

「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）
に対して提出された意見及びその意見に対する考え方

○ 意見募集期間：令和 8 年 7 月 22 日（水）～同年 8 月 4 日（火）

○ 意見提出数：22 件（法人・団体：6 件、個人：16 件）

※意見提出数は、意見提出者数としています。

※法人・団体と事務局で判断できるもの以外の御意見は個人としてカウントしておりますので、御了承ください。

※頂いた御意見につきましては、記載の明確化等のため、体裁の修正や実質的な内容の変更をもたらさない形式的な修正を行っております。

項番	意見提出者
1, 13～16	一般社団法人 ICT-ISAC
2	ソフトバンク株式会社
3, 22, 23, 36	NTT ドコモビジネス株式会社
17～19, 35	Infoblox 株式会社
20	KDDI 株式会社
21	AppLogic Networks Japan 株式会社
—	個人（16 件）

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
1	一般社団法人 ICT-ISAC	提言全体	ICT-ISAC は、本提言案の趣旨に賛同いたします。	賛同の御意見として承ります。
2	ソフトバンク株式会社	提言全体	本提言案が目指すレジデンシャルプロキシ対策を着実かつ持続可能なものとするためには、各対策の実効性や費用対効果を実施の過程で丁寧に検証し、その結果を踏まえて継続的に改善していくことが重要である。 特に、通信事業者による利用者の特定や注意喚起は、一定の業務負担を伴うことから、対象・期間・規模を限定した実証を行い、効果と負担の両面から評価すべきである。本取組を通して、分かりやすい注意喚起文面や対応導線の検討、利用者の反応や問い合わせ傾向の分析等、対策の実効性向上に期待したい。また、検証結果を踏まえ、継続の有無も含め検討や必要に応じて手法や対象を見直す仕組みを設けることを求める。	提言案にも記載のとおり、利用者への注意喚起の具体的な実施方法については、実態に合わせて関係者で適切に検討することが重要であると考えています。 御意見については、今後の検討を進める上で参考とさせていただきます。
3	NTT ドコモビジネス株式会社	提言全体	本提言の方向性に賛同いたします。家庭用 IoT 機器を悪用するレジデンシャルプロキシは、利用者が気付かないままサイバー攻撃の踏み台として悪用されるおそれがあり、利用者保護のみならず、我が国全体のサイバーセキュリティ確保の観点からも重要な課題であると認識しております。また、今後は AI 機能を搭載した家電製品や家庭内ネットワークに接続される各種スマート機器の普及が進むことが見込まれ、そのリスクがさらに拡大する恐れもあると考えます。 提言に示されているとおり、警察、NICT、ICT-ISAC、ISP、IoT 機器関連事業者及びセキュリティ事業者等が連携することにより、実効性の高い対策が実現するという考えに賛同いたします。その際、対策の対象として IoT 機器に加え、上述の AI 家電製品や、サポート終了を迎え脆弱性を抱えている家庭内のルーター設備など、家庭内に設置され得るネットワーク機器を幅広く対象として検討を進めるにより、対策の有効性を更に高めることが可能になると考えます。	賛同の御意見として承ります。 御意見については、今後の検討を進める上で参考とさせていただきます。
4	個人	提言全体	1. 総論(提言案に対する基本的立場と改善の視点) 本提言案が、近年深刻化している家庭用 IoT 機器等を踏み台としたレジデンシャルプロキシの悪用に対し、	賛同の御意見として承ります。 本提言案では、通信の秘密との

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			関係省庁、警察、国立研究開発法人情報通信研究機構(NICT)、一般社団法人 ICT-ISAC、および電気通信事業者(ISP)等の官民連携による多角的なアプローチを提示している点につき、深く賛同いたします。 一方で、本施策を現場で円滑かつ実効的に運用し、国民の理解と協力を得ながら推進していくためには、以下の3つの課題に対する配慮が重要であると考えます。 (1) 利用者の IT リテラシーに配慮した実効性ある対処サポートの提供 (2) 電気通信事業者(ISP)の法的リスク・運用負担の軽減とガイドラインの明確化 (3) 誤検知・過剰遮断を防止するための手続き的適正性と透明性の確保 これらの課題は、制度の根本的な再構築を要するものではなく、運用ガイドラインの提示や規定の追記・補強によって比較的に容易に実現可能なものです。パブリックコメントとして以下の具体的改善提案を提出いたしますので、ぜひご検討ください。 2. 各論(具体的改善提案) ■ 提案 1: 注意喚起通知における「分かりやすい対処手順」とサポート体制の追記 【該当箇所】 ・本文 P.4「3. (2) (5) 該当利用者に対して、個別に注意喚起を行う。」 ・本文 P.5「3. (5) 国民に対する広報啓発や注意喚起」 【意見・提案内容】 ISP から利用者へ個別注意喚起を行う際、単に「感染の事実や危険性」を通知するだけでなく、一般利用者が迷わずに復旧対応を実行できるよう、標準的な対処手順(機器の再起動、ファームウェアの最新化、初期パスワードの変更等)を記載した分かりやすいマニュアルや、問い合わせに対応する専用ヘルプデスク・ポータルサイトへの誘導情報(URL・Q&A 等)をあわせて提供する旨を提言内に明記することを提案します。 【理由】 一般的な家庭用 IoT 機器の利用者は、高度なネットワーク知識を有していないケースが大半です。単に悪用	関係を踏まえつつ、レジデンシャルプロキシによる被害への対応に必要と考えられる対策例を整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			の事実のみを告げられても、自力で機器の特定や不正プログラムの除去を行うことは困難であり、放置されてしまう恐れがあります。容易かつ具体的なアクションプランとサポート窓口を提示することが、実効的な被害防止につながります。 ■ 提案 2: 脅威インテリジェンス情報の品質基準と「誤検知防止プロセス」の明記 【該当箇所】 ・ 本文 P. 8 「1. (2) の対策について(目的の正当性・行為の必要性)」 【意見・提案内容】 警察からの情報提供に加え、民間の「脅威インテリジェンス情報」を組み合わせ注意喚起対象の IP アドレス群を推定・特定するプロセスにおいて、誤検知(正常な通信や動的 IP アドレス割り当て変更に伴う無関係な利用者の巻き込み)を未然に防ぐための「採用する情報の精度基準」および「段階的な照合・検証手順」に関するガイドラインを策定することを提言内に明記することを提案します。 【理由】 民間の脅威インテリジェンス情報には更新のタイムラグや精度差が存在します。古い情報や不正確な情報に基づき注意喚起や回線特定が行われた場合、無実の利用者に不利益が生じるだけでなく、通信の秘密への配慮という点でも正当性が揺らぐリスクがあります。情報照合の確実性を担保する基準を示すことで、施策の信頼性が大幅に高まります。 ■ 提案 3: 電気通信事業者 (ISP) 向け運用ガイドラインの早期策定と免責範囲の明確化 【該当箇所】 ・ 本文 P. 6 - P. 9 「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」 【意見・提案内容】 ISP がログの照合・特定、個別注意喚起、および C2 サーバ宛通信の名前解決遮断 (DNS ブロッキング) を実施	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			するにあたり、通信業界団体 (ICT-ISAC 等) や関係省庁と連携して「事業者向け標準運用ガイドライン」を早期に策定し公表する方針を記載することを提案します。また、同ガイドラインに沿って正当に実施された措置について、事業者側の免責範囲や問い合わせ対応の責任分担を明確化することを求めます。 【理由】 ISP にとって、通信の秘密に関わるログ照合やオプトアウト付き包括同意に基づく通信遮断の実施は、法的リスクや利用者からの苦情対応を伴う大きな負担となります。標準的かつ明確な運用指針が示されることで、事業者が安心して迅速に対応できる環境が整い、業界全体での一律かつ円滑な対策推進が可能となります。 ■ 提案 4: 既存枠組み (NOTICE プロジェクト等) との連携深耕とメーカーへのフィードバック 【該当箇所】 ・ 本文 P.2 「1. 背景」 ・ 本文 P.5 「3. (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」 【意見・提案内容】 現在 NICT 等が推進している「NOTICE」(IoT 機器の脆弱性調査・通知プロジェクト)等の既存の通知枠組みやシステム基盤と本施策を可能な限り一体的・相互補完的に運用することを提案します。また、レジデンシャルプロキシ化が確認された機器の種別や型番などの傾向情報を、個人や回線を特定できない形で集計し、IoT 機器メーカーや業界団体へフィードバックする仕組みを構築することを追記してください。 【理由】 既存の制度や通知スキームを活用することで、運用コストや事業者のシステム開発負荷を最小限に抑えられます。また、メーカー側に具体的な被害傾向や脆弱性情報を還元することで、製品の出荷時セキュリティ向上やファームウェア修正等の根本的な対策を同時に促進することができます。	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			■ 提案 5: 施策の実施状況・効果の定期公表による透明性の確保 【該当箇所】 ・ 本文 P. 5 「3. (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」 【意見・提案内容】 本対策の運用開始後、年次の実施状況(注意喚起の件数、C2 サーバ遮断の適用件数、誤検知等の発生有無および問い合わせ傾向等)を定期的に取りまとめ、個人情報や通信の秘密に配慮した上で公表・検証する規定を盛り込むことを提案します。 【理由】 通信の秘密の例外的な整理を伴う施策であるからこそ、実施状況や効果を定期的に可視化・検証することが不可欠です。透明性を持った運用と改善を継続することで、国民からの信頼と理解を長期的に確保することができます。 3. 結び 以上の提案は、本提言案の基本的な方向性を維持しつつ、現場での運用性、利用者の利便性・理解度、および法的安全性を高めるための実用的かつ容易に導入可能な改善策です。 貴省におかれましては、本意見をご検討いただき、より一層安全で持続可能な情報通信環境の実現に向けた最終提言の取りまとめに活かしていただくことを期待申し上げます。	
5	個人	提言全体	サイバーセキュリティ以前に、政府が 国民の個人情報（特定個人情報ファイル）を AI 企業に 本人の承諾無しに売り渡したり、国民を政府がサイバー監視する様な状況では、全く意味が無いだろう。 まず政府の行っている不正行為・違憲行為をやめろ。	御意見として承ります。
6	個人	提言全体	提言に基づく対策について、「不正アクセス防止対策に関する行動計画」（平成 23 年 12 月 22 日官民ボード決定）との役割分担を、どのような形とすることを想定されているか明らかにされたい。 家庭用 IoT 機器を悪用する行為は、「他人の ID・パスワードを悪用したり、コンピュータ・プログラムの不正	家庭用 IoT 機器を悪用するレジデンシャルプロキシによる不正アクセスは、これまでのインタ

