

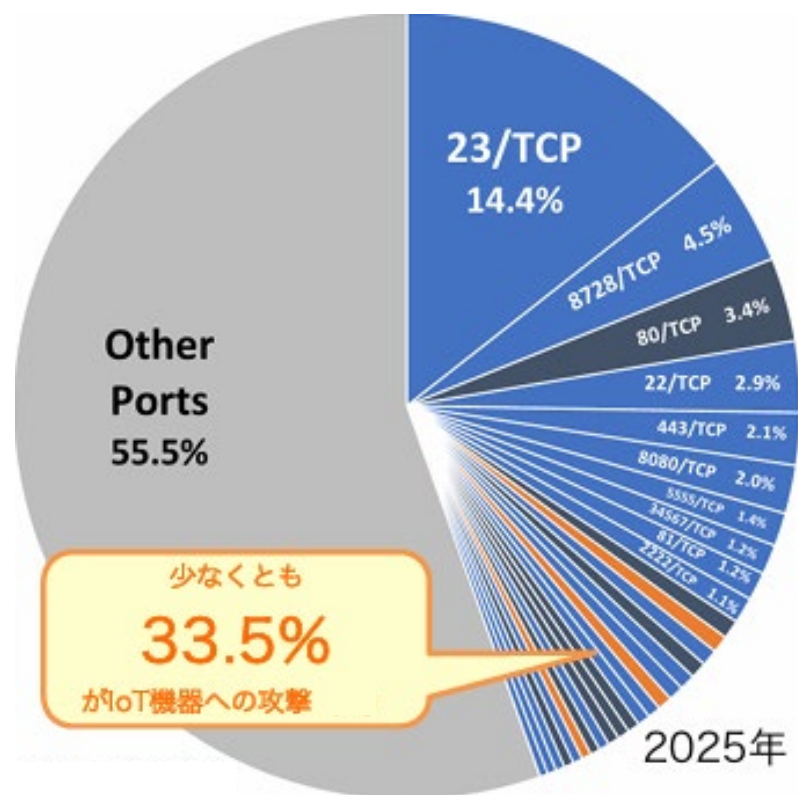
IoT機器調査（NOTICEプロジェクト）と レジデンシャルプロキシ対策について

令和 8 年 9 月 7 日
総務省
サイバーセキュリティ統括官室

1. NOTICEプロジェクトについて

2. レジデンシャルプロキシ対策について

- NICTERで観測されたサイバー攻撃のうち、**少なくとも3分の1以上**がIoT機器を狙った攻撃。
- NICTERで2025年に観測されたパケットのうち、調査目的パケット以外について、サービス種類（ポート番号）ごとに上位10ポートまでを分析。
- 上位10ポート以外のその他の宛先ポートの占める割合が増加傾向にあるが、IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。



宛先ポート別パケット数の割合
(NICTER観測レポート2025)

宛先ポート	攻撃対象
23/TCP	Telnet
8728/TCP	MikroTik RouterOS API
80/TCP	HTTP (Webサーバ)
22/TCP	SSH (サーバ、ルータ等)
443/TCP	HTTPS (Webサーバ)
8080/TCP	HTTP (Web管理画面)
5555/TCP	ADB (Android)
34567/TCP	Xiongmai DVR API
81/TCP	HTTP (Web管理画面)
2222/TCP	Telnet (ルータ、Webカメラ等)

IoT機器調査及び利用者への注意喚起（NOTICE）

4

- 情報通信研究機構(NICT)がサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、電気通信事業者(ISP)を通じた利用者への注意喚起を行う取組「**NOTICE※**」を平成31年2月より開始。さらに**令和6年度からID・パスワード設定の脆弱性の調査（特定アクセス行為等業務）に加え、ファームウェアの脆弱性等を有する機器やマルウェア感染済み機器の調査**も実施。

