特別インタビュー 2
special interview

横浜国立大学大学院
環境情報研究院/先端科学高等研究院
准教授
吉岡 克成 氏

マルウェアに感染するIoTデバイスが激増 ネットワーク攻撃に悪用

IoT(Internet of Things)の時代が到来し、すでに多くのデバイスがインターネットとつながり、さまざまな機能やサービスが提供され始めています。今、IoTデバイスはどのような脅威にさらされているのでしょうか――。マルウェアやネットワーク攻撃への対策を研究領域とする横浜国立大学大学院環境情報研究院/先端科学高等研究院の吉岡克成准教授は、脆弱な機器を模した囮システム“ハニーポット”を用いて、サイバー攻撃の実データを観測・分析しています。吉岡氏に、IoTデバイスが直面しているリスクの現状、これから起こりうる事態、さらに今後のIoTの発展のためにとるべき対策について伺いました。

すでに多くのIoTデバイスがマルウェアに感染

IoTの時代が到来し、大量のデバイスやセンサー、家電製品、自動車、産業機器・ロボット、インフラ設備など、多様なモノがインターネットに接続されつつあります。それに伴って、IoTデバイスを狙うサイバー攻撃も飛躍的に増加しています。

マルウェア解析やネットワーク攻撃分析を専門としている横浜国立大学大学院 環境情報研究院の吉岡克成准教授の研究グループは、どのような脅威が存在するかを把握することが情報セキュリティー対策の第一歩と考え、IoTデバイスがさらされているリスクの現実を把握するために、“ハニーポット”による観察・分析を続けています。ハニーポットとは、攻撃者が侵入しやすいように脆弱な

P R O F I L E

吉岡 克成 [よしおか かつなり]

2000年より情報セキュリティー研究に従事し、2005年より独立行政法人情報通信研究機構（現、国立研究開発法人情報通信研究機構）にて研究員としてネットワーク・セキュリティー・インシデント対策に関わる研究開発に従事。2007年12月より横浜国立大学特任教員（助教）。2011年2月より同学大学院環境情報研究院准教授。現在の研究テーマは、コンピューター・ウイルスなどのマルウェア活動観測・分析・対策をはじめとするネットワーク・セキュリティー技術全般。

設定を施した、いわば囮のサーバーやネットワーク機器で、ハニーポットにおびき寄せられてくる侵入やマルウェアの振る舞いを記録し調査することで、ネットワーク攻撃を仕掛けてきたデバイスやシステム、手段を把握することができます。

「IoTの進展で、すでに多くのデバイスや製品がインターネットに接続されています。それらに、実際にどういったセキュリティーの脅威が顕在化しているのか、ハニーポットとよばれる観測用ネットワークを国内に設置して観測を続けています。2015年4月から7月の4カ月間の観測では、約100個のIPアドレスを持つハニーポットにインターネット経由で攻撃を仕掛けてきたマルウェア感染機器やシステムは、IPアドレスで区別したもので約15万台で、その攻撃試行回数は実に90万回に上りました。私の研究結果は、まさに氷山の一角でしかなく、世界レベルで考えると膨大なIoTデバイスがすでにマルウェアに感染し、ユーザーの知らないうちに攻撃に悪用されていると予想されます」

ハニーポットを通じて吉岡氏が観測した「IoTデバイスからのサイバー攻撃」の実態は、まさに驚異だと言えるでしょう。さらに、これらの攻撃元の機器を判定するためにデバイス側へアクセスを仕掛けてみると、型番を確認できたものだけで361種類のデバイスが観測されました。これらは、デジタル・ビデオ・レコーダー、ルーター、ネットワーク・カメラ、Webカメラ、セットトップ・ボックスといった家庭用機器をはじめ、駐車場管理システム、LEDディスプレイ制御システム、ビル制御システム、火災報知システムといったインフラにまで至ります（図1）。

「驚くべきことに、ファイアウォールやゲートウェイといった、本来セキュリティーを守るべきネットワーク機器まで乗っ取られているケースがあります。社会のいたるところで見かける身近な機器がネットワーク攻撃に加担しているのです」と吉岡氏は説明します。