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			備をつくことにより、本来アクセスする権限のないコンピュータ（サーバ）を利用する行為」に該当するとすれば、同行動計画の対象であり、その異同・重複を整理する必要があると考えられる。 また、不正アクセス防止対策に関する官民意見集約委員会など、既存の産官学の連携スキームが存在するところ、官民意見集約委員会を「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」として活用することを提言に含めてはどうか。	ーネットバンキング等への不正アクセスとは異なり、不正なプログラムの開発者、IoT 機器のメーカー、IoT 機器に指令を出す C2 サーバの管理者などが技術的・経済的に複雑に関与し合いながら攻撃インフラを成立させる等、従来にはない複雑な仕組みによりサイバー攻撃が行われていることから、本提言案は、官民のステークホルダーが有機的に連携する取組を新たに提言するものです。
7	個人	提言全体	賛成 個人の消費者として意見 該当箇所 「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。」 質問 ここでいう「Badbox」というマルウェアは、インターネットマーケット、オンラインショッピングサイトで購入した Android や Android TV などの端末に、本来有効化されるはずのない開発者モードの adb プロトコルが、購入時から組み込みのバックドアとして起動して不正なサーバーと遠隔通信を行い感染するマルウェア	本提言案は、家庭用 IoT 機器を悪用するレジデンシャルプロキシへの対策を取りまとめたものであり、機器流通の抑止についても対策例として記載しており、御指摘については参考とさせていただきます。なお、御指摘の生成 AI サービスに係る規制等に関する事項については、本提言案の対象外となります。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			であると認識している。その結果ボットネットとして悪用された端末がレジデンシャルプロキシ化され、ダークフォーラムで販売されているという問題だったが、デジタルプラットフォームで販売されていた不正商品、違法製品について、事前にプラットフォームやショッピングを運営している事業者の責任はないのか たとえば、最近では EU が違法な製品を販売したとして Temu と Aliexpress に巨額な罰金を課している。 質問 また、最近では ChatGPT や Claude などのチャットボットを用いてサイバー犯罪に至る行為が多発しているが、商用 LLM がレジデンシャルプロキシも含めマルウェア作成、許可のない脆弱性スキャンの手段、方法を提供するのが容易であり、未成年やデジタルリテラシー不足の方たちがサイバー攻撃に加担しやすくなっているのではないのか そして日本人でも軽はずみで ChatGPT、Claude などの商用 LLM からネット犯罪等のために悪用する可能性は十分にあり、リスクのある AI のチャットボットが犯罪行為の教唆、加担する出力を行い、日本人も違法な行為に及ぶ可能性がますます拡大している。 これらの生成 AI を提供するデジタルプラットフォームが負う責任や規制は、将来の起こりうる犯罪対策の一環としても、安全のためにも AI 規制は行うべきではないのか 質問 通信の秘密はしっかり守られるのか	また、本提言案では、通信の秘密との関係を踏まえつつ、レジデンシャルプロキシによる被害への対応に必要と考えられる対策例を整理しています。
8	個人	提言全体	家庭用 IoT 機器の悪用などのサイバーセキュリティ対策およびその罰則規定に関して、以下の通り、企業側および犯罪者側の双方に対する強力な規制と罰則の強化を求めます。 1. 企業側に対するセキュリティ体制の義務化と厳罰化 ・販売企業に対し、セキュリティ対策を日常的に実施するシステム体制の構築を義務化すること。	本提言案では、家庭用 IoT 機器を悪用するレジデンシャルプロキシへの対策を取りまとめており、機器流通の抑止その他の対策についても対策例として整理

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			・国や第三者機関による監査で対策の怠慢が判明した場合、日本の訴訟環境の特性（被害者が個別に損害賠償を求めにくい現状）を考慮し、企業が形式的な謝罪のみで済ませて負担が低くならないよう、国の罰金を大幅に厳罰化することで実効性のある抑止力を強化すること。 2. 犯罪者側および犯罪グループに対する強力なペナルティの導入 ・サイバー攻撃やハッキングを行った犯罪者に対し、罰則をより一層強化すること。海外からの攻撃で逮捕が困難であっても、犯人が判明した場合には日本への入国禁止などの厳格な措置を講じること。 ・個人のみならず、身代金を要求するなどの犯罪グループを特定できた場合は、その組織に属する団員すべてを入国禁止等の対象とすることで、犯罪者の増加抑制につなげること。 ・立証が完全ではなくとも、警察側が関与の可能性を認定した段階で同様の措置を講じることにより、犯罪グループのメンバーに「旅行ができなくなる」等の不利益を被るリスクを意識させ、組織内での牽制や犯罪抑止の効果を高めること。 総じて、企業・犯罪者の双方に対してより厳格な罰則を適用し、特に逮捕や資産追跡が困難な犯罪者に対しても疑いの時点で強い不利益を与える仕組みを構築することを強く要望する。	しています。 御指摘の機器の安全性確保や流通段階における対策に関する事項については、今後の検討を進める上で参考とさせていただきます。 その他の事項については、御意見として承ります。
9	個人	提言全体	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を実施することについて賛同します。 提言の内容に加えて、IoT 機器を悪用された機器の利用者や、悪用するためのサービス事業者、端末販売者、端末をオンラインで販売する事業者についての罰則も必要ではないでしょうか。 特に「犯罪の踏み台となった事例」については何らかの対応をとるべきです。犯罪に加担した端末の利用者には、少なくとも当該 IoT 機器やサービスを使うことは禁止するべきです。	本提言案では、家庭用 IoT 機器を悪用するレジデンシャルプロキシへの対策を取りまとめており、機器流通の抑止その他の対策についても対策例として整理しています。 御指摘の関係事業者及び利用者への対応に関する事項については、今後の検討を進める上で参

