Miraiボットの観測状況と防犯機器における各種対策等について

警察庁サイバー警察局サイバー企画課　課長補佐　櫻井　仁

■はじめに

防犯カメラ等の防犯機器は、その普及に伴い、犯罪抑止や犯罪行為解明に大きく貢献しています。また、防犯機器をインターネットに接続することにより、遠隔監視することも可能になり、個人向けにスマートフォンのアプリで自宅を遠隔で監視できる製品も販売されています。このような中、防犯機器におけるセキュリティ対策の重要性が増加しています。

本稿では、警察庁におけるマルウェアMiraiの観測状況、各種対策等について説明いたします。

なお、文中の意見に渡る箇所は私見であることをご承知おきください。

■サイバー警察局の発足概要

サイバー空間の社会的な重要性等がますます高まり、セキュリティ確保に当たっての課題が山積する中、様々な主体がそれぞれの役割に応じて多角的に対策を強化していく必要があります。こうした中、警察としては、重大サイバー事案や国際捜査、犯罪インフラ対策、セキュリティ事業者等との官民連携など、治安機関として幅広い施策を展開することが求められています。

そうした中、令和4年4月1日、警察庁にサイバー警察局を設置するとともに、関東管区警察局に重大なサイバー事案について、国の機関として直接捜査等を行うサイバー特別捜査隊を設置しました。

○サイバー警察局

サイバー警察局の役割と目的について説明します。従前、サイバー分野については、警察庁各局がそれぞれの所掌を踏まえつつ連携し、サイバー事案に関する情報収集・分析、対策、人材育成等の事務を行っており、部門間の調整や情報共有が必要な際には、長官官房がその調整役を担っておりました。しかしながら、サイバー分野については各局間にまたがる事案も多く、深刻化するサイバー空間の情勢において的確に対処していくためには、長官官房が間に入る以前の体制では、情報共有の不足や遅れにより、対処に支障を来すケースも発生しかねない状況でした。

そのため、サイバー警察局では、今まで各局が対応していたサイバー関連事務を一元的に所掌し、生安、警備等の他部門と緊密に連携し、サイバー空間・実空間の両者にわたって隙間なく対応することで、迅速な情報集約を図り、各種サイバー事案に的確に対処していくことを目指しています。

○サイバー特別捜査隊

サイバー特別捜査隊は、国家が背景にあるサイバー攻撃や全国的な被害を及ぼすサイバー犯罪等、国家的・全国的規模で対処しなければならない重大サイバー事案に対して、国が直接捜査できるようにすることで、サイバー事案捜査をより強力に推進していくために、関東管区警察局に設置されています。

サイバー事案が発生した場合、その他の犯罪と同様、都道府県警察において、被害者からの通報などにより被害を認知し初動捜査を行います。その結果について都道府県警察から報告を受けたサイバー警察局は、サイバー特別捜査隊が捜査すべきと判断した事案（重大サイバー事案）について、サイバー特別捜査隊に指示を行い、サイバー特別捜査隊が当該指示に基づき捜査を行います。（図 1）