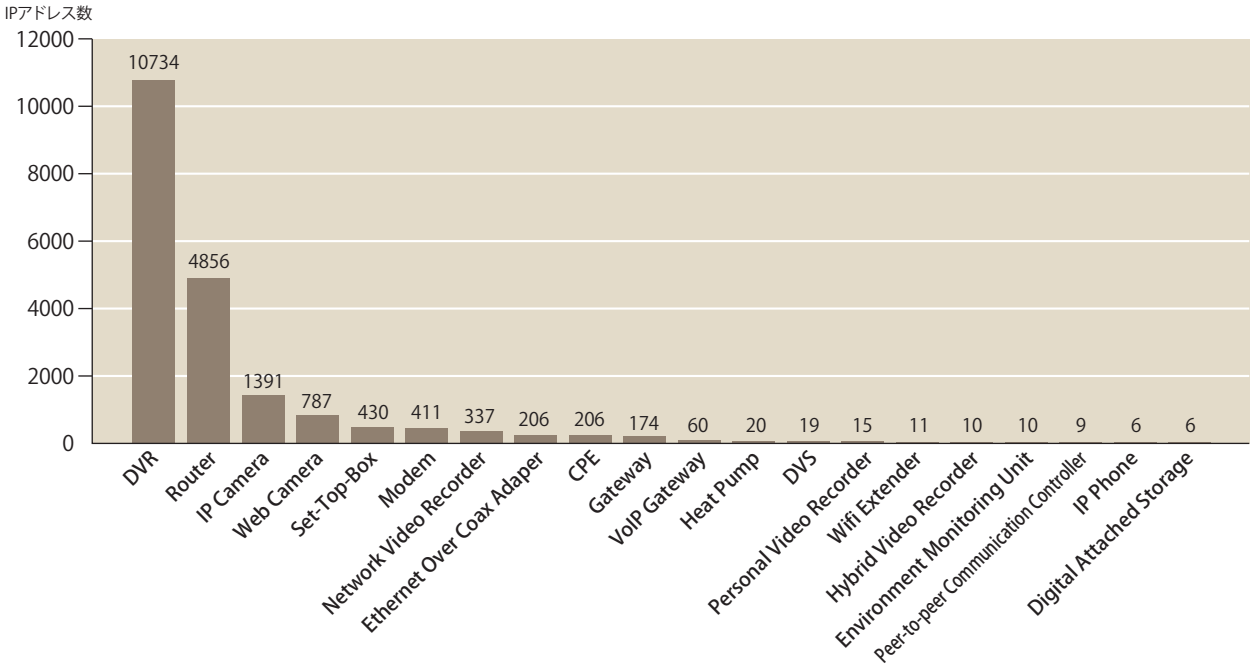


図1. ハニーポットで観測された感染機器の種類

IoTデバイスの大量感染 その元凶はTelnet

これほどまでに大量かつ多様な機器が、なぜ乗っ取られてしまうのでしょうか。IoTデバイスの大量感染の元凶はTelnetだと吉岡氏は指摘します。Telnetとは、TCP/IPネットワークを通じて他のコンピューターにアクセスするためのプロトコルの一つで、今から30年近く前のUNIXの黎明期にはリモート・ログインの代表的な手段として広く使われてきました。

「Telnetは暗号化などの仕組みを持っておらず、認証を含めた通信内容が通信路上で容易に観測されるためセキュリティー上問題とされています。現在ではTelnetでのリモート・ログインを受け付けているサーバーは少ないと言われ、推奨もされていません。実際、Telnetの脆弱性を突いたサイバー攻撃は、近年あまり耳にすることがありませんでした。ところが、一部の組み込み機器では、いまだにTelnetが機器の操作や設定変更などをリモートで行う手段の一つとして残っており、IoTの拡大とともに再びネットワーク攻撃の格好のターゲットとなっているのです。

さらに機器製造業者によっては、セキュリティーを十分に意識することなく、デフォルトのIDとパスワードを変更せずに利用していることが多いのです。攻撃者にとっては、機器のメーカーや機種を特定できれば、デフォルトのIDやパスワードはインターネットで簡単に検索できてしまうため、コストや手間をかけることなく、機器を乗っ取ることができます（図2）」（吉岡氏）