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
				考とさせていただきます。
10	個人	提言全体	<意見の概要> 本意見は、総務省「巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会」による標記提言案に対し、提言の方向性自体は評価しつつ、その対策が「対症療法」の域を出ておらず、脆弱性の根本原因?? IoT 機器のファームウェアが C/C++等のメモリ非安全言語で書かれていること??に踏み込んでいない点を厳しく指摘し、言語レベルでの抜本的対策の導入を求めるものである。 なお、本意見の提出にあたり、意見書提出様式が Word 形式 (.docx) で提供されていること自体がセキュリティホールである点を付言する。Word のマクロ機能 (VBA) は長年にわたりマルウェア感染経路のトップであり続けており、サイバーセキュリティを論じる政府機関が、皮肉にも自身の意見募集プロセスでマクロ付き文書形式を推奨している矛盾を認識されたい。 <問題の所在?なぜレジデンシャルプロキシ対策は対症療法に留まるのか> レジデンシャルプロキシとは、一般家庭の IoT 機器 (ルータ、IP カメラ、スマート TV 等) を乗っ取り、攻撃者の通信を経由させる踏み台網である。その根本原因は、これらの IoT 機器のファームウェアが C/C++で書かれており、メモリ安全性に起因する脆弱性??バッファオーバーフロー、use-after-free、ダングリングポインタ??が放置されていることにある。 Microsoft および Google の調査では、全セキュリティ脆弱性の約 70%がメモリ安全性問題に起因する。米国ホワイトハウス国家サイバー局長官室 (ONCD) は 2024 年 2 月、報告書「Back to the Building Blocks」において、C/C++を国家安全保障上のリスクと指定し、Rust 等のメモリ安全言語への移行を全産業に要請した。2025 年 6 月には CISA が「メモリ安全言語導入ロードマップの作成・公表」をソフトウェア製造業者に義務づけるガイダンスを発出。DARPA は 2023 年より TRACTOR プログラムにより C/C++コードの Rust への自動変換技術に巨額投資している。 一方、本提言案は“筆者が総務省サイトで確認した限り”ルータの初期パスワード変更啓発、ISP による通	御意見として承ります。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			信監視強化、消費者への注意喚起といった「運用対策」に終始している。これらは必要ではあるが、根本的解決ではない。C/C++で書かれたファームウェアが動き続ける限り、新たな脆弱性は無限に生まれ続ける。 ＜なぜ Rust なのか??メモリ安全性の技術的意義＞ Rust は、ガベージコレクション (GC) を用いずに、コンパイル時に「所有権 (ownership)」「借用 (borrowing)」「ライフタイム (lifetime)」の 3 概念によってメモリ安全性を保証する言語である。これにより C/C++と同等の実行性能を維持しつつ、全脆弱性の 70%を占めるメモリ安全性バグを原理的に排除できる。 筆者は Rust エコシステムにおいて数百のオープンソースクレート (crates.io 全登録数の約 0.3%) を運用し、GDAL 代替の OxiGeo、FFmpeg 代替の OxiMedia、SPARQL エンジン OxiRS 等の純粋 Rust 実装を手がけている。この経験から断言する??IoT 機器のファームウェアを Rust で再実装することは、もはや技術的困難ではなく、意思決定の問題である。 現に、Google は Android の新規コードを Rust で書き始め、メモリ安全性脆弱性が激減したことを報告している。Microsoft は Windows カーネルの一部を Rust で書き直し、「Year of Rust 2025」を宣言した。Amazon は AWS の中核仮想化基盤 Firecracker を Rust で実装した。IoT 分野では、Espressif 社が ESP32 シリーズの公式 Rust サポートを提供している。 ＜法制面の検討??サイバーセキュリティ基本法との関係＞ サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 12 条は「国及び地方公共団体は、サイバーセキュリティに関する施策の策定及び実施に当たっては、最新の技術的動向を踏まえる」と規定している。さらに第 14 条は「事業者の自主的な取組の促進」を国の責務としている。 第 217 回国会（令和 7 年 3 月 18 日）における石破茂内閣総理大臣の施政方針演説では、日本航空へのサイバー攻撃による欠航事案を引き合いに「サイバー対処能力強化」の必要性が強調された。しかし「対処能力」とは、攻撃を受けた後の対応だけでなく、攻撃を不可能にするアーキテクチャレベルの防御を含むべきである。	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			本提言案に欠けているのは、まさにこの「根本的予防」の視点？脆弱性を作り込まないプログラミング言語の採用？である。 <具体的提言> 一. 本提言に「IoT 機器ファームウェアのメモリ安全言語への移行促進」を明記すること。具体的には、政府調達基準において IoT 機器のファームウェアがメモリ安全言語（Rust 等）で実装されていることを加点項目とする制度設計を検討されたい。 二. IoT 機器のセキュリティ認証制度（JC-STAR 等）に、使用プログラミング言語のメモリ安全性を評価項目として追加すること。C/C++実装機器に比して Rust 実装機器の認証を優遇するインセンティブ設計が有効である。 三. 「巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会」の次期開催時には、OSS コミュニティにおける基盤ソフトウェア開発の実務者を委員に加えること。現行の構成では通信事業者・ISP・セキュリティベンダーが中心であり、脆弱性を「作る側」の言語設計・コンパイラ技術の知見が欠落している。 四. 意見書提出様式を Word から、マクロフリーの PDF またはプレーンテキストに変更すること。サイバーセキュリティを論じる政府機関がマクロ文書形式で意見を募ることの自己矛盾を解消されたい（.docx => PDF などの安全なツールの提供を国家レベルで促してほしい）。 <結論> IoT 機器のファームウェアが C/C++で書かれている限り、レジデンシャルプロキシ対策は永遠のモグラ叩きに終わる。総務省には、対症療法としての「啓発」「監視」に留まらず、メモリ安全言語の採用という根本的解決策を国家戦略として打ち出すことを強く求める。	
11	個人	提言全体	（御意見①） 「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	本提言案では、レジデンシャルプロキシ化した機器として動画

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			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、…（中略）…「レジデンシャルプロキシ」と呼ばれる。」 提言案では、レジプロの発生源を「IoT 機器に仕込まれた不正なプログラム」と定義づけています。しかし実際には、PC やスマートフォンにおいて以下のようなソフトウェア・SDK を介して出口ノード化されるケースが多発しています。 ・受動利益ソフトウェア（Honeygain 等）： ユーザーが余剰帯域を提供する対価として報酬を得るソフト。 ・アプリ内組み込み SDK（PacketSDK、BrightSDK 等）： アプリ開発者がマネタイズ目的で組み込むサードパーティ製 SDK。 これらはユーザーが（利用規約の細部を見落としのまま）自ら同意してインストールしているケースが多く、純粋な「マルウェア感染」とは異なるアプローチでレジプロのインフラが形成されています。 【提案】 IoT 機器の悪用だけでなく、PC やスマートフォン環境における「マネタイズ目的の SDK や受動利益ソフトウェアを通じた出口ノード化」も主要な発生源として明記すべきです。 （御意見②） 「1. 背景」「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…（中略）…④IoT 機器の製造はサプライチェーンが多層的であり、…（中略）…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。」 上記①～④で挙げられている理由は、すべて「IoT 機器のサプライチェーン」と「マルウェア感染」を前提と	ストリーミングデバイスを例示しておりますが、御指摘の PC、スマートフォン等によるレジデンシャルプロキシについても、今後、検討を進めてまいります。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			した分析にとどまっています。しかし、前述の SDK や受動利益ソフトの場合は、以下のような「IoT 機器とは異なるレイヤーでの複雑さ」が存在します。 ・ユーザーが形式上であれ規約に同意してインストールしているため、捜査機関や事業者が「不正アクセス」や「不正指令電磁的記録（マルウェア）」として取り締まる法的なハードルが高い。 ・正規のアプリストアの審査やアプリ開発者のマネタイズ構造が悪用されており、正規の利用と悪用の境界が極めて曖昧なエコシステムが形成されている。 【提案】 対策が容易ではない理由の列挙に、「⑤ PC やスマートフォンアプリにおいて、ユーザーの規約同意やアプリ開発者のマネタイズ目的を隠れ蓑にした SDK・ソフトウェアが流通しており、正規利用と悪用の境界が曖昧なエコシステムが存在すること」を追記すべきです。 （御意見③） 「3. 対策例（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」 調査のトピックが「不正なプログラム」「C2 サーバ」といった、IoT のマルウェア感染を前提とした言葉に偏っています。これでは、アプリストア等を通じて広範に流通している SDK やソフトウェア型レジプロの実態解明が漏れてしまう懸念があります。 【提案】 調査・分析の候補に、「正規を装うアプリ内 SDK や受動利益ソフトウェアの流通実態」および「それらを通じたレジプロ化の経緯とエコシステムの構造」を明確に追加し、IoT 機器以外からのアプローチも含めた包括的	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			な調査を行うよう修正すべきです。 (御意見④) 「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。」 「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。」 「2. 対策の基本的な考え方」(3 ページ目) 「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 (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」(3 ページ目 17 行目) 「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」 実際の IoT 機器や端末の感染事例を解析すると、レジプロ機能のプログラム単体で動作しているケースだけでなく、広告不正 (Ad Fraud) や暗号資産の発掘 (クリプトジャッキング) など、攻撃者が感染機器を多角的にマネタイズ (収益化) するための複数のモジュールが同時にインストール・実行されている実態が多々確認されています。 提言案および別紙 (p. 7-8) においては、正当業務行為を阻却する根拠として「DDoS 攻撃等が行われ、ISP の電気通信役務の提供に支障が生じること」を非常に重く位置付けています。しかし、「DDoS 攻撃や不正アクセスの踏み台 (レジプロ) に使われるから対策する」「プロバイダの通信障害を起こさない広告不正モジュール等は対象外とする」といった、攻撃の「機能・目的」に応じた限定的なアプローチでは、不当な利益を得ているサイバー犯罪者の収益モデル (エコシステム) 全体を断ち切ることはできません。 問題の本質は、「機器所有者の意図や認識とは無関係に、デバイスが乗っ取られ、金銭目的の不正なプログラムが勝手に動作させられていること」そのものにあります。	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			【提案】 1. 調査分析の対象拡大 3. (1)「実態の調査・分析」において、レジプロ機能の分析にとどまらず、同時に感染・実行される広告不正モジュール等を含めた「感染機器のマネタイズ構造全般」の実態解明を行うこと。 2. デバイス乗っ取り全般に対する包括的対策の推進 特定の手法や攻撃影響（DDoS 等）だけに着目した対症療法にとどまらず、金銭目的で所有者の意図に反して機器を操作・悪用する不正プログラム全般を検知・防除するための、より包括的かつ本質的なセキュリティ対策スキームとして制度設計および官民連携を進めること。	
12	個人	提言全体	本提言の公表および意見募集にあたり、スマートグラスをはじめとする先端的なウェアラブルデバイスやグローバルな次世代技術の普及・活用の観点、およびサイバー攻撃対策という名目の背後にあるリスクの観点から、以下の点において重大な懸念を抱き、強く意見を述べさせていただきます。 第一に、セキュリティ上の脅威や不正アクセスの対策という名目の下で、次々と新たな規制や管理的な枠組みを重ねるアプローチは、いわゆる「いたちごっこ」に終始し、実効性を伴わない形骸化した規制強化に陥る危険性が極めて高いという点です。こうした終わりなき対策や義務付けの強行は、かえって現場の事業者や利用者に過重なコストと対応の負担を転嫁するだけであり、技術の健全な発展を阻害するものと言わざるを得ません。 第二に、このような過剰なセキュリティ対策や国内独自の縛りは、スマートグラスや各種ウェアラブルデバイスなどのグローバルな最先端技術の潮流において、我が国を世界の国際標準やイノベーションの流れから決定的に乖離・遅れを取らせる要因になるという強い懸念です。国際的な競争力や利便性の向上を最優先すべきであり、国内の安全管理を口実にした過度な萎縮効果を生む制度設計は直ちに見直されるべきです。 第三に、サイバー攻撃対策やインフラの安全性確保といった大義名分の下で、個人情報の保護やプライバシーが軽視され、結果として国民の通信や行動に対する管理・監視の網が広げられることへの強い不安と拒絶です。行政や巨大事業者の都合による形骸化した管理強化ではなく、一般市民が世界基準の便利な先端デバ	御意見として承ります。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			イスを過度な負担やプライバシー侵害の不安なく享受できる、開かれた現実的な社会経済基盤の整備を強く求めます。	
13	一般社団法人 ICT-ISAC	1. 背景	【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。】 近年、マルウェア感染機器やレジデンシャルプロキシ等を悪用したサイバー攻撃が深刻化しており、利用者保護及び我が国のサイバーセキュリティ確保の観点から、官民が連携して感染機器対策を推進することは極めて重要であると考えます。	賛同の御意見として承ります。 引き続き、官民連携を図りながら検討を進めてまいります。
14	一般社団法人 ICT-ISAC	1. 背景	【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。】 特に利用者自身が感染や不正利用に気付いていないケースも多いことから、注意喚起や対処方法を含めた継続的な周知・広報活動は、本提言の実効性を確保する上で不可欠であり、関係機関・事業者が連携して積極的に取り組むことを期待します。	御指摘のとおり、利用者自身による適切な対策を促進するためには、継続的かつ分かりやすい周知啓発が重要であると考えています。 御意見については、今後の検討を進める上で参考とさせていただきます。
15	一般社団法人 ICT-ISAC	3. 対策例	【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】 通信事業者による対策の実施に当たっては、通信の秘密や利用者の権利・利益への十分な配慮が前提となります。制度・ガイドラインの整備に当たっては、通信の秘密との整合性を確保しつつ、事業者が安心して必要な対策を講じられるよう、法的・運用上の考え方を明確に示すことを要望します。また、利用者への通知	本提言案では、通信の秘密との関係を踏まえつつ、レジデンシャルプロキシによる被害への対応に必要と考えられる対策例を整理しています。 御意見については、今後の検討

