別紙１

家庭用 IoT 機器を悪用するレジデンシャルプロキシの対策について（提言）（案）

１．背景

近年、家庭用の動画ストリーミングデバイスをはじめとする IoT 機器に外部からの通信を中継するための不正なプログラムが仕込まれ、これを踏み台として行われるサイバー攻撃の被害が顕在化している。こうした IoT 機器や不正なプログラムは、インターネット・サービス・プロバイダ（ISP）から払い出される家庭用 IP アドレスを用いて通信の中継を行うこととなるため、「レジデンシャルプロキシ」と呼ばれる。レジデンシャルプロキシがサイバー攻撃のインフラとして認識され始めたのは概ね 2020 年以降である[1]。国内においても、同時期以降、サイバーセキュリティ上の脅威として取り扱われ、大学や研究機関における研究の対象となっている。

対策[2]については、警察庁が各都道府県警察の捜査を通じてレジデンシャルプロキシの悪用実態を認識し、いち早く取り組んできた。例えば、2025 年３月には「マルウェアに感染した家庭用パソコンや IoT 機器が悪用されプロキシサービスを通じて犯罪の踏み台となる事例」の注意喚起[3]を実施するとともに、2026 年３月には「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（被害件数 4,369 件、被害額約 86.9 億円）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のは少なくとも 1,918 件、被害額は約 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。」との報告[4]を行っている。

海外においてはより踏み込んだ対策が行われている例も見られ始めている。例えば、ドイツ連邦情報保安局（BSI）は、2024 年 12 月、ISP を通じて、レジデンシャルプロキシとして機能するマルウェア「Badbox」に感染したデバイスを所有するユーザへの通知を行っている旨を公表している。また、2026 年１月には、米 Google が、世界最大級のレジデンシャルプロキシネットワークを停止させる措置を講じたと発表した。

現状、我が国においてレジデンシャルプロキシの被害として可視化されているものは金銭的被害にとどまるが、これは氷山の一角であると考えられる。

---

[1] 例えば、Understanding Residential IP Proxy as a Dark Service(X. Mi et al.,2019)において、レジデンシャルプロキシをサイバー攻撃インフラとして成立させるための仕組みが初めて報告された。

[2] 国民を詐欺から守るための総合対策 2.0（令和７年４月２２日付け 犯罪対策閣僚会議）も参照

[3] 令和６年サイバー警察局便り「あなたの家の IoT 機器が悪用されている！？」（2025 年３月 13 日付け）

[4] 令和７年におけるサイバー空間をめぐる脅威の情勢等について（令和８年３月付け）

様々なサイバー攻撃を秘匿性高く実現するレジデンシャルプロキシの「サイバー攻撃インフラ」としての特性に鑑みると、今後、重要なインフラの機能不全を狙ったサイバー攻撃や政府機関等への標的型攻撃等に転用される可能性も十分に考えられるため、緊張感をもって状況を注視していくことが必要である。

レジデンシャルプロキシというサイバー攻撃インフラの存在やその国内被害の実態、今後のリスク等が徐々に認識される一方で、その対策が容易ではないことも明らかになりつつある。その理由としては、①IoT 機器は一般家庭の LAN 内に存在するため、ユーザが気付かなければ対策が進まない構造であること、②それにもかかわらず、様々な IoT 機器に巧みな方法で不正なプログラムが仕込まれるため、機器のユーザが悪用に気付けず、対策されにくいこと、③レジデンシャルプロキシが、日本国内の家庭用 IP アドレスを用いるため、海外からのアクセスを制限するサーバに対してもアクセスが容易であり、結果、被害組織側の対策を困難なものとしていること、④IoT 機器の製造はサプライチェーンが多層的であり、レジデンシャルプロキシ化させる不正なプログラムの開発者、それが仕込まれると対応が困難となる IoT 機器のメーカー、レジデンシャルプロキシ化した IoT 機器に指令を出す C2 サーバ[5]の管理者、さらにはレジデンシャルプロキシの IP アドレスを集約管理してプロキシサービスなどとして提供する者などが技術的・経済的に複雑に関与しあいながらレジデンシャルプロキシを成立させる仕組みが存在しており、サイバー攻撃インフラの維持・運営の主体がはっきりしないこと、などが挙げられる。