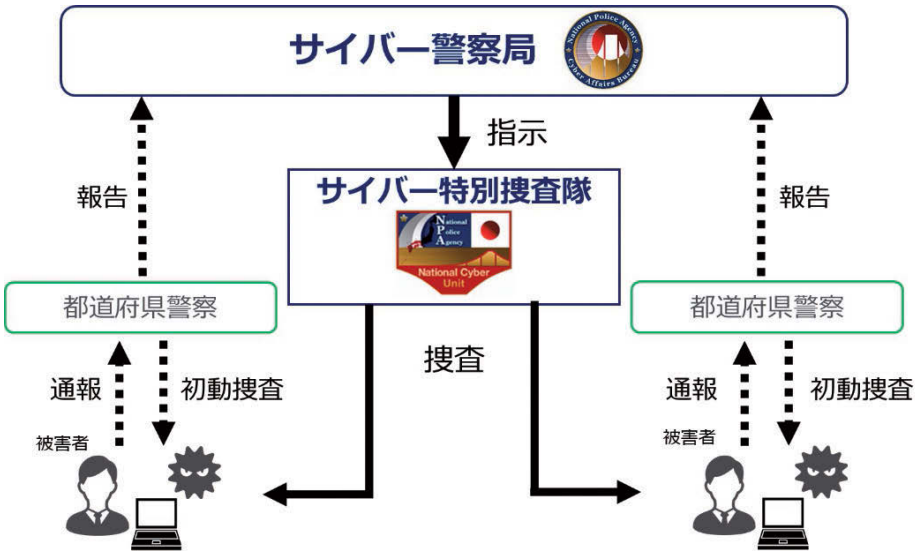

図1　国内で事案が発生したケースにおける捜査の流れ

重大サイバー事案の捜査においては、原則としてサイバー特別捜隊と都道府県警察の合・共同捜査になりますが、都道府県警察の重要性は何ら変わらず、引き続き捜査の主体として治安の維持に当たることになります。

■防犯カメラやレコーダ等IoT機器に感染するマルウェアMiraiとは

Miraiは、ネットワーク機器やインターネットに接続した防犯機器などのIoT機器に感染し、DDoS攻撃※1を行うマルウェアです。また､感染したIoT機器が自動的に感染先を探して自己増殖するように作られています。

○動作概要

① 侵入手口・・・・辞書攻撃。デフォルトID/パスワード。システム毎の固定ID/パスワード等。
② C&Cサーバから指令・・・・攻撃指令。アップデート指令。
③ DDoS攻撃・・・・C&Cサーバから感染機器に攻撃指令をする。
④ 感染拡大・・・・他のIoT機器に感染拡大動作をする。

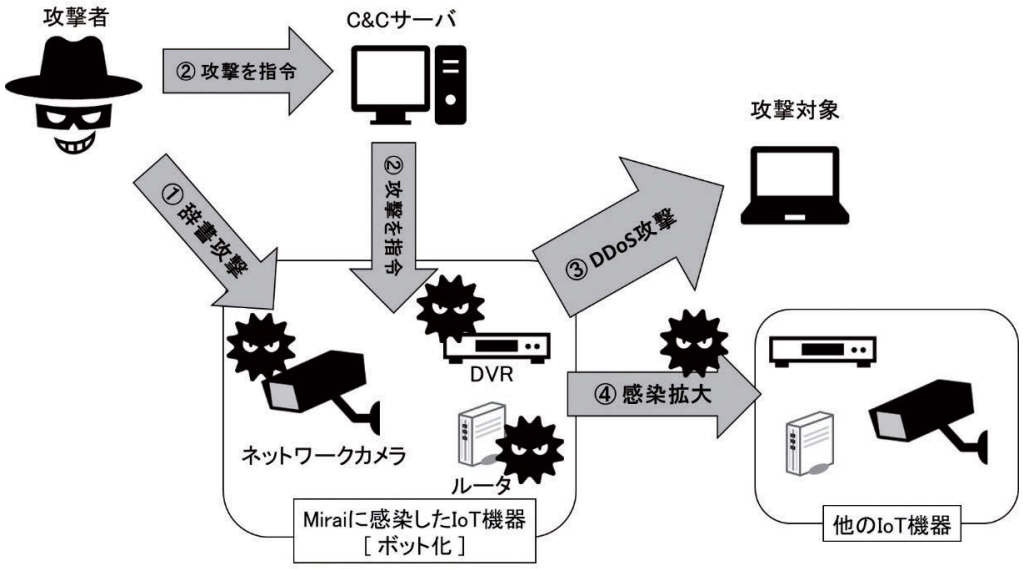

図2　IoT機器に感染するMiraiの動作概要

※1 DDoS攻撃とは、サーバに対して大量のリクエストを送りつけ、サーバを機能停止に陥らせますが、Miraiボットにおいては、一般的なDDoS攻撃とは違い規模が大きいのが特徴です。

Miraiに感染してもIoT機器は本来の動作をしていることから、利用者において直ちに感染に気付かないことが特徴です。また、IoT機器は専用機器であるため、直接IoT機器にウイルス対策ソフトを導入することは困難です。