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			については、通信事業者を騙る詐欺やフィッシング等に悪用・混同されないよう配慮するとともに、正当な通知であることを利用者が判別できる仕組みや周知を進めることで、通信事業者による注意喚起の信頼性と実効性を高めることが重要であると考えます。	を進める上で参考とさせていただきます。
16	一般社団法人 ICT-ISAC	3. 対策例	【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】 利用者への通知や通信の遮断等は被害拡大防止の観点から重要ですが、これらはあくまで対症療法です。サイバー空間全体の安全性向上のためには、最終的には感染機器からマルウェアを除去し脆弱性を解消する、またそれらができない機器については撤去を指導するとともに新たにネットワークに接続させないなど、感染機器そのものをネットワーク上から減らしていく根治的な対策まで見据えた取組を推進することが重要であると考えます。そのためには、通信事業者だけでなく、機器メーカー、セキュリティベンダ、販売事業者、行政等が連携し、感染機器の復旧・撤去までを視野に入れた継続的なエコシステムを構築することを期待します。	賛同の御意見として承ります。 御意見については、今後の検討を進める上で参考とさせていただきます。
17	Infoblox 株式会社	3. 対策例	【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】 Infoblox は、マルウェア、コマンド・アンド・コントロール（C2）サーバー、および機器がどのようにプロキシネットワークへ組み込まれるのかといった仕組みに関する調査を含め、レジデンシャルプロキシ活動の調査・分析を強化するという提案を強く支持します。 当社は、本項において、ドメイン名、インターネットインフラ指標、および関連する脅威インテリジェンスを、レジデンシャルプロキシネットワークを理解する上で重要な情報源として明示的に位置付けることを提言します。 レジデンシャルプロキシは、参加している機器がプロキシ管理システムを発見し通信できるようにするインフラに依存しています。このインフラには一般的に以下が含まれます。 ・プロキシ管理および制御システムに関連するドメイン名	御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			・レジデンシャルプロキシ事業者を支えるインターネットインフラ ・プロキシ機能を提供するソフトウェアの配布に使用される類似ドメインおよび関連インフラ ・悪性インターネットインフラに関する各種指標や脅威インテリジェンス（信頼できる関係者間で分析や防御目的のために共有可能なもの） インターネットインフラに関する情報は、レジデンシャルプロキシネットワークの特定および分析に有益です。多くの場合、特定の犯罪行為が個人に帰属されるよりも前の段階で不審なインフラを発見できるため、悪意ある活動を支える広範なネットワークの把握につながります。 これらの情報源を調査活動に組み込むことで、レジデンシャルプロキシインフラへの理解を深め、将来的な対策を支援するという本提案の目的をさらに強化できると考えます。	
18	Infoblox 株式会社	3. 対策例	【利用者への注意喚起】 Infoblox は、利用者の機器がレジデンシャルプロキシ活動に参加している可能性を示す証拠が確認された場合、当該利用者へ通知を行うという提案を支持します。 侵害された家庭用機器は、一般利用者自身が特定することが難しいケースが多いため、利用者の認識向上と是正措置は依然として重要です。 当社は、ネットワーク記録、IP アドレス割当記録、および ISP 加入者情報が、通知プロセスの正確性、迅速性、有効性の向上に役立つことを明確化するように提言します。 提案案では、被害組織、法執行機関、業界団体、NICT および ISP が連携して影響を受けた利用者を特定し、注意喚起を行う枠組みが示されています。 ネットワーク記録は、機器が既知の悪性インフラと通信しているかを確認するのに役立ち、ISP 加入者情報は通知対象となる適切な利用者の特定に活用できます。 その一方で、こうした情報は、適用されるプライバシー保護規定およびデータ最小化の原則に従って利用されるべきであることを強調すべきです。	賛同の御意見として承ります。 本提言案では、通信の秘密との関係を踏まえつつ、レジデンシャルプロキシによる被害への対応に必要と考えられる対策例を整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			目的は、悪用されている可能性の高い機器の利用者へ通知を行うことであり、サイバーセキュリティ目的に関係のない情報の不必要な収集や保存を避けることにあります。 適切に活用すれば、これらの情報は通知の信頼性を高め、誤検知を減らし、利用者および通信事業者双方にとってより良い結果をもたらします。	
19	Infoblox 株式会社	3. 対策例	【C2 サーバに係る FQDN 等を把握】 Infoblox は、レジデンシャルプロキシの活動を阻止するためには、利用者の機器だけでなく悪性インフラそのものを対象とした対策が必要であるという提案の考え方を強く支持します。 これは本提案の中でも特に重要な提言の一つであると考えています。 提案案では、C2 サーバーリストの整備や、ISP が DNS ベースの仕組みを用いて特定された悪性インフラとの通信を防止することが検討されています。当社はこのアプローチを支持します。 提案案でも指摘されているように、レジデンシャルプロキシを利用した攻撃は通常、参加機器と C2 システムとの通信に依存しています。この通信を遮断することで、当該機器がプロキシ活動に利用される能力を大幅に低減または排除できます。 特に DNS ベースのセキュリティ対策は、悪性インフラとの接続が確立される前の段階で機能するため、高い効果が期待できます。 そのため当社は、プロテクトティブ DNS を含む DNS ベースのセキュリティ対策や類似技術を、「3(3)」を実施するための合理的かつ均衡の取れた手段として明示的に位置付けることを提言します。法執行機関、NICT、その他信頼できる組織が悪性インフラを特定した場合、DNS ベースの制御は、そのインフラとの通信を防止する効率的かつ拡張性の高い手段となり得ます。 こうした対策は、対象を限定し、証拠に基づき、適切な監督の下で実施されるべきです。また、犯罪捜査、利用者通知、機器の復旧対応、国際連携を代替するものではなく、それらを補完するものとして位置付けるべきです。	賛同の御意見として承ります。 今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
20	KDDI 株式会社	3. 対策例	今回取り纏めていただいた提言は、昨今のサイバーセキュリティ上の脅威として取り扱われるレジデンシャルプロキシへの具体的な対策例をご提示いただいたと認識しております。 また、各種対策における通信の秘密との関係について整理がなされたことは、今後の官民連携による取り組みの実効性が高まると考えております。 提示された対策例における注意喚起では、事業者による対象利用者の特定や、個別の注意喚起の実施といった実務が想定されていると認識しております。本取り組みを実効的かつ継続的なものとするため、注意喚起の内容に優先度をつけていただくなど、事業者に対して実務（運用・コスト面等）での過度な負担が生じないよう、ご配慮をいただきますようお願いいたします。	提言案にも記載のとおり、利用者への注意喚起の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ことが重要であると考えています。 御意見については、今後の検討を進める上で参考とさせていただきます。
21	AppLogic Networks Japan 株式会社	3. 対策例	提言案の調査・分析候補例においては、レジデンシャルプロキシ(以下 RESIP)が動作する端末と RESIP が通信を行う C2 サーバの実態調査として妥当と考える。一方、RESIP が実ネットワークにおいてどのように通信を行い被害を引き起こしているのか実態の調査が必要と考えられる。 (2) の対応に至るには RESIP を経由した不正アクセス通信と RESIP 端末の利用者を特定する通信証跡が必要となるが、両通信の相関性を分析するには実ネットワークでの通信分析が有効である。海外でのサイバーセキュリティ対策においても実通信の相関性分析が導入されている。RESIP の複雑・巧妙な仕組みから実態解明、実対策に至るまでの情報取得が迅速、かつ効率的に実施できることが必要になるが、被害者からの申告、各関係者が持つ情報の収集・突合・分析には相当な時間を要すると想定される。サイバーセキュリティ対策においては被害の拡大防止、被害者保護の観点から迅速な対応を行えることが重要となる。特に RESIP の利用情報の特定から RESIP 上の通信の相関性を分析、蓄積しておくことは、対策に至るまでの実態調査の加速、効率化において効果を期待できる。 対策として実ネットワークでの通信分析を実施することは、各関係者（被害者、当事者、調査関係者・機関等）の人的、時間的負担を低減し、本提言の対策を迅速化することに効果的であると考えます。 上記から調査・分析の実施項目として実ネットワークでの通信分析の実施を提案するものである。	御指摘の事項については、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に関する調査・分析を進める上で、参考とさせていただきます。
22	NTT ドコモビジネス株	3. 対策例	当社は、ISP としてのネットワーク運用の知見及びセキュリティサービス提供事業者としての脅威分析・対応	賛同の御意見として承ります。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
	株式会社		に関する知見を活用し、本提言に基づく取組に協力してまいりたいと考えております。一方、レジデンシャルプロキシ対策は、継続的な官民連携及び関係事業者間の情報共有が重要であることから、今後も連携体制の強化をお願いしたいと考えます。	引き続き、官民連携及び関係事業者間の連携を図りながら検討を進めてまいります。
23	NTT ドコモビジネス株式会社	3. 対策例	本提言の実効性を高めるためには、利用者自身による適切な対策が不可欠であると考えます。一方で、提言でも指摘されているとおり、利用者は自身の IoT 機器がレジデンシャルプロキシとして悪用されていることに気付きにくい構造にあります。また、今後は AI 家電等の普及により、こうしたリスクの増大が懸念され、国民の安心・安全な生活への影響も懸念されます。 このため、国や関係団体等において、レジデンシャルプロキシの危険性、IoT 機器のセキュリティアップデートの重要性、ISP 等からの注意喚起の意義等について、継続的かつ分かりやすい広報啓発を実施いただきますようお願いいたします。本課題の解決に向けては、継続的な周知啓発及び注意喚起が極めて重要であるとともに、利用者の認知向上は、本提言に基づく各種施策の受容性及び実効性向上にも資するものと考えます。	御指摘のとおり、利用者自身による適切な対策を促進するためには、継続的かつ分かりやすい周知啓発が重要であると考えています。 御意見については、今後の検討を進める上で参考とさせていただきます。
24	個人	3. 対策例	本件は、家庭用 IoT 機器が不正なプログラムによりレジデンシャルプロキシ化され、不正アクセス、不正送金、サイバー攻撃の踏み台として悪用される問題について、関係主体が連携して対策を進めるための提言案であると理解しています。 家庭用 IoT 機器は、利用者が十分に管理状況を把握しにくく、脆弱性や不正プログラムの存在に気付きにくいという特徴があります。そのため、利用者本人の注意喚起だけに依存する対策には限界があり、ISP、通信事業者、NICT、警察、機器メーカー、販売事業者、セキュリティ事業者等が連携した多層的な対策が重要だと考えます。 本提言案では、不正アクセスの発信元に係る IP アドレス、ポート番号、タイムスタンプ等を用いた注意喚起や、C2 サーバに係る情報共有、DNS による通信遮断等が示されています。これらは重要な対策ですが、同時に、被害者情報、利用者情報、ログ、通信関連情報、機器識別情報等の取扱いにも十分な配慮が必要です。 レジデンシャルプロキシ対策では、不正通信を止めることに加え、調査・分析・注意喚起・情報共有の過程で扱われる情報が漏えいした場合の被害を最小化する観点も重要です。特に、IP アドレス、ポート番号、タイ	本提言案では、レジデンシャルプロキシによる被害への対応に当たり、関係主体が連携して取り組む対策例を整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			ムスタンプ、契約者情報、機器情報、ログ等が組み合わせられると、個人や家庭の通信環境、利用状況、被害状況を推測し得る場合があります。 また、家庭用 IoT 機器が踏み台化される問題は、端末側に重要情報や認証情報、設定情報が不用意に保存されている場合のリスクも示しています。今後は、IoT 機器そのものについても、認証情報、設定情報、ログ、利用者情報等が外部に流出しても、単体では復元・悪用されにくい設計を促すことが重要だと考えます。 さらに、家庭用 IoT 機器や通信環境の安全対策では、利用者に注意喚起を行い、設定変更やアップデート、不要アプリの削除、パスワード変更等を求めることが重要である一方、利用者が常に正しく対応できるとは限りません。企業や自治体の情報システム部門がルールを定めても現場で完全には守られない場合があるのと同様に、一般家庭においても、セキュリティ対策を利用者の判断や注意だけに委ねることには限界があります。 そのため、家庭用 IoT 機器や通信サービスにおいても、「利用者が自分で正しく守る」ことを前提にするだけでなく、通常どおり使っているだけで危険な設定や不正な通信が抑止され、認証情報・設定情報・ログ等が過度に平文で残らず、万一流出しても単体では悪用されにくい設計を重視すべきです。これは、利用者任せにしない安全対策として重要だと考えます。 同時に、レジデンシャルプロキシを経由した攻撃を受ける企業・金融機関・行政機関側でも、侵入防止や検知だけでなく、侵害を受けた場合に重要データが単体では復元・悪用されにくい状態で保護されていることが重要です。従業員が暗号化対象や鍵管理を都度判断する運用ではなく、通常どおり保存するだけでシステム側が自動的にデータを分散・無意味化する仕組みは、被害組織側の対策としても有効だと考えます。 つきましては、本提言案及び今後の具体的対策において、以下の観点を検討対象に含めることを要望します。 1. レジデンシャルプロキシ対策に伴い関係主体間で共有される IP アドレス、ポート番号、タイムスタンプ、機器情報、利用者情報、被害申告情報、ログ等について、必要最小限の利用、目的外利用の防止、保存期間の限定、アクセス制御、暗号化に加え、流出時の被害最小化を重視すること。	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			2. 調査・分析・注意喚起・情報共有の過程で扱われる情報について、流出したデータ単体では意味を持たず、復元・悪用されにくい状態にする「データ無意味化」「秘密分散」「分散保管」等の技術的対策を、選択肢として検討すること。 3. 家庭用 IoT 機器の設計・流通・運用において、認証情報、設定情報、ログ、利用者情報等が機器内又はクラウド上に保存される場合には、端末紛失、乗っ取り、クラウド流出、委託先流出を想定した保護設計を促すこと。 4. 利用者への注意喚起だけに依存するのではなく、機器メーカー、販売事業者、通信事業者、セキュリティ事業者が、初期設定、アップデート、認証情報保護、不要な通信の抑止、ログ保護を含めた多層的な対策を進めること。 5. 一般利用者が高度なセキュリティ判断を常に行うことを前提にせず、通常どおり利用しているだけで安全な状態に近づく設計、すなわち利用者任せにしない安全対策を重視すること。 6. レジデンシャルプロキシ化された機器を経由した攻撃を受ける被害組織側においても、侵入防止・検知だけでなく、万一侵害された場合に重要データが単体で復元・悪用されにくい状態となるよう、データ無意味化、秘密分散、分散保管等の対策を検討すること。 7. 被害組織の従業員が暗号化対象や鍵管理を都度判断する運用に依存するのではなく、通常どおり保存するだけでシステム側が自動的にデータを分散・無意味化し、保護する仕組みも選択肢として検討すること。 特定の企業や製品の採用を求めるものではありません。秘密分散、データ無意味化、分散保管といった技術カテゴリを、家庭用 IoT 機器、通信事業者、被害組織、関係機関の間で扱われる情報を守るための選択肢として検討していただきたいという趣旨です。 レジデンシャルプロキシ対策は、不正通信を止める対策であると同時に、家庭・通信事業者・被害組織・関係機関をまたいだ情報管理の問題でもあると考えます。本提言案においても、「不正利用を防ぐ」だけでなく、「対策の過程で扱われる情報や、被害組織の重要データが漏えいした場合の被害を最小化する」観点を反映	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			していただくことを要望します。	
25	個人	3. 対策例	「その他の対策」に関し、ネットワーク（例：ISP）側だけでなく、可能な限り情報空間全体におけるインフォメーション・ヘルス（情報的健康）の確保のため、ユーザ装置側からもモニタリング（監視／遠隔解析）可能な仕組みの追加が重要と考えます。 そのため世界に先駆けるようなユーザ装置側からも監視／遠隔解析が可能なシステム実現に向けては、下記のような既に公開されている考え方も参考にして、例えば政府機関や行政機関等、先ずは信頼できる機関でプライバシー侵害の恐れのない箇所を優先／選定しながら、モニタリング装置を配布（例：私物化できないようレンタル）して複数個所でモニタリングしていくような、新たな（物理レベルだけでなく通信制御も含めた）インフラを速やかに検討／実現し全国展開していく方が良いと考えます。 上記取り組みで、将来的には技術戦略上重要な企業からの要望も受けながら、民間企業等へも展開し情報空間全体のセキュリティ強化を図っていくことが重要と考えます。 ===（参考）既に公開されている考え方===== 特開 2007-28576 (P2007-28576A) https://www.j-platpat.inpit.go.jp/c1801/PU/JP-2007-028576/11/ja ===（参考）ブロードバンドルータなどのネットワーク装置の遠隔監視や遠隔制御の活用技術例=== 特開 2007-28576 (P2007-28576A)（2007/2/1）より抜粋 （3）本発明による有利な効果 【課題】 インターネットなどの通信ネットワークと別個の通信ネットワークを用いることなく、ブロードバンドルータなどのネットワーク装置の遠隔監視や遠隔制御をさらに確実に実行することができるネットワーク装置管理アダプタを提供する。 【0016】 本発明の第5の特徴は、本発明の第3または第4の特徴に係り、前記稼動問合せの送信時刻、及び前記稼	御意見として承ります。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			動問合せに対する前記ネットワーク装置からの応答の受信時刻を含むネットワーク装置稼動状況を記録する稼動状況記録部（情報記録部１７０）をさらに備え、前記中継通信制御部は、前記第１送受信部を経由して、前記稼動状況記録部に記録されている前記ネットワーク装置稼動状況を前記通信ネットワークに向けて送信することを要旨とする。 【００１７】 本発明の第６の特徴は、本発明の第１乃至第５の特徴に係り、前記第１送受信部及び前記第２送受信部を経由せずに、前記通信ネットワークと前記ネットワーク側ポートとを直結するバイパス部（バイパス部１１５）をさらに備え、前記中継通信制御部は、前記送受信情報の内容の監視が必要な場合のみ、前記第１送受信部及び前記第２送受信部を経由するように前記バイパス部を制御することを要旨とする。 【００１９】 本発明の第８の特徴は、本発明の第１の特徴に係り、前記ネットワーク装置の端末側ポート（端末側ポート３０Ｄ）と接続される第３送受信部（第３送受信部１３１）と、前記第２送受信部及び前記第３送受信部を経由して試験用データを送信し、前記ネットワーク装置の稼動状態を取得する状態取得部（自動解析部１９１及び遠隔解析部１９２）とをさらに備え、前記中継通信制御部は、前記状態取得部が取得した前記稼動状態を、前記通信ネットワークに向けて送信することを要旨とする。	
26	個人	2. 対策例	（意見の趣旨） 本提言（案）に示された官民連携によるサイバー攻撃対策の必要性には一定の理解を示すものの、対策の推進にあたって行政機関の権限拡大や民間事業者（ISP 等）への過度な義務付けによる「実質的な国民負担増（隠れ増税、コスト転嫁）」および「通信の自由、経済活動の阻害」につながる施策には慎重であるべきです。 新制度や監視スキーム構築による公的資金（税金）の過度な投入を抑え、既存予算、組織の効率的な再配分によって対応すること、また民間への過剰なコスト負担要請（巡り巡って利用料金の値上げという国民負担増につながるもの）を避けることを強く求めます。	本提言案では、通信の秘密との関係を踏まえつつ、レジデンシャルプロキシによる被害への対応に必要なと考えられる対策例を整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			(具体的理由) 1. 新たな税金、公的資金投入の抑制（行政膨張、隠れ増税への反対） 提言案ではNICTや警察庁、関係機関による新たな調査、分析、情報共有スキーム（第3章（1）から（4））が示されています。しかし、これらを理由とした安易な省庁予算の増額や新たな補助金、天下り団体の創設（いわゆる「サイバーセキュリティ権益」による税金の無駄遣い）は断じて認められません。 セキュリティ対策は、既存の警察予算、総務省・NICTの既存デジタル関連予算の徹底した効率化・優先順位の見直しによって賄うべきであり、国民の税負担を増やす形での対策拡大には反対します。 2. 民間事業者への過度な負担要請による「隠れコスト転嫁」の防止 ISP（電気通信事業者）等に対する注意喚起（3（2））やDNSブロッキング、名前解決遮断（3（3））の対応要請は、事業者側にシステム改修やログ運用管理などの膨大な実務・コスト負担を生じさせます。 民間事業者への法的、事実上の義務付けが過度になれば、そのコストは最終的に通信料金の値上げやサービスの質の低下として国民（消費者）に転嫁されます（実質的な負担増）。事業者の自主的な取り組みを尊重し、不要な事務負担やシステム投資を強いる規制、指導とならないよう配慮が必要です。 3. 「通信の秘密」の保護と市場のイノベーション阻害リスク （別紙）にて整理されている「通信の秘密」に関する正当業務行為やオプトアウト付き包括同意の適用拡大については、行政や通信事業者による個人の通信監視、アクセス制限の「便宜的な正当化」に利用される懸念があります。 法的な解釈を拡大解釈して安易に通信ログの照合や遮断を行うことは、憲法で保障された「通信の秘密」や個人のプライバシーを脅かすだけでなく、通信関連市場の自由な経済活動を冷え込ませる恐れがあります。 国民の権利侵害や市場の自由度を削ぐような過剰な規制、関与は厳に慎むべきです。 4. メーカー、ユーザーへの市場原理に基づく対策の促し レジデンシャルプロキシ化の根本原因は、脆弱なIoT機器の流通やID、パスワードの管理不備にあります。 これらに対しては、政府が過度な介入や法規制を行うのではなく、市場競争の中でセキュリティに優れた機	