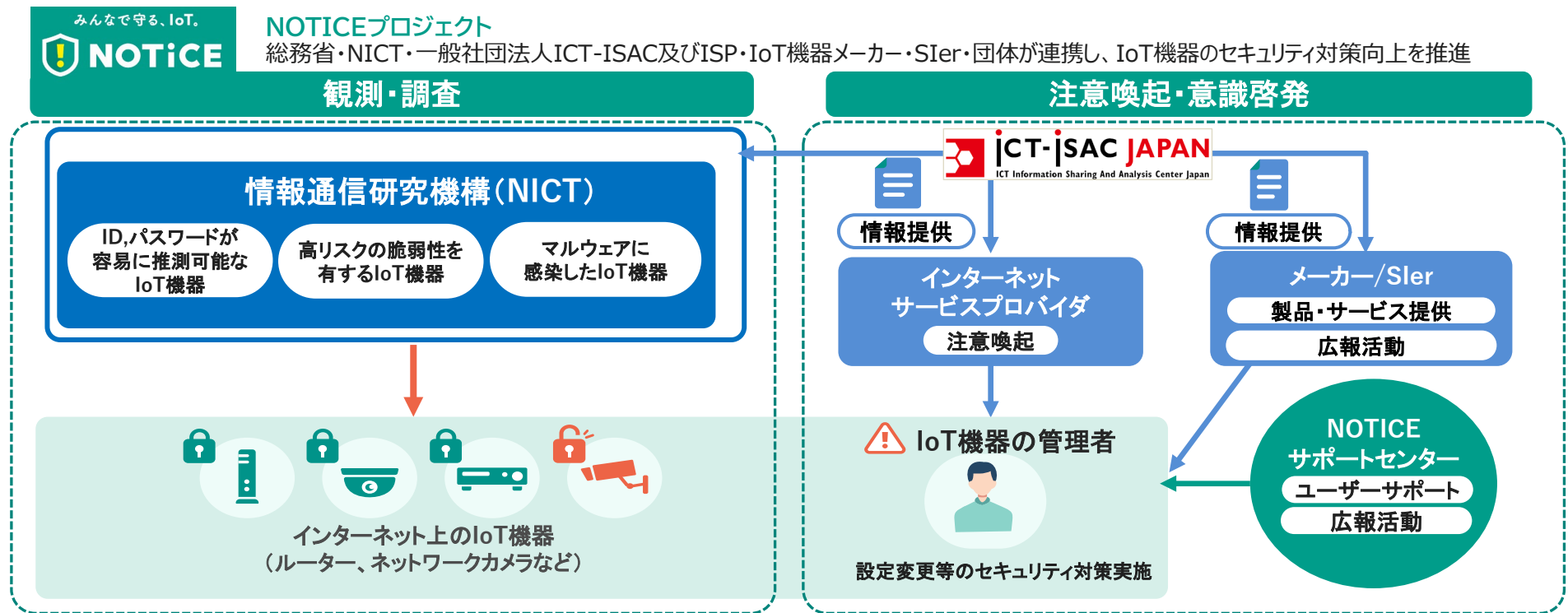
※ National Operation Towards IoT Clean Environment



脆弱なIoT機器への対処（NOTICE）について

5

- NICTがインターネットを観測・調査し、**悪意あるプログラムに感染したネットワーク機器（IoT機器）や、今後感染する危険性が高い脆弱なネットワーク機器（IoT機器）を発見**
- **電気通信事業者を通じ、当該機器の管理者に注意喚起**して対応を促すことで、被害の発生を防止