このようなレジデンシャルプロキシに係る複雑・巧妙な仕組みを踏まえると、引き続き実態解明を進めるとともに、警察庁において行っているサイバー攻撃者の実態解明・検挙等の取組に、官民のさまざまなステークホルダーの対策を掛け合わせ、複数のレイヤーからの多角的なアプローチを展開していくことが必要であろう。例えば、サイバー攻撃が飛び交うサイバー空間そのものを担う電気通信事業者や IoT 機器の脆弱性調査（NOTICE[6]）を実施している国立研究開発法人情報通信研究機構（NICT）との連携により、実効性の高い対策が実現すると考えられる。また、レジデンシャルプロキシ化しうる IoT 機器の流通に関与する事業者やセキュリティベンダが行う対策との連携も、検討の余地があると考えられる。レジデンシャルプロキシに関与するすべてのステークホルダーの英知を結集し、一丸となって対策を進めることで、社会全体として、不

[5] Command and Control サーバの略。外部から侵入して乗っ取るなどしたコンピュータ群に対して攻撃者からの指令を送り、制御を行うサーバコンピュータのこと。

[6]総務省、NICT、一般社団法人 ICT-ISAC、ISP、IoT 機器メーカー・SIer 等が連携し、IoT 機器のセキュリティ対策向上を推進することにより、サイバー攻撃の発生や、その被害を未然に防ぐためのプロジェクト。2019 年から実施

正なサイバー攻撃インフラのおそれのない安心・安全な社会を築いていくことが望まれる。

２．　対策の基本的な考え方

サイバー攻撃が飛び交うサイバー空間そのものを担う電気通信事業者、レジデンシャルプロキシ化した端末の利用者及びレジデンシャルプロキシで中継されるサイバー攻撃の被害者の三者を含む社会全体に資する対策を目指し、これにより不正なサイバー攻撃インフラのおそれのない安心・安全な社会を築いていくことが重要である。

３．　対策例

例えば、次の（１）から（５）までの対策が考えられる。

（１）レジデンシャルプロキシのサイバー攻撃インフラとしての実態の調査・分析

例えば、次のようなトピックが調査・分析の候補として考えられる。

① レジデンシャルプロキシ化した端末に仕込まれた不正なプログラム
② レジデンシャルプロキシの C2 サーバ
③ 機器がレジデンシャルプロキシ化する経緯

（２）レジデンシャルプロキシ化した端末を経由した不正アクセス行為等に係る被害申告に基づく利用者への注意喚起

本件注意喚起について、例えば、次の①～⑤のような連携が考えられる。なお、具体的な実施方法については、実態にあわせて関係者で適切に検討する必要がある。

① 不正アクセス行為等の被害者は、都道府県警察の捜査等の過程において、不正アクセスの発信元となる端末の利用者を特定するために必要な不正アクセスの発信元に係る IP アドレス、ポート番号及びタイムスタンプといった情報を提供する。
② 被害者が、不正アクセスの発信元となる端末の利用者に対して注意喚起を行うことを申し出た場合や注意喚起の実施に同意した場合は、警察庁又は都道府県警察は、当該 IP アドレス、ポート番号及びタイムスタンプといった情報を、ICT-ISAC などの通信業界団体に情報共有する。

③ 情報共有を受けたICT-ISACなどの通信業界団体及びNICT[7]等の機関は、発信元となる端末がDDoS攻撃等をも行いうるサイバー攻撃インフラに該当するかどうかを合理的に確認したうえで、対象となるISPを特定し、当該ISPに対して当該IPアドレス、ポート番号及びタイムスタンプといった情報の共有とともに注意喚起の要請を行う。