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			器が選ばれる仕組みや、製品スペックの透明化、ユーザーへの自己責任に基づく適切な周知（コストをかけない広報啓発）といった、民間主導、市場原理に基づいたアプローチを優先すべきです。 （まとめ） サイバー空間の安全性確保は重要ですが、「セキュリティ」を大義名分とした[「税金の無駄遣い」「民間負担増を通じた実質的な国民負担（通信料等）の上昇」「官の権限拡大」]は固く防止すべきです。既存リソースの範囲内かつ市場経済の自由を損なわない形での対策運用を強く要望いたします。	
27	個人	3. 対策例	「3. 対策例（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」（6 ページ目 2～3 行目） 「3. 対策例（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」（6 ページ目 5～6 行目） 「別紙 1. 3(2)の対策について」（7～8 ページ目） 提言案ではプロバイダ側の通信抑止やマルウェア感染対策などの「技術的アプローチ」に主眼が置かれていますが、「受動利益ソフトウェア」や「マネタイズ用 SDK」によって構成されるレジデンシャルプロキシに対しては、「事業者への法規制」と「利用者への法的リスク周知」という行政・法的なアプローチを検討する必要があります。 1. 提供事業者に対するアプローチ（電気通信事業法上の整理） ユーザーの端末を中継ノードとし、第三者の通信をルーティングして利益を得るビジネスモデルは、実質的に「業として他人の通信を媒介する」行為に他なりません。これらを提供する企業（海外事業者含む）に対し、電気通信事業法における登録・届出の有無や適法性を問い、監督省庁として指導や国内での流通規制等の措置を講じるべきです。 2. 利用者（ユーザー）側に対する法的整理とリスク周知	御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			ユーザーは「手軽な小遣い稼ぎ」感覚で帯域を提供していますが、この行為は以下の重大な法的・契約的リスクを孕んでいます。 ・ISP 利用規約違反リスク： 契約回線を第三者に提供・中継させる行為は多くの一般向け ISP 規約で禁止されており、回線の強制解約等の対象となります。 ・犯罪加担（幫助）リスク： 自宅回線が不正アクセスや DDoS 攻撃に悪用された場合、対価を得てインフラを提供していた以上、単なる「被害者」ではなく、サイバー犯罪のインフラ提供者（加担者・幫助）として法的責任を問われるリスクが生じます。 （補足） なお、提言案の別紙（p.7）では「知らないうちにマルウェアに感染したボット被害者」を前提として通信の秘密侵害に係る違法性阻却（正当業務行為）を組み立てています。しかし、ユーザーが自ら導入するソフトや SDK の場合、この「被害者前提のロジック」が適用できなくなる懸念があります。この点からも、従来のマルウェア対策の枠組みだけに依存せず、上記のような「事業者規制」と「利用者の法的リスク整理」を新たな柱として明確に組み込む必要があります。 【提案】 1. 対策(4)関連： 3. (4)のステークホルダー連携において、「業として通信を媒介するソフトウェア」の提供事業者に対し、電気通信事業法等の法令に基づく適法性整理を行い、監督省庁としての指導や流通規制を検討・実施項目に加えること。 2. 対策(5)関連： 3. (5)の国民への広報啓発において、受動的なマルウェア対策にとどまらず、小遣い稼ぎ目的で帯域を提供する行為が「ISP 規約違反（強制解約）」や「犯罪加担（幫助）」に直結するという重大な法的リスクを明確に整理し、強く国民に警告・問題提起する内容を盛り込むこと。	
28	個人	3. 対策例	「1. 背景」 「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…（中略）…ユーザーへの通知を行っている旨を公表している。」	本提言案では、通信の秘密との関係を踏まえつつ、レジデンシャルプロキシによる被害への対