Telnetへの攻撃が増えていることは、データからも明らかになっています。国立研究開発法人情報通信研究機構のインシデント分析センター（NICTER）における観測結果（図3）に示す通り、2014年からTelnetサービスへの攻撃が急増しています。以前はWindowsの脆弱性を突く攻撃が目立っていましたが、PCよりも狙いやすいため、Linux系の組み込み機器のTelnetへの攻撃が急増していると吉岡氏は指摘します。NICTERでは、TCP宛先ポート別パケット数を毎日公開しており、2015年12月の数値ではポート23（Telnet）への攻撃は、全体の48%にも上っています。

攻撃が“量から質”へシフトすると 事態はますます深刻化する

では、乗っ取られたIoTデバイスは、どんなことに悪用されているのでしょうか。吉岡氏によると、

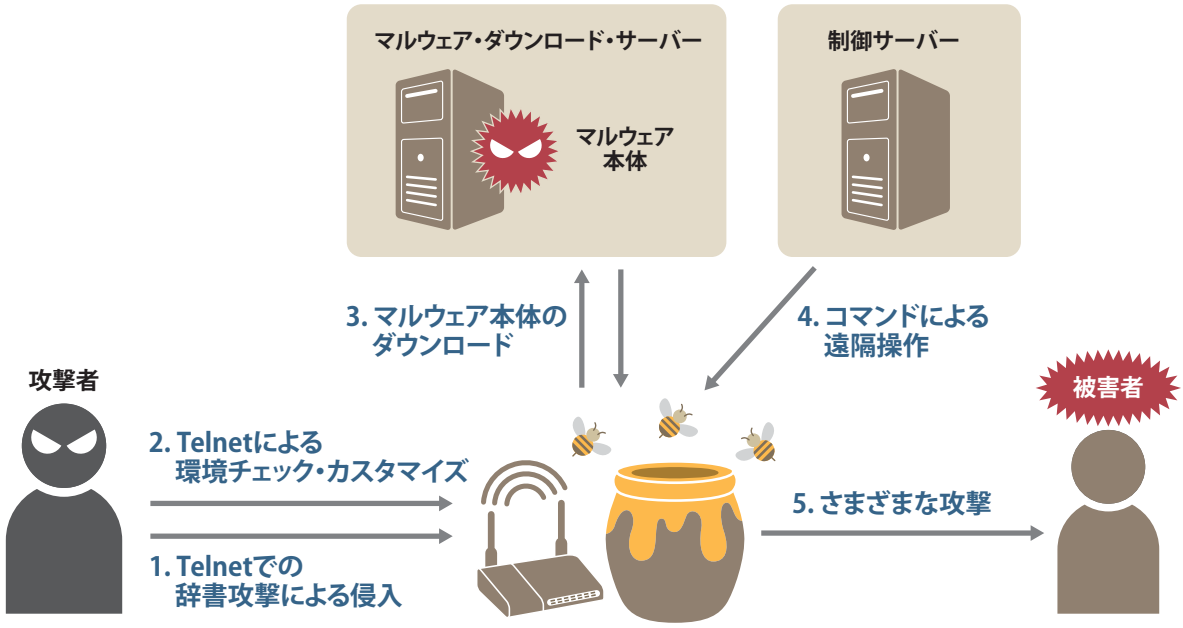


図2. Telnetベースのマルウェア感染の流れ

最も多いのはインターネット上の特定サイトやサーバーに一斉攻撃を仕掛けてサービスを妨害するDDoS攻撃です。また、アフィリエイト広告を多数のユーザーがクリックしたように見せかけて金銭をだまし取る詐欺行為に使われているケースや、他のデバイスにマルウェアを拡散させる目的にも悪用されています（図4）。

「IoTデバイスはPCよりも処理能力が低く、攻撃の威力も小さいと思うかもしれません。しかし、ポイントはその“数”です。数が大量になり、それが一斉に攻撃を仕掛けてくると大きな脅威になります。また、製造業者や利用者が乗っ取られていることに気が付きにくいというのもIoTデバイスの課題となっています。