令和8年4月の結果

IOT機器観測総数

月 1.18 億件

ID, パスワードが
容易に推測可能なIoT機器

月 12,636 件

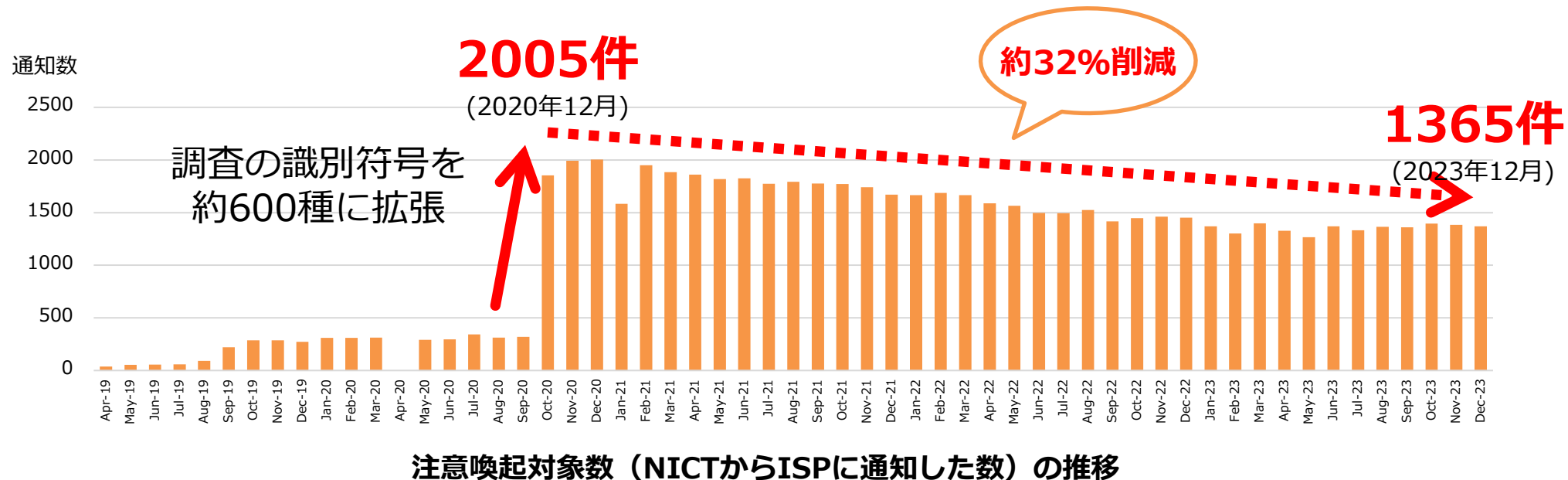
高リスク脆弱性を有するIoT機器

月 2,502 件

マルウェアに感染した
IoT機器検知数

最大 95 件/日

- NOTICEにより、マルウェアが悪用する機器（Telnet/SSH）について、ID/パスワードの脆弱性を調査。
- 特定アクセスに成功した接続先をISPに通知し、ISP経由で注意喚起を実施。
- その結果、ISPへの通知数は、ピーク時比で約32%減少。



1. NOTICEプロジェクトについて

2. レジデンシャルプロキシ対策について

レジデンシャルプロキシ機器

- 家庭内に設置され、サイバー攻撃等を経由する機器は、国内に数万台規模で存在と推定

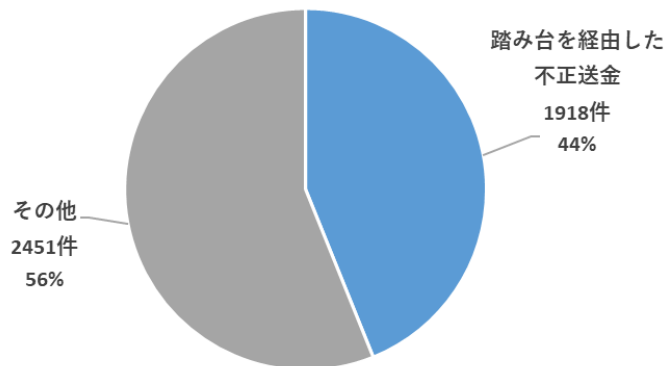


動画ストリーミングデバイスのイメージ（生成AIで作成）

➤ 昨今、家庭用IoT機器を経由したサイバー攻撃（レジデンシャルプロキシ）による被害が確認。これらは、無料で国内外のテレビ番組が視聴できると謳う「動画ストリーミングデバイス」等の様々な形で存在。利用者が気付くことなく、サイバー攻撃に悪用。

