第3章 最新の脅威＆対策事例から設計の基礎知識まで

IoT開発における セキュリティ機能の重要性

辻 宏郷

表1　IoT機器に感染するウイルスの分類

IPAによる分類	特　徴	代表的なウイルス例
機器乗っ取り型ウイルス	感染したIoT機器上で不正なプログラムを実行し，ボットネットを構成するとともに，サイバー攻撃への悪用を試みる．主な悪用方法は，DDoS攻撃の踏み台としての利用であるが，この他に不特定多数を対象とした不正なアプリケーション（ウイルス）感染，プロキシ・サーバとしての悪用，暗号資産（仮想通貨）のマイニングへの悪用などと，方法が多様化しており，IoT機器の利用者自身に被害が及ぶ恐れもある．また，同じウイルスに感染可能なIoT機器を探索し，ボットネットの拡大を図る	• Miraiとその亜種 • Gafgytとその亜種 • VPNFilter
機器保護型ウイルス	感染したIoT機器上で不正なプログラムを実行し，ボットネットを構成するとともに，IoT機器を狙った他のウイルスが感染に悪用する通信ポートの遮断などを実行して，結果的に機器を他のウイルス感染から防御する．サイバー攻撃への悪用は行わない．また，同じウイルスに感染可能なIoT機器を探索し，ボットネットの拡大を図る	• Hajime
機器破壊型ウイルス	感染したIoT機器上で不正なプログラムを実行し，機器の機能を破壊することで使用不能とする	• BrickerBot • Silex

1．IoTのセキュリティ動向

IoT（Internet of Things）技術の普及に伴って，セキュリティ設定が不十分なまま，あるいは脆弱性を有したままインターネットに接続されたコンピュータ以外の機器（IoT機器）が増大し，サイバー攻撃の対象となっています．2016年，ウイルス「Mirai」に感染して乗っ取られたIoT機器によって構成されたボットネットがDDoS（Distributed Denial of Service）攻撃に悪用された結果，世界中で利用されているSNSや音楽配信サービスに影響を与えたことは大きな衝撃となりました．2022年2月24日に開始されたロシアのウクライナ侵攻の前後においても，ウクライナおよびロシア双方のウェブ・サイトへのDDoS攻撃にIoT機器によるボットネットが悪用されていることが確認されています．

● IoT機器に感染するウイルスとは？

IPA（独立行政法人情報処理推進機構）では，毎年発行している『情報セキュリティ白書』[注1]において，IoTに対する脅威の動向やウイルス感染の実態などの調査分析結果を報告しており，IoT機器に感染するウイルスを機器乗っ取り型ウイルス，機器保護型ウイルス，機器破壊型ウイルスに分類しています（**表1**）．現在，脅威の中心となっているのは，機器乗っ取り型ウイルスです．

2016年に初めて出現したMiraiは，Telnetプロトコルが動作しており，典型的なユーザ名とパスワードで，または製品出荷時の初期ユーザ名と初期パスワードのままでリモート・ログイン可能なIoT機器を感染対象としていました．IoT機器を狙うウイルスは進化を続けており，現在は，PCを狙ったウイルスと同様に，IoT機器のハードウェアやソフトウェア（ファームウェア）に含まれる脆弱性（セキュリティ上の欠陥）を攻撃して感染を試みます．

● ウイルス感染したIoT機器はどうなる？

機器乗っ取り型ウイルスに感染したIoT機器は，サイバー攻撃者によって遠隔操作可能となります．攻撃者の主な目的は，ウイルス感染させたIoT機器上で不正なプログラムを実行して，第三者への攻撃に悪用すると共に，同じウイルスに感染可能な機器を探索して感染拡大を図ることです．機器乗っ取り型ウイルスのうち，ランサムウェアに感染した場合は，IoT機器の

注1：『情報セキュリティ白書2018』～『情報セキュリティ白書2023』のPDFファイルは，IPAのウェブ・ページからダウンロード可能です．
https://www.ipa.go.jp/publish/wp-security/index.html