いまはまだ、IoTデバイスに対するサイバー攻撃も“質より量”といった段階ですが、これが“質”を重視した攻撃になる可能性が十分に考えられます。機器ごとの特性・機能を狙い撃ちする攻撃に発展する兆候も見えています」

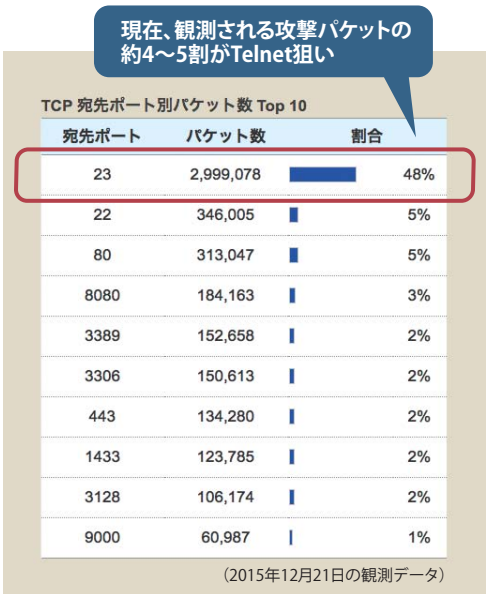
例えば、オンデマンドの視聴が可能な有料TV放送のセットトップ・ボックスに侵入し、決済可能な認証情報を盗み出そうとする振る舞いも観測されています。

「特定デバイスの機能や特徴に特化した攻撃にシフトしてくると、事態は深刻です。防犯用に設置したインターネット・モニターが乗っ取られた場合、家庭内の映像が外部に流出してしまう恐れがあります。Wi-Fiルーターが乗っ取られた場合には、フィッシング・サイトへの誘導も簡単に行われてしまいます。さらに、大勢の買い物客が集まる商業施設や駅、空港などのビル管理システムが乗っ取られた場合、テロのリスクも大きくなります」と、吉岡氏はその深刻さを強調します。

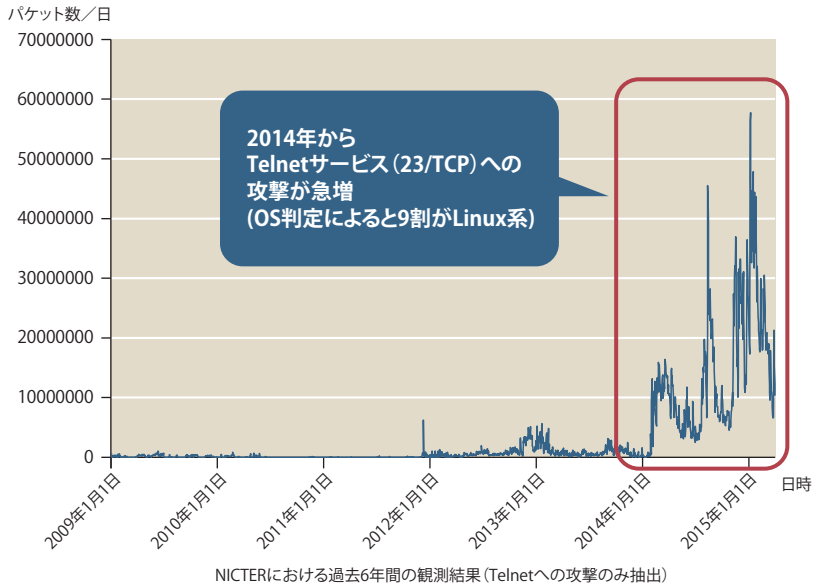
IoTデバイスのセキュリティー・レベルの底上げが事態を好転させる

こうした脅威からIoTデバイスのセキュリティーを守っていくためは、どんな対策をとるべきなのでしょうか。

吉岡氏がその一例として紹介するのは、内閣府が主導する戦略的イノベーション創造プログラム（以下、SIP）における「重要インフラ等におけるサイバーセキュリティの確保研究開発計画」の取り組みです。同計画では、重要インフラの安定運用を担っている制御機器や通信機器に対するサイバー攻撃の対策として、ネットワークの動作監視および解析技術、防御技術の研究開発を推進しています。2020年東京オリンピック／パラリンピックに向けて、その成果を通信・放送、エネルギー、交通などのインフラ・シス