➤ 攻撃者グループは、当該機器を経由し通信元を一般家庭と偽ることで、サイバー攻撃の検知を困難なものとしている。

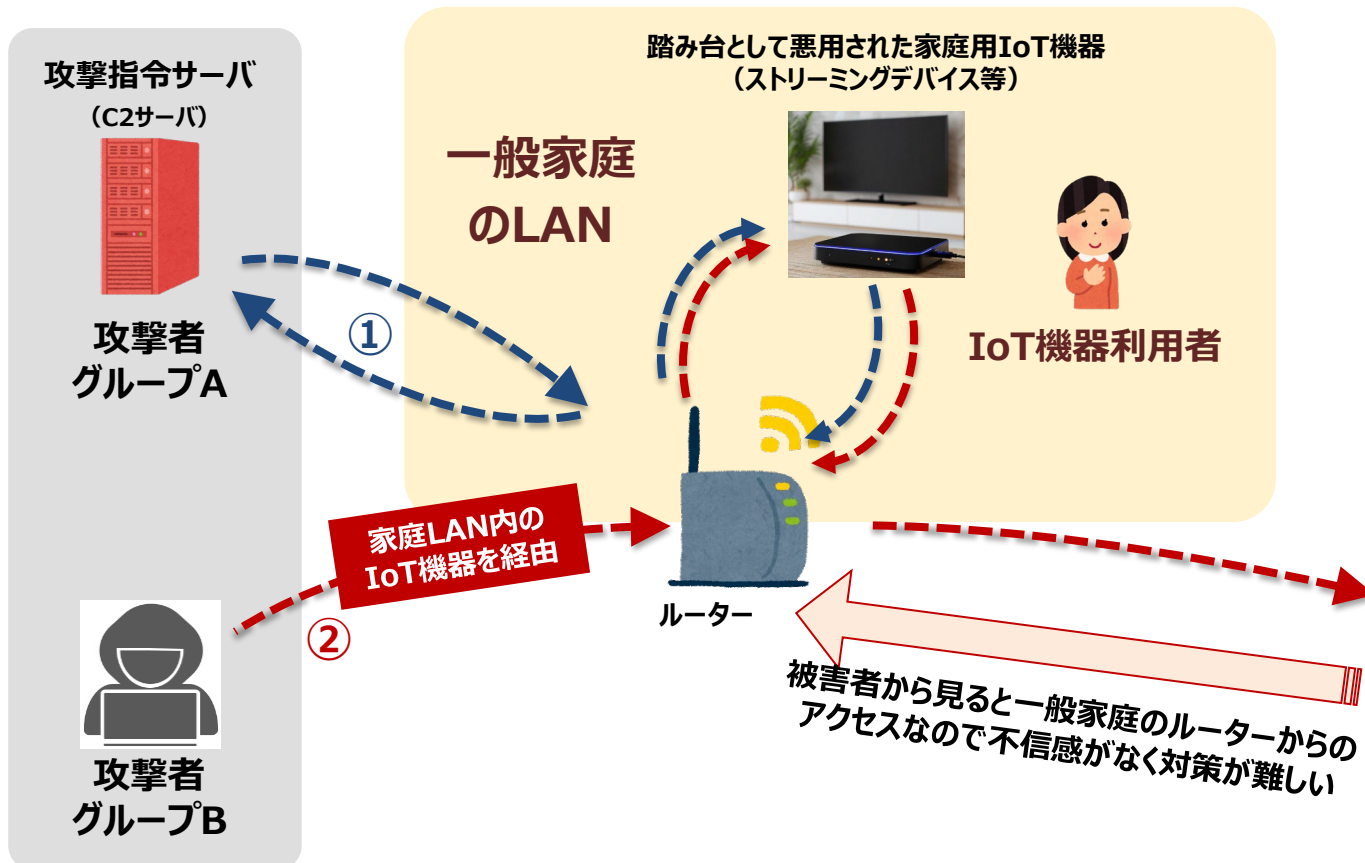
家庭用IoT機器を悪用したサイバー攻撃



➤ 令和6年中のネットバンキング不正送金事案のうち、少なくとも約44%がレジデンシャルプロキシ経由とされ、被害額については、約30億円との試算のほか、証券会社不正アクセス等での悪用も報告

➤ こうした機器は家庭等のLAN内に潜伏することで、従来のプロジェクト（NOTICE）による検知が困難なものとなっている。

- ① 利用者が、家庭内に動画ストリーミングデバイス等のIoT機器を設置すると、攻撃指令サーバ（C2サーバ）にアクセスを行い、攻撃者グループAがIoT機器を管理。
- ② 攻撃者グループBは、攻撃者Aが管理する不特定なIoT機器を経由して、金融機関等に不正アクセス等を行い、不正送金等の被害が発生。
- 家庭内に設置されたIoT機器を経由したサイバー攻撃であるため、被害組織にとっては、国内の家庭からアクセスがあったようにしか見えず、対策が困難であるとともに、利用者にとっては、自身の使用するIoT機器がサイバー攻撃の踏み台になっていることに気付くことは困難。



サイバー攻撃の被害者・考えられるサイバー攻撃

被害者が銀行・証券会社等の場合は、、、

「不正送金」



被害者が民間企業の場合は、、、

「身代金攻撃」



被害者が通信事業者の場合は、、、

「DDoS攻撃」



被害者が個人の場合は、、、

「フィッシング」



【構成員等限り】

【構成員等限り】

【構成員等限り】

【構成員等限り】