令和８年７月２１日
警察庁
総務省
国立研究開発法人情報通信研究機構（NICT）

家庭用 IoT 機器を悪用するレジデンシャルプロキシの現状

昨今、通信を中継する踏み台として家庭用 IoT 機器を悪用することでサイバー攻撃者が自らの所在や身元を隠しながら行われる事案が多発していることが明らかとなっています。

一般家庭等のインターネット回線に接続された IoT 機器が通信を中継するプロキシとして動作することから「レジデンシャルプロキシ（Residential Proxy）」と呼ばれています。レジデンシャルプロキシを経由して通信すると、通信先にはレジデンシャルプロキシとなっている一般家庭等に割り当てられた IP アドレスが記録され、本来の通信元の IP アドレスを把握することが困難となるほか、レジデンシャルプロキシに係る IoT 機器は「テレビに接続して無料で国内外の動画を視聴できます」などとうたって販売されている動画ストリーミングデバイス等の形で存在しており、IoT 機器の利用者の認識しないところでレジデンシャルプロキシとなっている場合もあります。

IoT 機器を利用する皆様におかれましては、以下に示すレジデンシャルプロキシとなる仕組み、レジデンシャルプロキシとして IoT 機器が悪用されるリスクを低減するための対策例等を参考に適切な対策を講じていただくようお願いいたします。

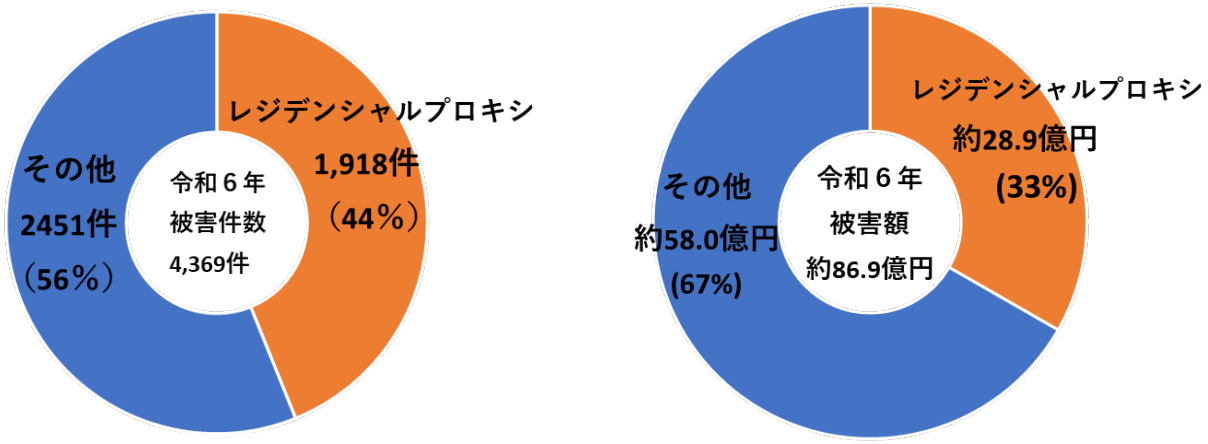
１．レジデンシャルプロキシの実態

レジデンシャルプロキシは、一般家庭向けのインターネット回線に接続された IoT 機器が第三者の通信を中継する仕組みです。通信先サーバ等のアクセスログにはレジデンシャルプロキシとなっている当該家庭等に割り当てられた IP アドレスが記録されるため、通信先の企業等において本来の通信元の把握や正規ユーザーとの判別が困難となります。また、海外からのサイバー攻撃対策として、海外からのアクセスを制限したサーバにもアクセスが可能となるなど、企業等におけるセキュリティ対策を回避しやすく、サイバーセキュリティ対策上の重大な脅威となるとともに、サイバー犯罪捜査においても深刻な障害となっています。

国立研究開発法人情報通信研究機構（NICT）の調査において、本年１月以降、１日平均で最大約 27,000 の IP アドレスがレジデンシャルプロキシの出口ノードとして観測されており、レジデンシャルプロキシは国内に少なくとも数万台以上の規模で存在すると推定されています。

警察では、レジデンシャルプロキシが不正アクセス事犯、詐欺等のサイバー事案において攻撃者の追跡や攻撃の検知を困難にする手口として悪用されている実態を把握しており、警察庁では、令和６年中に発生したインターネットバンキングに係る不正送金事犯において、犯行時にレジデンシャルプロキシが用いられたものが少なくとも 1,918 件、被害額約 28.9 億円に及び、被害件数全体の約 44%、被害額では約 33%を占めると分析しています。

インターネットバンキング不正送金被害の割合（令和６年中）



このほか、海外においては、レジデンシャルプロキシが DDoS 攻撃やランサムウェア攻撃に悪用されていることも報告されています。レジデンシャルプロキシは汎用性の高い攻撃ツールであるため、今後、重要なインフラへのサイバー攻撃を含む様々な攻撃に使われていくおそれがあります。