TCP 宛先ポート別パケット数



NICTERにおける過去6年間の観測結果（Telnetへの攻撃のみ抽出）

図3. 情報通信研究機構インシデント分析センター（NICTER）における観測結果

テムに適用していくことを目指しています。

こうした国レベルの取り組みが行われているとはいえ、OSベンダーが主導することで一定のガバナンスが保たれてきたPCの世界と異なり、一筋縄ではいかないのがIoTデバイスの難しいところです。それは、あまりにも多種多様のIoTデバイスが混在しているからです。しかし、「IoTデバイスが最低限として守るべきセキュリティーのガイドラインを、それぞれの応用分野に応じて適切に設定し周知するだけでも、事態は大きく好転するはずです」と吉岡氏は言います。

「現状はセキュリティーに対して無防備なIoTデバイスが世界中に散在している状態です。Telnetという攻撃の手口を知っているサイバー攻撃者に対し、前述したように攻撃されていることにも気付いていない製造者や利用者は、まだ勝負の土俵にさえ立てていないということです。そこで、IoTデバイスのセキュリティーを一定レベルにまで引き上げることが重要だと思います。それを達成できれば攻撃数は減少し、今度はIoTデバイスの多様性が有利に働くようになります。一定のセキュリティーが確保された個々の機器を攻撃するには、これまでのTelnetのようにはいかず、攻撃側にもそれなりのコストや手間がかかるからです。しかしこれは同時に、攻撃者が攻撃する価値があるかどうかを見極めるようになるということでもあり、守る側のセキュリティー対策もそこからが本当の勝負になるのだと思います」

今後IoTデバイスを開発する企業に対して、例えば、開発ガイドラインを作ったり、Telnetのような脆弱なプロトコルをインターネット経由で利用できる状態で放置してはならないといった原則を徹底すること、各社が製造したIoTデバイスにセキュリティー上の問題がないかどうか、業界団体や第三者機関がチェックする体制も有効だと、吉岡氏は指摘します。

それでも、問題は残ります。吉岡氏が行ったハニーポットを使った観測では、実は日本製のIoTデバイスからのサイバー攻撃はあまり検出されておらず、検出されたサイバー攻撃の大半を占めているのは、海外の途上国で作られた製品だと言います。

「売り切り型の価格勝負を臨んでいる海外メーカーのセキュリティー意識を短期間のうちに変えるのは難しく、市場にはリスクを抱えた製品もどんどん流れてきます。加えてIoTデバイスのライフサイクルはPCと比べて圧倒的に長く、すぐには新しい製品には置き換わりません。また、利用用途も多様で裾野も広いため、セキュリティーに問題のある機器をインターネット上からなくすことは容易ではありません」(吉岡氏)