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			「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」(5～8 ページ目) 海外においては、実効性のある対策を行うには、ISP やセキュリティ機関同士がレジデンシャルプロキシ（以下、レジプロ）に係る通信の特徴を能動的に分析・検知し、事業者間で迅速に情報共有を行うことが必要であると言われています。 しかし、日本国内においては、電気通信事業法上の「通信の秘密」の保護規定に対する過度な懸念や法的整理の不透明さから、プロバイダ等の通信事業者が自社網内の通信実態を能動的に分析することすら躊躇せざるを得ない現状があります。提言案の別紙では「警察等から特定された IP アドレス等の照合」における正当業務行為等の整理がなされていますが、その前段階である「実態把握や異常通信の能動的な検知・分析・事業者間共有」における法的裏付けやガイドラインが不足しているため、事業者が実態を確認できず、手出しができない構造になっています。 【提案】 海外の先進事例を参考に官民連携を進めるのであれば、単に警察からの共有に基づく照合手続き（別紙）を整理するだけでなく、「ISP 等がレジプロ対策を目的として通信パターン等を能動的に分析・検知・事業者間共有すること」について、通信の秘密との関係を明確に整理したガイドライン等を策定し、事業者が安心して実態確認と即応的対策を行える環境を整備することを提言します。	応に必要と考えられる対策例を整理しています。 御指摘の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・分析に関する事項については、今後の検討を進める上で参考とさせていただきます。
29	個人	3. 対策例	「3. 対策例 (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」(3 ページ目 21～22 行目、4 ページ目 1～11 行目) 対策(2)では「被害申告」を起点とし、捜査過程で把握した IP アドレス等を通信業界団体（ICIT-ISAC 等）や ISP へ共有して利用者を特定・注意喚起するフローが提案されています。しかし、このフローには以下の実質的な機能不全リスクが存在します。	本提言案では、家庭用 IoT 機器を悪用するレジデンシャルプロキシへの対策を取りまとめており、利用者への注意喚起についても対策例として整理しています。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			1. タイムラグとログ保持限界 被害の発生から申告、警察の捜査・IP 特定、さらに ISAC や ISP を経由した利用者特定に至るまでには膨大な時間を要します。その間に ISP 側の通信ログ保存期間が切れるか、あるいは攻撃者がすでに別の IP へ移行している可能性が高いです。 2. 捜査情報の壁と CGNAT による特定困難性 警察が把握した IP アドレス等は刑事捜査情報に該当するため、円滑な外部共有には法制度・運用の面で大きなハードルがあります。また、キャリアグレード NAT (CGNAT) 環境下では、IP アドレス・ポート番号・正確なタイムスタンプ (秒単位) の組み合わせが完璧に揃わなければ発信者を特定できず、注意喚起に至らない事例が頻発することが予想されます。 3. 被害者側へのアクション支援の欠如 被害者側から見れば、単に「発信元へ注意喚起が行われる」だけでは被害の回復や根本的な解決に至りません。 【提案】 1. 被害申告を待つ受動的なスキームだけに依存せず、より迅速・能動的に発信者を特定できるルートを別ラインで確保すること。 2. 不正アクセスの被害者が、レジプロのノードを提供した側 (あるいは不当な利益を得てノード化を許容した者) に対し、プロキシ機能の提供・放置に対する損害賠償請求等の適切な民事上の措置を取れるよう、発信者情報開示手続きの円滑化や法的整理等の支援策を盛り込むこと。	御指摘の利用者特定や注意喚起の実効性向上に関する事項については、今後の検討を進める上で参考とさせていただきます。
30	個人	3. 対策例	「3. 対策例 (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」(3 ページ目 21~22 行目) 「3. 対策例 (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」(4 ページ目 5~6 行目)	御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			「別紙 1. 3(2)の対策について（注 12）」（7 ページ目） 提言案の別紙注 12（7 ページ）において『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』と明記されている通り、レジプロ網の多くは商業的に販売されており、脅威インテリジェンスの活用やサービス利用（クローリング）を通じて中継ノードとなっている IP アドレス群を能動的かつ容易に事前収集できる性質を持っています。 自らプロキシ IP 群を入手可能であると認識しているにもかかわらず、本対策案（対策(2)）が「被害が発生し、申告されてから IP アドレスを照合する」という極めて受動的なプロセスにとどまっている点には大きな疑問があります。これでは後手に回り、被害の拡大を防ぐことができません。 また、端末がレジプロ化している利用者への通知についても、単なるマイルドな「お知らせ（注意喚起）」レベルでは無視されるか、深刻度が伝わらない恐れがあります。 【提案】 1. 能動的収集に基づく早期対処の主軸化 別紙注 12 で示されている通り、被害申告を待つことなく、市場に出回るレジプロサービス等から能動的にプロキシ IP リストを収集・購入し、NICT や ICT-ISAQ 等を通じて該当プロバイダへ提供することで、被害が発生する前に利用者特定と対策を行う「能動的アプローチ」を対策の主力に据えること。 2. 強い警告（法的・契約的リスクの明示）の実施 レジプロ化している利用者に対する通知は、単なるソフトな注意喚起にとどめず、「自身の端末がサイバー犯罪の踏み台として悪用されていること」「放置した場合、ISP の利用規約違反による回線停止や、犯罪加担（幫助）・損害賠償請求等の法的リスクに直面する可能性があること」等を明確に示した「強い警告」として実施すること。	
31	個人	3. 対策例	「1. 背景」（1 ページ目 27～28 行目） 「また、2026 年 1 月には、米 Google が、世界最大級のレジデンシ	本提言案では、レジデンシャル