■警察庁におけるMiraiボット観測状況

警察庁のインターネット定点観測において、Miraiボットの特徴（宛先IPアドレスとTCPシーケンス番号の初期値が一致する）を有するアクセスを行うホスト（Miraiボット）数を観測しており、平成31年1月1日から令和4年8月31日までの間で観測したMiraiボット数の推移は図3のとおりです。平成31年1月のピーク後、しばらくの間落ち着いていましたが、令和4年5月頃から増え始め令和4年8月には、減少に転じています。（図3）

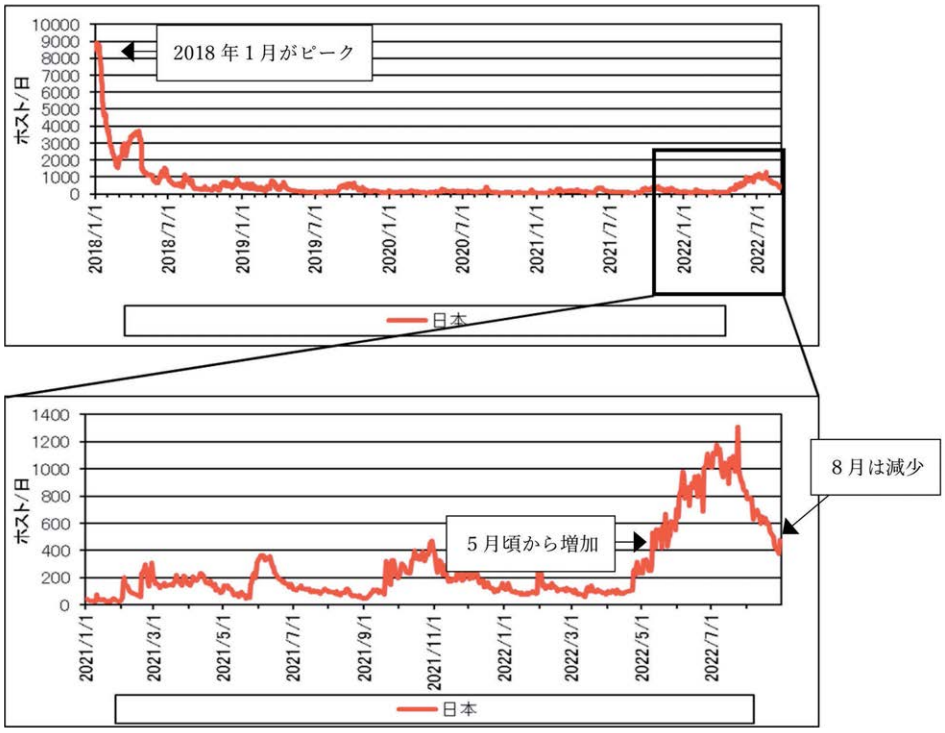

図3　日本国内からのMiraiボット数の推移（H30.1.1～R4.8.31）

令和4年5月１日から令和4年8月31日までの間における日本国内からのMiraiボットからのアクセスについて、詳細に分析したところ、その多くは23/TCPに対するアクセスでした。また、令和4年6月下旬以降では、22/TCPに対するアクセスが観測されるようになり、その後一か月弱の間、当該ポートに対するアクセスが増加しました。（図4）

