

愛 知 発 明 賞

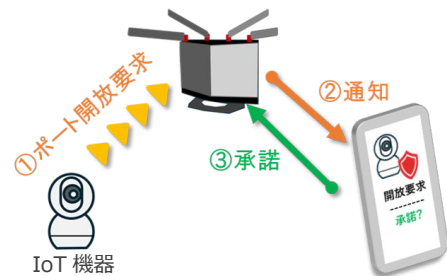
「危険なポート開放要求をブロックするルータ」

(特許 第 7 3 1 1 7 8 0 号)

稲田 哲也 株式会社バッファロー ネットワーク第一開発部
山田 大輔 株式会社バッファロー ネットワーク第一開発部

① 応募発明の概要

ワイドエリアネットワーク (WAN) とローカルエリアネットワーク (LAN) とを中継するルータであって、ルータが受信したパケットが、予め定められたリストに含まれるポートの開放を要求するものであった場合に、ユーザに対して通知を行い、ユーザの承諾を受けてからポート開放を行う。

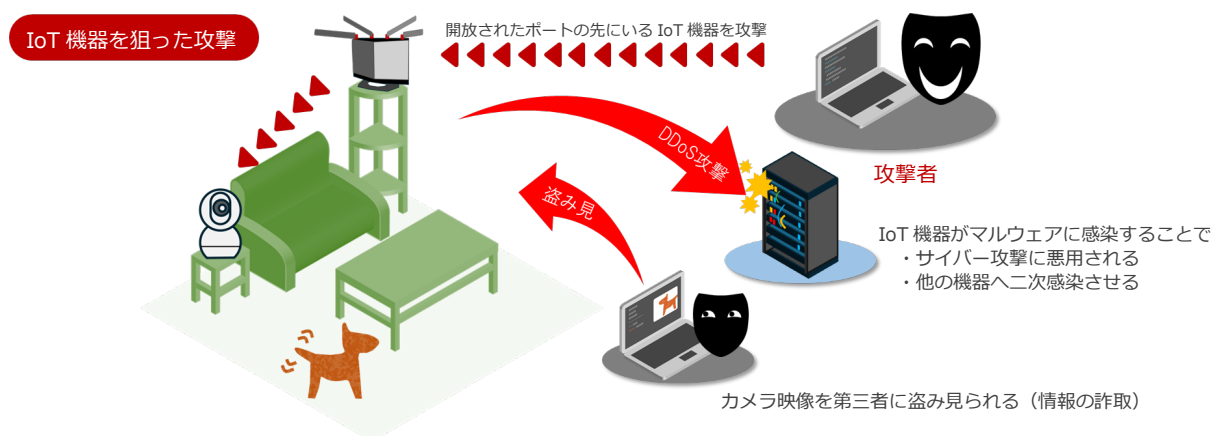


② 従来発明等の課題と開発ニーズ

近年、外出先からの自宅内の様子を見守る IP カメラや外出中でも来訪者に対応できるドアホン、録画番組を外出先で視聴可能なレコーダなど、宅内 (LAN 内) に設置して宅外 (WAN 側) からのアクセスが可能な様々な IoT 機器が普及している。この普及の背景には UPnP (Universal Plug and Play) による設定の容易化が挙げられる。

それまでは、WAN 側から LAN 内の IoT 機器にアクセスするためには、WAN と LAN の通信を中継するルータにおいて、その IoT 機器が通信に使うポートを WAN 側に対し開放する設定が必要であった。UPnP はこの設定を IoT 機器とルータ間で自動化することにより、知識のないユーザでも IoT 機器を LAN に接続するだけで簡単にポート開放の設定を可能とするもので、これにより様々な IoT 機器が広く普及することになった。

しかし、UPnP 対応機器の普及に伴い、悪意ある攻撃者がこれらの IoT 機器を標的とすることとなり、開放されたポートの先にある IoT 機器の脆弱性をつく攻撃が増加していた。特に見守りカメラのような IP カメラは、PC 等と比較してセキュリティ対策が十分でなく、また開放するポートが一般的に特定のポート番号と定められているため、攻撃者にとっては既知のポート番号を経由して IP カメラの存在を特定することが容易なため攻撃を受けるリスクが高いといわれている。

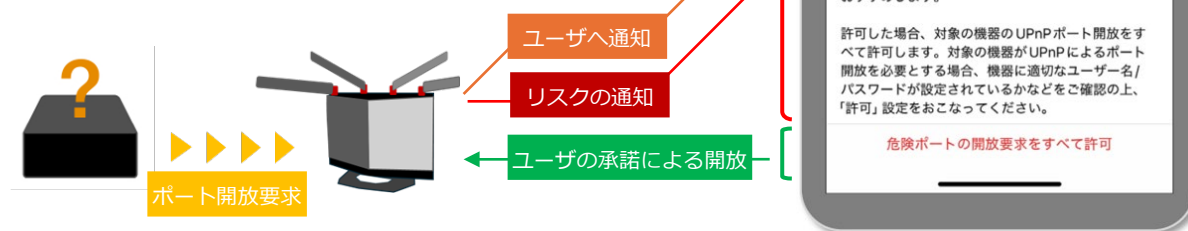


この点、特に大きな被害をもたらしたのものとして、2016 年に Mirai というマルウェアに感染した IoT 機器による大規模なサイバー攻撃が行われ、現在も Mirai を模倣した亜種による被害も継続的に発生している。これらの攻撃はいずれも UPnP の仕組みやポート開放に対するユーザの理解不足や IoT 機器の脆弱性を悪用したものであるため、ユーザに対しての意識啓発や注意喚起、IoT 機器に代わるセキュリティ上の対策が必要となっていた。

③ 応募発明等の特徴

応募発明に係るルータは、受信するパケットを監視し、そのパケットが特定のポートを開放する要求であった場合に、ユーザに対して通知を行い、ユーザが承諾をしたことに応じてポートの開放をすることとした。

また、通知の際にユーザに対してポート開放によるセキュリティ上のリスクを通知することで、ユーザはリスクを把握したうえで開放するか否かを選択することが可能となり、ユーザへの意識啓発や注意喚起につながることとなった。



また、ユーザは導入した IoT 機器を使わなくなった場合に、電源を入れたまま放置していたり、電源オフや機器の取り外しをしてもルータのポートを開放したままにしているケースがある。このような場合、放置した IoT 機器への攻撃や開放したままのポートに対して攻撃者の侵入を許すことになるため、セキュリティリスクが残ったままとなっている。

そこで、開放されたポートが所定時間使われていない場合には、ユーザにその旨を通知し、ポート開放の停止をすることとした。これにより IoT 機器の利用停止後のセキュリティリスクを低減することが可能となる。

さらに、導入した IoT 機器が運用中にも外部からの攻撃を受けるリスクはあるため、運用開始から所定時間アクセスが無かった外部デバイスから IoT 機器へのアクセスがあった場合にその旨を通知し、ユーザの承諾が無ければアクセスを許可しないこととした。これにより運用中に身に覚えのないアクセスがあった場合にそれを阻止することが可能となる。

上記の特徴により、ポート開放が必要な IoT 機器の利用開始から利用終了までを通してユーザへの意識啓発や注意喚起を行うことや、セキュリティリスクの低減が可能となった。

応募発明にかかる機能は「危険 UPnP ブロック機能」として、他のセキュリティ対策機能とともにネット脅威ブロック2として多数の無線 LAN ルータに搭載され、製品を通じてユーザへの啓発、注意喚起等を行い、安全に IoT 機器を利用できる環境をお客様に提供している。