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			ヤ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。」 「3. 対策例 (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」(4 ページ目 13～29 行目) 「③ ISP は、提供されたリストに基づき、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 サーバの FQDN の名前解決要求に係る通信を遮断する。」 「別紙 2. 3(3)の対策について」(9 ページ目) 対策(3)では、別紙2に示される過去の整理(第二次とりまとめ)に基づき、警察やNICT等が把握したC2サーバのFQDNリストを用いて、ISPの自社DNSサーバにおいて名前解決要求を遮断する(FQDNブロッキング)手法が提案されています。しかし、現代のレジプロインフラの運用実態を鑑みると、このアプローチは技術的に十分な効果を生まない可能性が高いと考えます。 1. ドメインの大量生成・頻繁変更への追従限界 サイバー攻撃者は、DGA(ドメイン生成アルゴリズム)やFast Flux技術等を活用し、数百から数千に及ぶドメインを短期間で頻繁に変更します。手作業や周期的リスト共有によるDNSブロッキングでは、ドメイン追加・変更のスピードに追従できません。 2. DNSを経由しない通信形態への無効性 C2通信がIPアドレスを直に指定して行われる場合や、端末側がDoH(DNS over HTTPS)等の暗号化DNSを利用してプロバイダ以外の外部DNSを参照している場合、ISPの自社DNSにおけるFQDN遮断では通信の確立を防ぐことができません。 本文1ページ目において、米Googleが世界最大級のレジプロネットワーク(IPMoyu、IPIdeas、NetNuts等)を停止させた成果が引用されていますが、同作戦において実施されたのは単なるプロバイダのDNSブロックではなく、法的手続きやクラウド・ホスティング事業者と連携したC2インフラそのものの直接停止(IPアドレス・BGP/ASレベルでの通信制限やサーバーの強制停止・解体)です。 【提案】	プロキシによる被害への対応に当たり、関係主体が連携して取り組む対策例を整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			1. IP アドレス帯/BGP レベルでの能動的通信制限の検討 対策(3)の手法をFQDN(ドメイン名)単位の名前解決遮断だけに限定せず、悪用されているC2サーバが集中して設置されている「IP アドレス」「IP アドレス帯(CIDR ブロック)」「自律システム(AS/BGP レベル)」を対象とした大規模かつ機動的な通信制限・遮断スキームについて、法的・技術的整理を行い検討項目に加えること。 2. Google 等の先行事例にならった構造的テイクダウン(インフラ解体)作戦の導入 単にプロバイダヘリストを配って水際で止めさせる受動的なDNS ブロック(二次とりまとめの手法)にとどまらず、提言本文で引用されているGoogle等によるテイクダウン事例を参考に、警察庁・総務省・NICT・大手インフラ事業者・海外当局等が連携し、悪質なレジプロ事業者のC2インフラ自体を根本から停止・解体させる「構造的テイクダウン作戦」を日本の対策の柱として明確に位置付けること。	
32	個人	3. 対策例	「1. 背景」(1 ページ目 5～7 行目) 「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。」 「3. 対策例 (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」 提言案の背景(1 ページ目)でも言及されている「家庭用動画ストリーミングデバイス」の多くは、実態として「違法な動画コンテンツ等を無料で閲覧できる」ことを売りに販売・流通している不正なストリーミング端末(STB 等)です。ユーザーは違法視聴目的で購入・設置していますが、これらの機器には製造・流通段階から最初からレジデンシャルプロキシ(以下、レジプロ)化させる不正プログラム(バックドア等)が組み込まれており、サイバー攻撃インフラの温床となっています。 現状の対策における大きな課題は、以下の通りです。 1. 利用・所持に対する法的規制の欠如 こうした不正機器について、警察が捜査の過程で個別に押収する以外の手段がなく、「利用すること自体」「所	本提言案では、家庭用IoT 機器を悪用するレジデンシャルプロキシへの対策を取りまとめており、機器流通の抑止その他の対策についても対策例として整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			持すること自体」に対する強力な法的禁止規定や没収・回収の仕組みがないため、ユーザーの手元に端末が残り続け、レジプロとしての稼働を止められません。 2. サプライチェーン（流通経路）での規制不十分 国内の悪質販売事業者だけでなく、海外の越境 EC サイトや大手 EC モール等を通じて容易に輸入・購入できる状態が放置されているため、利用者の根絶に至っていません。 単に感染後の注意喚起や個別押収にとどまる対症療法では、次々と輸入される不正端末の増加に追いつかず、根本的な解決になりません。 【提案】 1. 水際・流通規制の徹底（対策(4)関連） 不正ストリーミング端末等を国内で販売・流通させる事業者に対する摘発・厳罰化を進めるとともに、越境 EC プラットフォームや大手 EC モール事業者と連携し、該当機器の出品禁止、輸入・関税段階での差し止めなど、国内市場へ流入させない総合的な水際対策を実施項目に明記すること。 2. 利用・所持の違法化および没収・回収スキームの検討 サイバー攻撃インフラ化している不正ストリーミング端末等について、個別の事件捜査を待たずとも、利用・所持自体を禁止（違法化）し、行政的・司法的手続きにより迅速に回収・没収してネットワークから排除できる法的枠組みの整備を検討すること。	
33	個人	3. 対策例	レジデンシャルプロキシ化した可能性のある端末の利用者への注意喚起については、技術的に正確であるだけでなく、一般家庭の利用者が実際に内容を理解し、疑わず、対応できる形にすることが重要と考えます。 通知を受けた利用者が、「内容が分かりにくい」「対応が面倒」「平日昼間に問い合わせる時間がない」「本当に国や関係機関からの正規の通知なのか分からない」と感じた場合、報告や対処を行わず、結果として対策の実効性が下がるおそれがあります。	御意見については、今後の検討を進める上で参考とさせていただきます。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			そのため、注意喚起は、国や関係機関からの一方的な連絡としてだけでなく、利用者が契約している通信事業者、すなわち ISP 等の公式な契約者向け通知枠組みと連携して行うことを検討してください。例えば、通信事業者の会員ページ、公式アプリ、請求書同封、郵送、正規窓口での確認手段等を活用し、利用者が詐欺メールや偽通知と区別できるようにすることが望ましいと考えます。 また、通知には、注意喚起が利用者による不正行為の認定ではないこと、通知の根拠、確認すべき機器、利用者が行う具体的手順、正規の問い合わせ先を分かりやすく記載してください。高齢者やデジタル機器の設定に不慣れな利用者でも対応できるよう、メールだけでなく、電話、郵送、休日・夜間対応、通信事業者の窓口、販売店、機器メーカー等への接続を含む支援手段を検討することが望ましいと考えます。	
34	個人	3. 対策例	C2 サーバリストに基づく DNS 遮断及び、IP アドレス、ポート番号、タイムスタンプ等の情報共有については、通信の秘密やプライバシーにも関係するため、誤通知や誤遮断が生じた場合に利用者が回復を求められる手続を、あらかじめ整備することが重要と考えます。 利用者にとって、通信遮断や注意喚起の理由、問い合わせ先、解除条件が分からない場合、「面倒」「分からない」「どこへ言えばよいかわからない」と受け止められ、対応や申出を諦めるおそれがあります。 そのため、C2 サーバリストについては、攻撃者に悪用され得る内容を公開する必要はありませんが、登録、更新、有効期限、失効、誤登録時の訂正、緊急解除、解除判断を行う主体を運用上明確にしてください。 また、共有される通信関連情報についても、利用目的、保存期間、共有範囲、目的達成後の削除、目的外利用の防止を明確にし、ISP、警察、NICT、ICT-ISAC、機器メーカー等の責任分界を整理することが望ましいと考えます。	本提言案では、通信の秘密との関係を踏まえつつ、レジデンシャルプロキシによる被害への対応に必要と考えられる対策例を整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。
35	Infoblox 株式会社	別紙	【通信の秘密との関係についての整理】 当社は、適切なガバナンスの下で実施されるサイバーセキュリティ対策は、プライバシーや通信の秘密の原則と整合性を保ちながらサイバーセキュリティ目標の達成に貢献できることを明確化しよう提言します。	本提言案では、通信の秘密との関係を踏まえつつ、レジデンシャルプロキシによる被害への対応に必要と考えられる対策例を