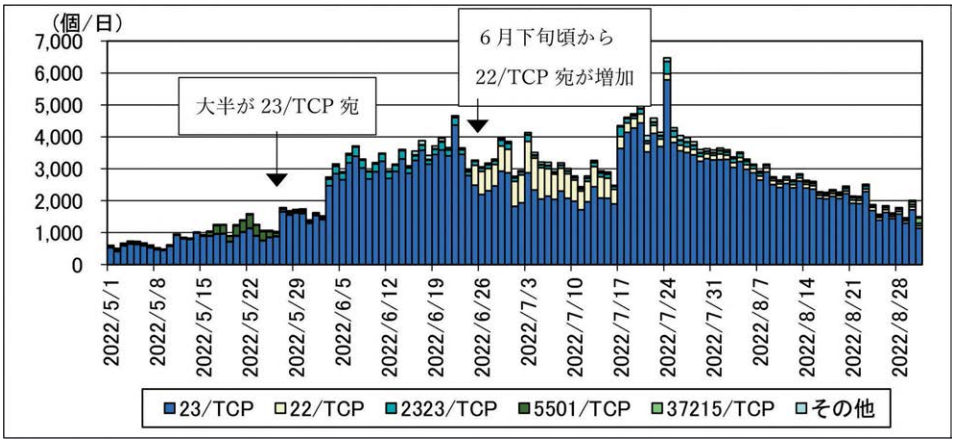

図4　日本国内からのMiraiボットからのアクセス件数の推移（宛先ポート番号別、R4.5.1～R4.8.31）

○23/TCP（telnet）のアクセスについて

日本国内からの23/TCPに対するアクセスを行うMiraiボットを調査したところ、17000/TCPが接続可能であり、DVRの製品名と思われる製品名が記載されていました。また、ブラウザで17000/TCPに接続したところ、認証画面が表示されました。（図5）

○22/TCP（ssh）のアクセスについて

日本国内からの22/TCPに対するアクセスを行うMiraiボットを調査したところ、80/TCPと50100/TCPが接続可能であり、プロダクト名に「Boa」というソフトウェア名とバージョン名が記載されていました。このバージョンではディレクトリトラバーサル の脆弱性（CVE-2017-9833）が報告されています。また、ブラウザで80ポートに接続したところ、認証画面が表示され、海外メーカーと思われるDVRが動作している可能性があることがわかりました。（図6）

国内で動作しているDVR機器等で、Mirai（亜種）が感染拡大していた可能性があります。

図5　23/TCPで観測したIPアドレスに接続した状況

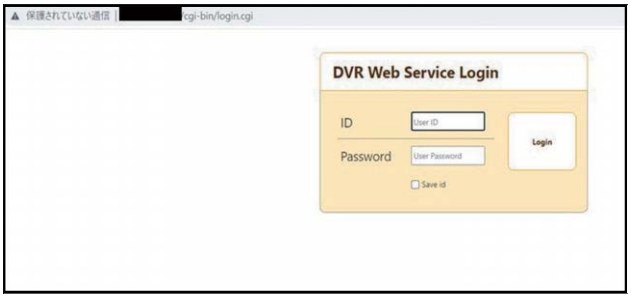

図6　22/TCPで観測したIPアドレスに接続した状況

■防犯機器を取り巻く課題とセキュリティ対策

○OEM製品でファームウェアの更新が困難な事例

OEM製品をとして販売されていた防犯機器において、OEM製造元が倒産したことにより、ファームウェアが更新できないケースが発生しています。（図7）この場合は、新たな脆弱性が発見されても対策が講じられたファームウェアが提供されることはありません。もし使用し続けた場合は、不具合の発生や攻撃される対象となる可能性があることから、早急にサポートされている製品に変更する必要があります。

