

本アライアンスの検討項目

令和 8 年 9 月 7 日
令 務 事 局

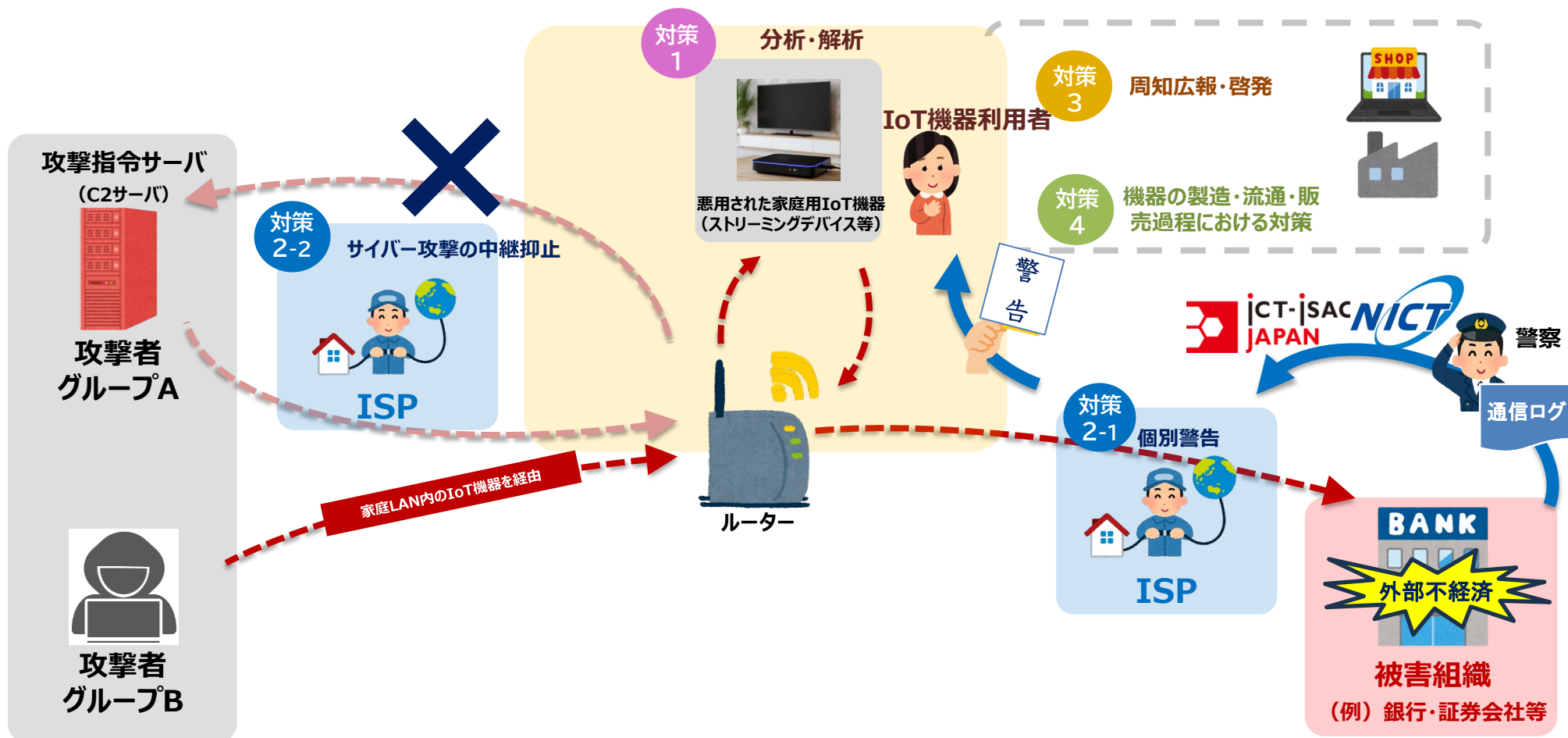
レジデンシャルプロキシを介したサイバー攻撃への対策（全体像）

1

対策の方向性 警察庁・総務省・NICT・ICT-ISAC・JC3等の関係者で緊密に連携し、攻撃システム全体に一気通貫で対応。

- ① レジデンシャルプロキシを介したサイバー攻撃関連情報の収集・分析 等
- ② IoT機器利用者への個別警告（2-1）やサイバー攻撃の中継抑止（2-2）などの対策 等
- ③ 周知広報・啓発手法
- ④ 機器の製造・流通・販売過程における対策

このほか、攻撃者グループの実態解明、警察による検挙、被害組織のセキュリティ対策強化を推進。



【構成員等限り】

【構成員等限り】

①レジデンシャルプロキシを介したサイバー攻撃関連情報の収集・分析等	・国内のレジデンシャルプロキシの実態把握 ・悪性機器に関する情報源の確保(どのメーカー/どの機器にマルウェアが予め仕込まれているのかの一次情報をどうやって得るか) ・実機による悪性性検証
②IoT機器利用者への個別警告やサイバー攻撃の中継抑止などの対策	(個別警告) ・被害組織の情報提供に係る手続き(被害者からの同意取得手続き/定期共有の頻度等) ・警察庁からICT-ISACに提供される情報 ・ISPから利用者への個別警告の手法 (C2サーバへの通信抑止) ・警察庁、NICTから提供されるC2サーバの情報(FQDN、情報の提供頻度等) ・C2サーバ情報の提供方法 ・通信抑止の効果測定の方法 (共通) ・利用者支援内容の整理(問い合わせ窓口、FAQ等) ・事業者(ISP)用ガイドライン 等
③周知広報・啓発手法	・利用者への周知広報・啓発手法(サイバーセキュリティ月間の活用を含む) ・利用者向けのレジデンシャルプロキシ判定方法の検討
④機器の流通・販売・製造における対策	・機器の流通経路・販売店・メーカー情報、国内流通規模等の把握 ・各過程(流通、販売、製造等)※における対策 ※製造過程(機器を構成するハードウェア及びソフトウェアが設計・製造されてから出荷されるまでの過程)、流通過程(機器が出荷されてから利用者以外に取引・売買される過程)、販売過程(機器が販売者と利用者間で売買される過程)

※ 検討項目について、構成員の意見等を踏まえ、随時更新を行う