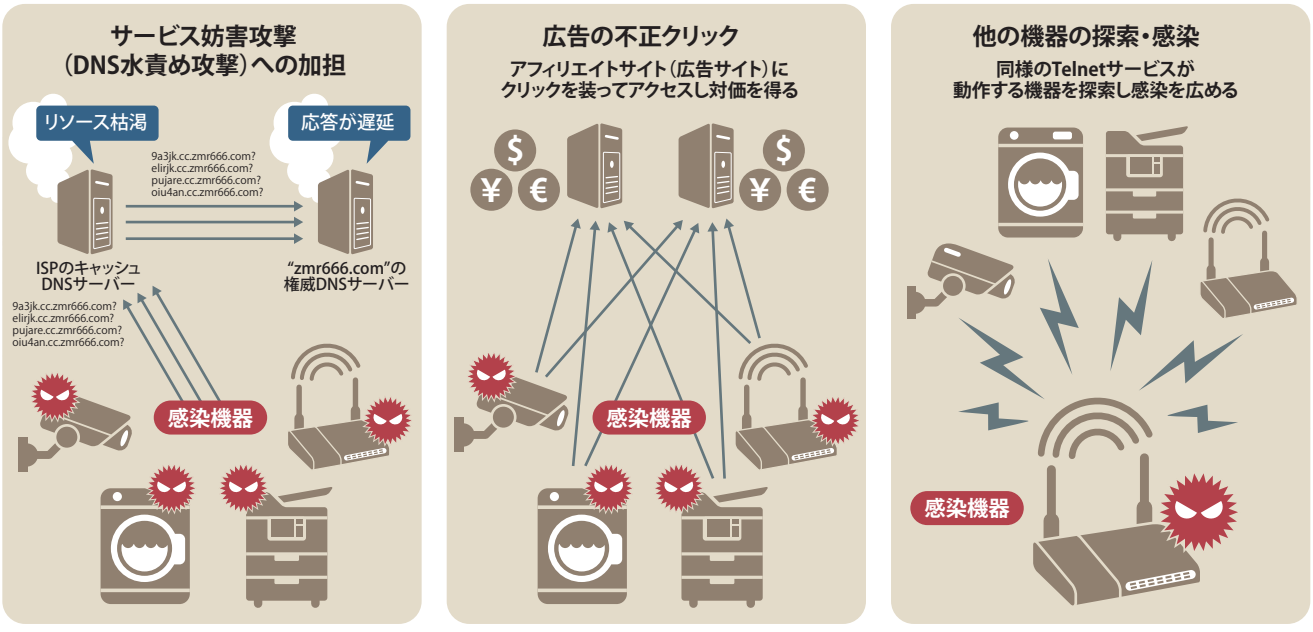


図4. マルウェア感染による悪用例

加えて個々のIoTデバイスは、セキュリティーを強化したくても、仕様変更や更新・メンテナンス機能の実装が容易ではないという側面があると吉岡氏は指摘します。

IoTデバイス単体だけではなく全体として安全性を担保する仕組みが必要

IoTデバイスのレベルでセキュリティー強化を図っていくことは重要です。それと同時に、機器レベルよりも高いレイヤーからも包括的な対策を行っていく必要があると吉岡氏は提言します。

「仮にデバイス単体としてのセキュリティーが不完全だったとしても、それを取り囲むシステム全体で補完し合って安全性を担保できるようなソリューションが、本格的なIoT時代に向けて求められています」

わたしたちが暮らしているリアルな社会を見わたしても、どこかに犯罪者やテロリストは存在します。彼ら全員を改心させられるなら理想的ですが、それはおそらく不可能でしょう。それでも世界が壊滅的な事態に陥ることなく全体としての秩序が守られているのは、入国審査や警察、公安、地域住民の目といった社会のさまざまな仕組みが機能しているからに他なりません。同じようなスキームをサイバーの世界でも構築していく時期に来ていると言えるでしょう。

そこで何よりも重要となるのが、IoTネットワークの中で起こっているさまざまなインシデントを継続的に監視し把握することです。吉岡氏は、特定のIoTデバイスをより正確にエミュレートしたハニーポットを設けて、サイバー攻撃の狙いや手の内を掴むことも必要だと説明します。また、IoTデバイスを狙ったサイバー攻撃がさらに高度化していくことも想定し、TelnetだけではなくFTPやSSHなどのプロトコルについても安全性に問題がないかを引き続き調査し、万が一脅威が発生した場合にどうやって警告するのか、あるいは無効化するのかといった議論をあらかじめ行っておくことが重要だと言います。

「世界各国の政府や研究機関、大学、ITベンダー、IoTデバイスメーカーなどがそれぞれの視点や専門知識に基づいた監視や調査を行い、お互いに情報を共有することで、多くの知見が生み出されてくるはずです。そうした情報や知見をもとに、今後起こりうることを予測しながら先手を打っていく、そうしたプロアクティブなセキュリティー対策の確立のために、ネットワーク攻撃の観測・分析・対策という私の研究が貢献できればと考えています」