④ 注意喚起の要請を受けたISPにおいて、不正アクセスの発信元となる端末に係るIPアドレス、ポート番号及びタイムスタンプといった情報を基に、タイムスタンプに示された時刻において当該IPアドレスをどの利用者に割り当てたか確認して、該当利用者を割り出す。

⑤ 該当利用者に対して、個別に注意喚起を行う。

（別紙の１．参照）

（３）レジデンシャルプロキシによるサイバー攻撃の中継の抑止

本件サイバー攻撃中継抑止について、例えば、次の①～④のような連携が考えられる。

① 都道府県警察やNICT等が、捜査や研究等により、不正送金や不正アクセス等に悪用されているレジデンシャルプロキシ化した端末を支配下に置いているC2サーバに係るFQDN[8]等を把握し、C2サーバリストを作成する。

② 警察庁又は都道府県警察、NICT等は、当該C2サーバリストを、ISPに対して提供する。

③ ISPは、提供されたリストに基づき、自社DNS[9]サーバで処理する契約回線からのアクセスに係るFQDNを検知し、C2サーバのFQDNの名前解決要求に係る通信を遮断する。

④ レジデンシャルプロキシ化した端末による不正アクセス等は、レジデンシャルプロキシ化した端末がC2サーバとの通信を確立した後にはじめて行われることから、③によって、レジデンシャルプロキシ化した端末とC2サーバとの通信の確立を防ぐことで、その後に行われるサイバー攻撃の中継を抑止することができるため、結果として、不正アクセス等による被害の減少が見込まれる。

（別紙の２．参照）

---

[7] IoT機器の脆弱性調査（NOTICE）においては、NICTが、サイバー攻撃に悪用されている、または悪用される危険性があるIoT機器を観測し、ICT-ISACに対して、その観測結果や対処方法の通知を行っている。

[8] Fully Qualified Domain Name の略。サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ（サーバ等）を特定するもの

[9] Domain Name System の略。インターネット上のコンピュータ同士が通信する際に、通信相手を特定するためにドメイン名とIPアドレスを対応づける仕組みのことをいう。

（４）上記対策及び機器流通の抑止その他の対策を官民のステークホルダーにより有機的に連携させる取組

（５）上記（１）から（４）までの対策を踏まえた、国民に対する広報啓発や注意喚起

（別紙）

３．（２）及び（３）の対策に関する通信の秘密との関係についての整理

１．　３（２）の対策について

- 注意喚起の要請を受けたISPにおいて、不正アクセスの発信元となる端末に係るIPアドレス、ポート番号及びタイムスタンプの情報を基に、タイムスタンプに示された時刻において当該IPアドレスをどの利用者に割り当てたか確認して、該当利用者を割り出すことは、当該利用者だけでなく、検索の際に参照される他の利用者の通信の秘密をも侵害するものである。もっとも、本件対策については、以下の検討のとおり、正当業務行為として違法性が阻却されると考えられる。

＜検討＞

- 「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第三次とりまとめ」[10]第２章第２節（以下「三次２節」という。）において、「マルウェアに感染している可能性が高い端末の利用者に対する注意喚起」についての考え方が整理されているところ、この考え方を適用することができないか検討する。
- まず、三次２節では、対策の概要として「ISPが、信頼できる第三者機関からの情報提供や事業者自身による個別の検知等により、マルウェアに感染している可能性が高い端末が行った通信に関する当該端末のIPアドレス、ポート番号及びタイムスタンプを情報として得た場合において、ISPの保有する契約者情報、通信履歴等と上記IPアドレス、ポート番号及びタイムスタンプを照合し、当該端末に係る通信回線の契約者及び連絡先を特定した上で、当該契約者に対して電子メールの送付等の方法により注意喚起を行うことが考えられる。」としている。

