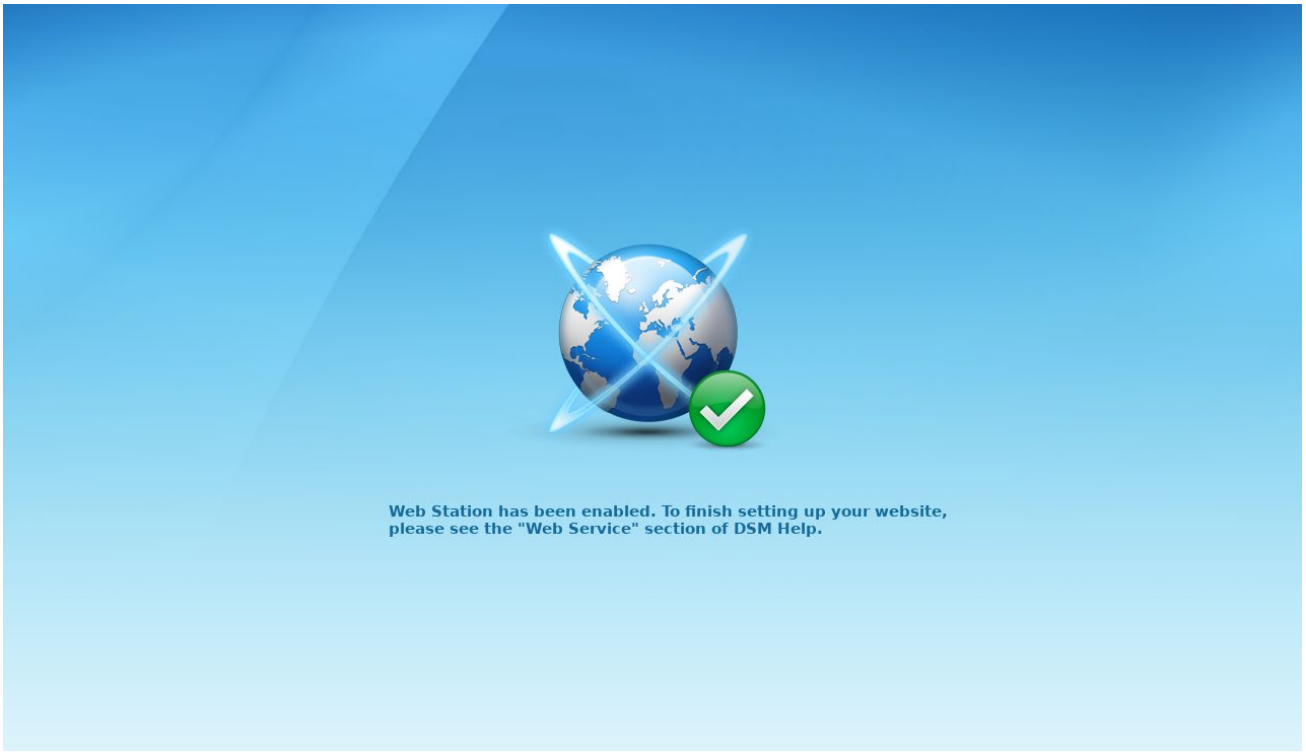

［図 3-5：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例（5）］



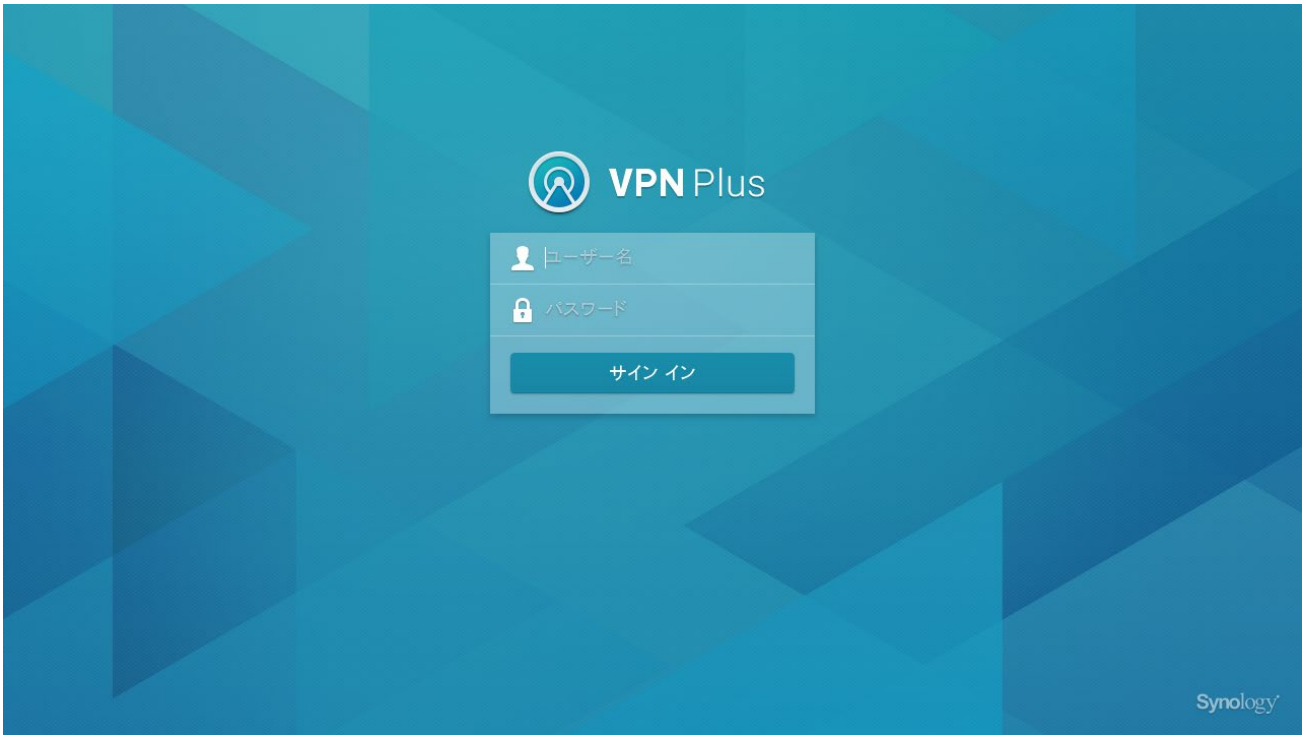

［図 3-6：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例（6）］




［図 3-7：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例（7）］




［図 3-8：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例（8）］




［図 3-9：非 Mirai 型パケットの送信元に Web ブラウザーでアクセスすると表示されるページの例（9）］

## 3. JPCERT/CC からのお願い

JPCERT/CC では、不審なパケットの送信元 IP アドレスについて ISP を通じて当該 IP アドレスのユーザーに確認と対応をお願いすることがあります。このような依頼を受け取った際には、調査活動へのご理解をいただき、可能であれば、使用していた製品やファームウェアのバージョン、侵害の有無などの情報の提供などのご協力をいただければ幸いです。本報告書で紹介したものを含め、不明な探索活動が複数あり、提供いただいた情報が解明の重要な糸口になり得ます。

## 4. 参考文献

（1）Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

本活動は、経済産業省より委託を受け、「令和 5 年度サイバー攻撃等国際連携対応調整事業」として実施したものです。