２．レジデンシャルプロキシとなる仕組み

「テレビに接続して無料で国内外の動画を視聴できます」などとうたって販売されている動画ストリーミングデバイスのほか、デジタルフォトフレーム、ルータ、ネットワークカメラ等の一般家庭向けのインターネット回線に接続して使用される IoT 機器等が次のような手口でレジデンシャルプロキシとなる事例が確認されています。

これらの機器やアプリ等においては、利用規約等の中にレジデンシャルプロキシとしての利用について記載されていたり、利用者の同意を求める画面が表示されていたりしても、利用者にとってわかりにくい場合があり、利用者が認識しないままレジデンシャルプロキシとしての機能が動作してしまう場合もあります。

(1) プロキシ化ソフトウェアのインストール等に伴うもの

- **プロキシ化マルウェアやアプリ**

  壁紙設定や無料 VPN サービス等の IoT 機器向けのソフトウェアやアプリ等の中には、プロキシ機能を持たせるためのソフトウェア開発キット（SDK：Software Development Kit）が組み込まれたものやレジデンシャルプロキシとして動作させるためのマルウェアが含まれている場合があり、これらを機器にインストールして使用する際に利用者の端末がレジデンシャルプロキシとなる事例が確認されています。

- **収益をうたう通信帯域提供サービスやアプリ**

  いわゆる「収益アプリ」と呼ばれる「使用していない通信帯域（データ通信量）を共有することで収益を得られる」とうたうサービスやアプリを利用することで、利用者の端末がレジデンシャルプロキシとなる事例が確認されています。

(2) IoT 機器自体に仕込まれたマルウェア（不正なソフトウェア）によるもの

- **製造過程又は流通過程で仕込まれたマルウェア**

  動画ストリーミングデバイス等の家庭用 IoT 機器の中には、購入前の製造・流通段階からレジデンシャルプロキシとして動作させるために必要なマルウェアやダウンローダー等が仕込まれているものもあり、当該機器をインターネットに接続することにより、使用者の気づかないうちに自動的にレジデンシャルプロキシとして動作したり、別のマルウェアをインストールしてレジデンシャルプロキシとなったりする事例が確認されています。

- **IoT 機器のぜい弱性等を突く**

  IoT 機器にぜい弱性やセキュリティ設定の甘さがある場合に、外部から侵入され、レジデンシャルプロキシとして動作させるためのマルウェアが仕込まれてしまう可能性があります。

３．レジデンシャルプロキシとして悪用されるリスクを低減するための対策例

(1) レジデンシャルプロキシとして悪用されることによる影響

IoT 機器等がレジデンシャルプロキシとして悪用された場合、当該機器の利用者自身が直接サイバー攻撃等を行っていなくても、通信の発信元として当該 IoT 機器が接続されたインターネット回線契約者に割り振られた IP アドレスや回線情報が通信先のサーバ等に記録されます。そのため、利用者自身がサイバー攻撃を行った者と疑われてしまう危険性があります。

さらには、当該 IoT 機器を介して家庭内のネットワークに侵入され、情報の流出、他の機器へのマルウェア感染拡大等の不利益が生じる危険性があります。

(2) レジデンシャルプロキシとして悪用されるリスクを低減するための対策例

利用する IoT 機器等がレジデンシャルプロキシとして悪用されるリスクを低減するため、利用者自身が現時点で取り得る対策例として以下を参考にしてください。

○ 提供元不明のソフトウェア、アプリ、無料 VPN 等を安易に利用しない

インターネット上で配信されている提供元不明のソフトウェア、アプリ、無料 VPN 等を安易にダウンロードしたり、使用したりしないでください。アプリ等は信頼できる提供元から入手するようにする、インストールする際にアプリの開発元、利用規約等を確認するなどを日頃から行ってください。

○ 収益をうたう通信帯域提供サービスやアプリを安易に利用しない

「使用していない通信帯域（データ通信量）を共有することで収益を得られる」などとうたうサービスを利用することは、知らないうちに自身の端末や契約回線をサイバー攻撃者の通信に利用させることにつながります。このようなサービスを安易に利用しないでください。

○ 不審な動画ストリーミングデバイス等の IoT 機器を使用しない

オンラインショップ等で販売されている「テレビに接続して無料で国内外の動画を視聴できます」などとうたう動画ストリーミングデバイス等の、本来有

料であるはずのサービスを無料で利用できるとうたう製品や価格が相場と比較して安価であるなど不審な製品の購入、使用はしないでください。

○　OS、ファームウェア等を最新の状態に保つ

パソコンやスマートフォンの OS、IoT 機器のファームウェア等のセキュリティ更新を適切に適用し、既知の脆弱性を放置せず、常に最新の状態に保つようにしてください。メーカーのサポートが終了した IoT 機器等は買い換えをすることも検討してください。

IoT 機器を利用している事業者・組織等においても、使用する端末や回線がレジデンシャルプロキシとして不正な通信に悪用されないよう、上記の対策に加え、次のような対策を講じることが重要です。

- 組織で承認していない機器や端末の業務ネットワークへの接続を防止する
- 業務用ネットワークと IoT 機器等のネットワークを適切に分離する
- ファイアウォールやアクセス制御の設定を適切に運用する