  本件注意喚起においても、都道府県警察が捜査等の過程で把握した不正アクセスの発信元に係るIPアドレス、ポート番号及びタイムスタンプの情報を警察庁又は都道府県警察から提供を受け、レジデンシャルプロキシ化した当該端末に係る通信回線の契約者及び連絡先を特定して、当該契約者に対して電子メールの送付等の方法により注意喚起を行うことを想定しているため、対策の構造としては同一視できると言える。

[10] https://www.soumu.go.jp/main_content/000575399.pdf

- **違法性阻却事由**：三次２節において整理を行った対策は、「マルウェアに感染している可能性が高い者全体を対象」としており、また、「マルウェアに感染して被害が生じていると判断できない者を対象としている」ことから、「現在の危難又は急迫不正の侵害が生じているとまではいえず、緊急避難又は正当防衛として許容されるとの整理は困難である」とされている。また、「ISP において自主的に行われる取組であることから、法令に基づく行為にも該当しない」とされている。

  本件注意喚起においては、申告された通信元のレジデンシャルプロキシ化した端末が、「知らないうちにマルウェアに感染するなどして乗っ取られた一般利用者の通信機器（ボット）」であることはほぼ確実であるが、現在の危難又は急迫不正の侵害の具体的内容や法益の権衡について明確でないことから、三次２節と同様に、正当業務行為として整理される余地はないか検討することとする。

- **目的の正当性**：三次２節における対策の目的は、「注意喚起を行うことにより、電気通信役務の利用者がマルウェアによる被害を受けることを防止するとともに、マルウェアに感染した端末が DDoS 攻撃等の通信を行うことで当該利用者に対して電気通信役務を提供する ISP の電気通信役務の提供に支障が生じる場合に当該支障を防止することにある。」としている。

  この点、警察庁又は都道府県警察から提供される IP アドレス、ポート番号及びタイムスタンプの情報は、不正アクセスに係るものであり、提供の趣旨もこの解決であるといえる。もっとも、レジデンシャルプロキシ化した端末は、一般に、不正アクセスにとどまらず、DDoS 攻撃等の通信にも用いられるというサイバー攻撃インフラとしての性質を持つことから、当該利用者に対して電気通信役務を提供する ISP の電気通信役務の提供に支障が生じるおそれは十分に考えられる上[11]、提供された IP アドレス等と脅威インテリジェンス情報[12]を組み合わせることで、提供された IP アドレスが DDoS 攻撃等を行いうるサイバー攻撃インフラであることが確認できるため、当該利用者に対して電気通信役務を提供する ISP の電気通信役務の提供にも支障が

---

[11] 三次２節において、「なお、対象となっている端末が感染しているマルウェアの性質、予想される攻撃やそれに対する対処の困難性等からみて、電気通信役務の提供に支障を生じさせる通信をするおそれが低い場合は、専ら利用者の被害を防止する目的で行われることとなるから、目的の正当性が肯定できないと考えられる。」とあるが（第三次とりまとめ 14 頁）、端末が不正に操作されうるレジデンシャルプロキシであるという事実は、常に DDoS 攻撃等のおそれを潜在的に生じさせるものである。

[12] サイバー攻撃の兆候や手法、攻撃者の動向に関する情報を収集・分析し、組織がセキュリティ対策の決定や防御に活用できる形に加工した情報のこと。関係者コミュニティでの情報交換やウェブサイトからのクローリングなどで入手するほか、専門の民間事業者が販売していることもある。レジデンシャルプロキシについても、レジデンシャルプロキシサービスが提供している IP アドレスを入手できるほか、これを脅威インテリジェンス情報として販売する事業者も存在している。

生じる場合があるとして、当該支障を防止する目的で注意喚起を行うことが可能であると考えられる。なお、提供された情報に関連するサイバー攻撃が当該サイバー攻撃インフラによるものであるとの確認は、複数の主体により合理的かつ継続的に実施されることが重要である。