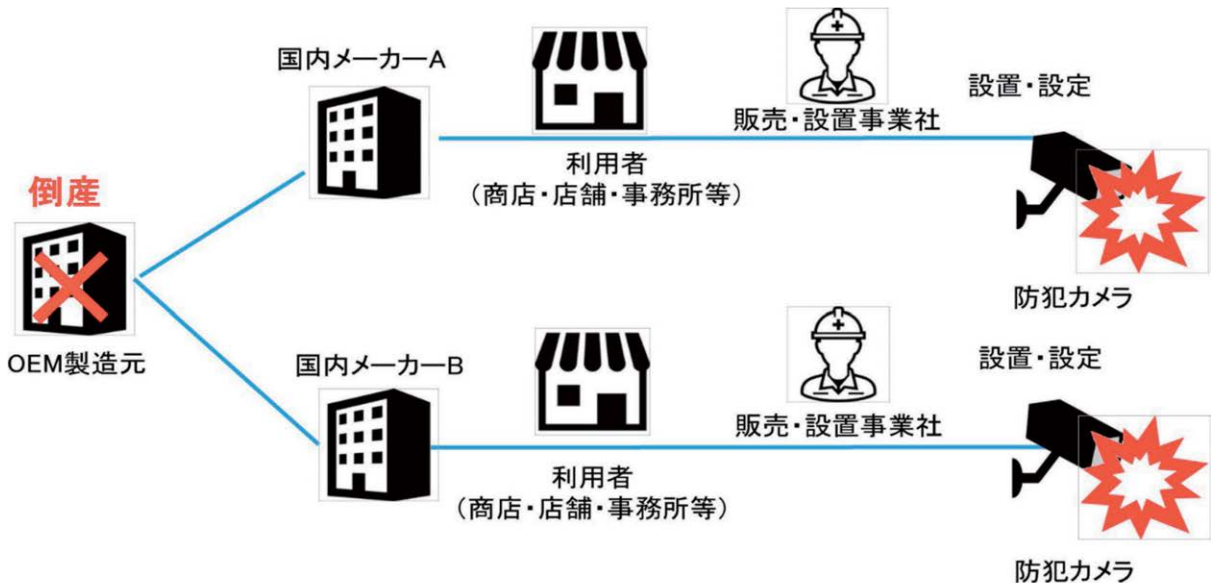

図7　ファームウェアの更新が困難な事例

○外部ネットワークから容易に接続されない工夫

IoT機器をインターネットに接続する場合には、直接インターネットに接続せず、ルータやFWを使用し外部から容易に接続出来ないようにしてください。また、ルータ等で防犯機器にポート転送設定をする場合は、インターネットに直接接続しているのと同様であるため、接続元IPアドレスの制限を行うかVPN等を活用し、外部から接続できない状態にするなど、より安全に防犯機器の運用を行う必要があります。(図8)

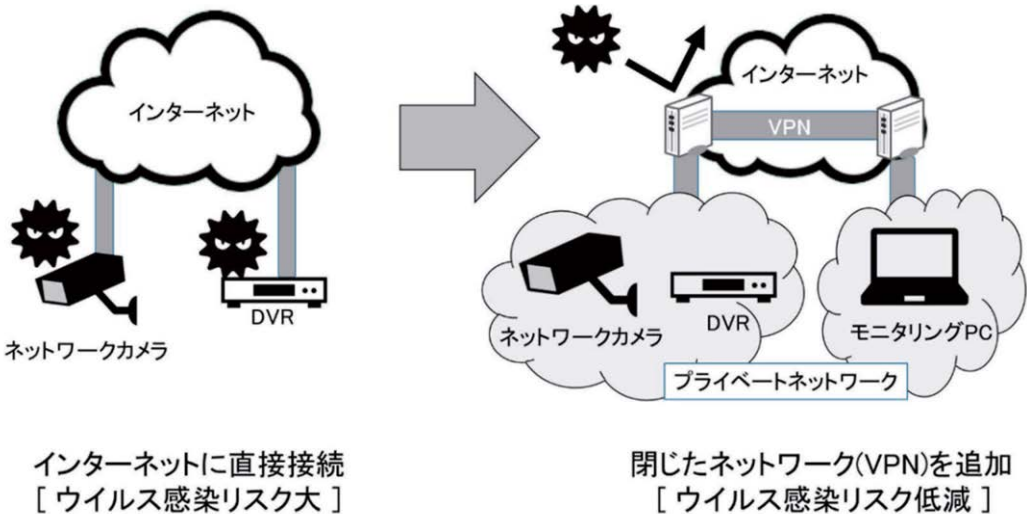

図8　防犯機器をVPN内に収容する接続例

○安全なVPNネットワーク構成例

インターネットを利用したネットワーク構成を検討する際は、IPoE（IP over Ethernet）接続によるIPv6高速インターネットサービスでVPN接続の環境を構築することも有効と考えています。NGN網内のIPv6で拠点間接続（VPN）を行い、ファームウェア等の更新に必要な接続は、IPv4でインターネットからダウンロードを行うVPNネットワーク構成例です。また、IPv4においては、プロバイダー側でNAT変換をしているため、インターネットからの接続はできないネットワーク構成になっており、両方の利点を生かしたハイブリット環境を構築することができます。

筆者が構築したネットワーク構成事例は、拠点間 VPN（IPSec）のみ IPv6 で接続し、拠点間の内部ネットワーク及びインターネットへの接続は IPv4 で接続するネットワーク構成です。(図 9)