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			DNS ベースの多くのセキュリティ対策は、通信内容そのものを監視するのではなく既知の悪性インフラとの通信を識別または遮断することに重点を置いています。具体的には、個々の通信と結びつく情報（IP アドレス、送信元、時刻など）ではなく、送信先のドメイン情報のみを良性悪性判断の材料としています。 検証済みの悪性ドメイン、信頼できる脅威インテリジェンス、透明性の高いガバナンス、および説明責任の仕組みに基づくリスクベースのアプローチは、より侵襲的な監視を必要とすることなく、実質的なセキュリティ効果を提供できます。 これは、利用者の通信内容を調査することではなく、悪性 C2 インフラとの通信を防止することが目的となるレジデンシャルプロキシ対策において、特に重要な考え方です。 当社は、総務省が今後も、対象を限定し、均衡性があり、透明性と監査可能性を備えた対策を重視することを提言します。このようなアプローチは、通信ネットワークに対する信頼を維持しつつ、レジデンシャルプロキシの悪用に対する効果的な対策を可能にし、通信の秘密を保護することにつながります。	整理しています。 御意見については、今後の検討を進める上で参考とさせていただきます。
36	NTT ドコモビジネス株式会社	別紙	本提言に基づく取組を推進するに当たり、利用者保護及びサイバーセキュリティ向上とともに、通信の秘密及び利用者プライバシーへの十分な配慮が重要であると考えます。提言では、利用者への注意喚起及び DNS を活用した中継抑止措置について、既存の研究会の整理を踏まえた法的考え方が示されておりますが、これらの施策を社会全体に普及させていくためには、通信の秘密保護との関係について利用者や社会の理解を深めることも重要であると考えます。今後の制度運用やガイドライン整備に当たっては、通信の秘密の保護とサイバーセキュリティ確保との両立が図られるよう、解釈の明確化及び周知を継続いただくとともに、国による丁寧な説明及び広報をお願いいたします。	御意見については、今後の検討を進める上で参考とさせていただきます。
37	個人	別紙	3(2)の対策について、このような注意喚起を受けた利用者は、以後違法行為の幫助の故意が生じ得ることとなり、刑事責任や民事責任の追及を受けるおそれが生ずるという重大な不利益を受ける。 したがって、このような重大な不利益について検討しないまま手段の相当性があるとするのは、疑問である。	御意見として承ります。
38	個人	別紙	手段の相当性について	「ISP が検知する行為」の意味

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			「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」だけでなく、そもそも、ISP が検知する行為自体は全ての利用者の通信先を確認する必要があり、通信内容を他者に知られない憲法上の通信の秘密及びプライバシーの侵害になる恐れがある。 また、令状なく、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るだけで、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する行為は違法性阻却事由とはいえない。	するところが必ずしも明らかではありませんが、「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」については、①目的の正当性、②行為の必要性、③手段の相当性が認められる行為であることから、正当業務行為としてその違法性が阻却されると整理したものです。 また、本対策は、警察庁又は都道府県警察から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の提供を受けたことのみをもって正当業務行為であると整理したものではありません。
39	個人	別紙	本提言案は、不正な通信を最も直接に把握できるサービス提供者側の対策を十分に具体化しないまま、ISP による契約者の特定や DNS 遮断を詳細に示している。対策の優先順位は再検討すべきであると考ええる。また、端末がレジデンシャルプロキシ機能を有することから、当該端末が DDoS 攻撃を行う蓋然性、さらに ISP の役務提供に具体的な支障を生じさせる危険を導くまでには、論理の飛躍ないしは拡大解釈があると考えられる。 レジデンシャルプロキシを経由した不正アクセス等の具体的な危険を最もよく把握できるのは、ISP ではな	本提言案では、レジデンシャルプロキシ対策について、関係者が連携して、社会全体として対策を進めることを提言し、その中で、今後の対策例を示したも

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			く、通信を受信する金融機関、行政機関、オンラインサービス等である。これらのサービス提供者は、通信の一方当事者として、認証の成否、アクセス頻度、操作内容、送金先、金額等を直接確認できる。HTTP ヘッダ、TLS・TCP フィンガープリント、認証行動等を組み合わせてリスクを評価し、追加認証、レート制限、取引保留等を行う対策を、主要な対策として位置付けるべきである。 サービス提供者側の対策は、自ら受信した通信を安全確保のために分析するものであり、少なくとも、ISP が通信履歴等を契約者情報と照合する場合と同種の通信の秘密への介入を伴わない。このため、制度上も、まず実施を検討しやすい対策であると考ええる。 また、本提言案は、不正アクセスの発信元となった端末について、利用者の知らないうちにマルウェアに感染した機器であることは「ほぼ確実」としている。しかし、利用者が収益を目的としてレジデンシャルプロキシ機能を意図的に利用している場合等も考えられる。当該 IP アドレスから不正アクセスが行われたことと、端末が利用者の知らないマルウェア感染端末であることは、分けて考える必要がある。 特定の IP アドレス群に DDoS 攻撃等に利用される IP アドレスが含まれることから、その群に含まれる個別端末も DDoS 攻撃等を行い得ると評価することにも慎重であるべきである。 さらに、ある端末がレジデンシャルプロキシとして利用されていることは、第三者の通信を中継し得ることを示すにとどまる。それだけで、当該端末が DDoS 攻撃を行う機能又は蓋然性を有し、ISP の役務提供に具体的な支障を生じさせるとまではいえない。レジデンシャルプロキシ化していることと、ISP の役務提供に対する具体的な危険との間には、なお確認すべき事実があり、通信の秘密に踏み込む以上、より丁寧な立証が必要である。なお、ISP による利用者への注意喚起や、既知の C2 との通信の抑止を否定するものではない。 以上から、ISP による介入に先立ち、具体的な危険に最も近く、通信の秘密への介入がより小さいサービス提供者側の対策や、不正な機器の流通を防止する対策等を具体化すべきであると考ええる。 本提言案が参照する「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」の整理も、通信の秘密への介入について、具体的な危険と行為の必要性を慎重に判断することを前提としている。 サービス提供者側で実施可能な、権利利益への介入がより小さい対策を十分に検討しないまま、ISP による契	のであり、御意見に記載のサービス提供者側の対策についても、取り組むべきものの一つであると考えます。 また、御意見にあるレジデンシャルプロキシと DDoS 攻撃等との関係については、外国の事例を踏まえ、1 ページから 2 ページまでの「1. 背景」に「米国では、DDoS 攻撃とレジデンシャルプロキシの機能が同居したボットネットも報告されており、」という記載を追加いたしました。

項番	意見提出者	該当箇所	頂いた御意見	御意見に対する考え方
			約者情報の照合等に踏み込むべきではないと考える。 ISP による契約者の特定、注意喚起及び通信遮断は、対象端末及び通信の危険が十分に確認され、他の対策では十分に対処できない場合の、補完的かつ必要最小限の措置として位置付けるべきであるとする。	