警察庁又は都道府県警察から提供される IP アドレス、ポート番号及びタイムスタンプの情報と脅威インテリジェンス情報の組み合わせによるサイバー攻撃インフラの確認の具体的な方法としては、次のようなものが考えられる。まず、提供された IP アドレスが、脅威インテリジェンス情報として得られた IP アドレス群に含まれるかどうかを確認する。その上で、この IP アドレス群が、DDoS 攻撃等を行いうる IP アドレスも同時に包含するものであるかを確認する。これにより、提供される IP アドレスの特性が、ある IP アドレス群の特性と同一視でき、さらに、この IP アドレス群は DDoS 攻撃等を行いうるものでもあるため、提供された IP アドレスについても DDoS 攻撃等を行いうるものであることが言える。

- 行為の必要性：三次２節における対策において、「(ISP の電気通信役務の提供に生じる支障を防止するという)目的を達成するという観点からみて行為の必要性があるといえるのは、利用者の意思の如何にかかわらず、利用者に対して注意喚起を行って対処を求めなければ DDoS 攻撃等によって電気通信役務の提供に支障が生じるといえる程度に具体的な危険が予見される場合であると解される」としており、「具体的な危険」の例として、「DDoS 攻撃等を行うマルウェアに感染している蓋然性がある端末が、当該端末に係る利用者に対して電気通信役務を提供する ISP において多数存在する場合には、一般には上記のような具体的な危険が予見される」としている。

  この点、警察庁又は都道府県警察から提供される IP アドレス、ポート番号及びタイムスタンプの情報に含まれるレジデンシャルプロキシ化した端末の IP アドレス等の数は限定的であると考えられるが、先に述べたとおり脅威インテリジェンス情報として得られた IP アドレス群と組み合わせることで同類のレジデンシャルプロキシ化した端末が多数存在することが推定できる場合には、具体的な危険が予見されるものと判断して差し支えないと言える。

- 手段の相当性：三次２節においては、「多くの利用者は注意喚起に必要不可欠な限度においてこれら[13]を利用することを許容すると解されるものの、具体的な氏名、連絡先等を含むことからすれば、通信の秘密及びプライバシー

[13] 「IP アドレス、ポート番号及びタイムスタンプといった通信の秘密のほか、氏名、連絡先等のプライバシーに係る情報」(三次取りまとめ 15 頁)

の侵害の程度は客観的にみて小さいとはいえない。そのため、自らの権利利益を害されたくないと望む利用者を含めた利用者全体に対して注意喚起を行うことにつき手段の相当性が認められるのは、そのような措置をとることが電気通信役務の提供のために必要やむを得ない場合」、すなわち、「既にDDoS 攻撃等を行った端末やマルウェアに感染している蓋然性のある端末等の利用者に対して注意喚起を行う場合等」に限られるとしているところ、本件注意喚起においてはこの条件を満たして行われるものであり、手段の相当性が肯定できるものと考えられる。

- 上述のとおり、本件注意喚起についての通信の秘密に係る整理は、三次２節と同一視できるものであり、その適用に際しては、行為の必要性を判断するための「具体的な危険」を明確にする必要がある。

２．３（３）の対策について

- 本件サイバー攻撃中継抑止については、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ」[14]第２章第１節の整理に基づき実施することが可能と考えられる。なお、同整理は、C2 サーバ等の FQDN が判明している場合において、マルウェアの感染者が情報窃取や金銭的被害等の深刻な被害を受けることを防ぐとともに、感染者を踏み台にした新たな攻撃の発生を防ぐため、ISP が自社 DNS サーバで処理する契約回線からのアクセスに係る FQDN を検知し、C2 サーバ等の FQDN の名前解決要求に係る通信を遮断することについて、オプトアウト付き包括同意により利用者の有効な同意を取得することができるとされている。

[14] https://www.soumu.go.jp/main_content/000376396.pdf