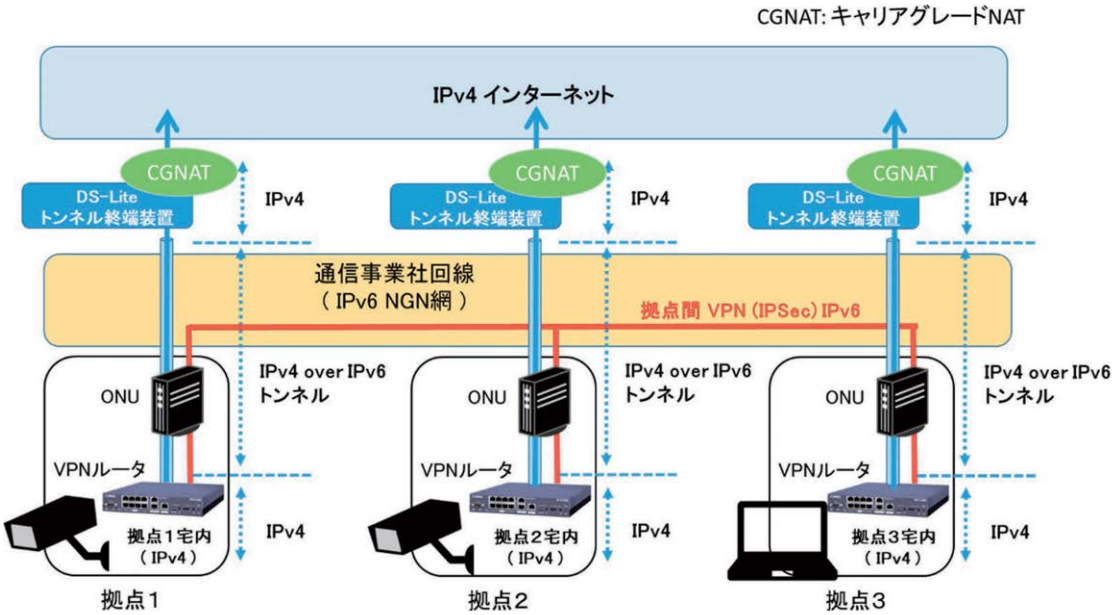

図9　VPN間をIPv6で接続しIPv4でインターネット接続するハイブリットネットワーク構成

○IoT機器におけるセキュリティ対策

・マルウェアに感染したIoT機器においては、初期パスワードで管理されているなど、パスワード管理の問題が考えられます。パスワードの変更や推測しにくいパスワードに設定するなどの対策が必要です。「admin」や「password」など、製造元が設定したIDやパスワードは、「辞書攻撃」に破られるおそれがあることから、必ず変更をしてください。

・脆弱性対策（ファームウェアアップデート）

製造元のウェブサイト等で周知される脆弱性情報を確認し、脆弱性が存在する場合にはファームウェアのアップデート等の適切な対策を実施してください。また、製造終了から年月が経過した製品は、製造元のサポートが終了し、脆弱性への対策が実施されない場合があります。そのような製品を使っている場合には、サポート中の製品への変更を検討してください。

■おわりに

警察庁の観測から分かるように、ピーク時から約４年が経過した現在でもMiraiボットは活動を続けています。紹介したセキュリティ対策を実施するだけでも、Miraiボットネットに感染するリスクは軽減します。また、感染しにくいネットワーク環境を構築することで、「当社のシステムが御社のネットワークからDDoS攻撃されている」と外部から抗議されることを避けることができます。Miraiボットに限らず、脆弱性を放置するとウイルス感染により、遠隔操作による情報漏洩のおそれがあるほか、情報セキュリティに関する事故や法令違反を起こせば、企業にとって重大な経営的影響を受ける可能性があります。

IoT機器だけでなく、デジタル端末はリリースから時間が経過すればするほど、脆弱性が発覚する可能性が高まります。こうした現実を受け止め、適切な対策をとるべきと考えます。

防犯設備士のみなさま方は、防犯設備の専門家として、安心・安全な防犯設備の設置及び運用に携わっていることと思います。従来、防犯設備の設計・施工、維持管理に関する知識が中心でしたが、今日では防犯設備機器のみならず、ネットワーク技術やサイバーセキュリティなど幅広い知見が求められています。本稿が、IoT機器におけるサイバーセキュリティ対策に関する理解の深化と、それぞれの職場等におけるサイバーセキュリティ対策を見直すきっかけの一助となれば幸いです。