資料3-1

# インターネットを取り巻く新しい脅威への対応

2026/2/26

一般社団法人 ICT-ISAC
ステアリングコミッティ委員長
小山　覚

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

# はじめに：ICT-ISACとは



- ICT分野（通信・放送・セキュリティ・SI）の情報共有・分析センター（Information Sharing and Analysis Center）
- 2002年発足のTelecom-ISACを前身とする、日本で最も歴史があるISAC組織
- 定款事業：サイバーセキュリティに関する情報収集・調査・分析、会員間の情報共有と共同対処等

**2002年のTelecom-ISACを皮切りに、日本のISAC組織は、現在7組織が活動中**


| ICT-ISACの定款事業 | 関連の活動 |
|---|---|
| **1. サイバーセキュリティに関する情報収集・調査・分析**<br>ICT分野の情報セキュリティに関する情報（インシデント情報を含む）の収集・調査・分析 | 保有観測システムによる観測 |
| **2. 会員間の情報共有と共同対処**<br>情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ、会員企業間で相互協調する仕組みを整備し、それを促進する | WG/SiG活動 |
| **3. セキュリティ人材の育成、セキュリティ啓発**<br>情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ、会員企業間で相互協調する仕組みを整備し、それを促進する | WG/SiG活動 |
| **4. セキュリティガイドライン等の整備に関する活動**<br>会員企業が情報セキュリティ対策を円滑に行う上で必要となるガイドラインの検討及び法制度に関する政府研究会等への参画 | WG/SiG活動 |
| **5. 認定協会としての活動**<br>電気通信事業法の規定による総務大臣の認定を受けた認定送信型対電気通信設備サイバー攻撃対処協会（認定協会）としての業務 | 認定協会業務 |
| **その他事業**<br>・重要インフラ情報通信分野におけるT-CEPTOAR事務局<br>・サイバーセキュリティ協議会第二類構成員<br>・ISACs参加メンバー | WG/SiG活動 |

# 総務省のサイバーセキュリティ政策への協力



- 2006年から、インターネット空間（デジタルインフラ）の安心安全に向けた官民連携施策に取り組む
- 2019年から、IoT機器の悪用によるサイバー攻撃を防止する取り組み「NOTICE」に参画中

## サイバー攻撃のトレンド

IoTマルウェア

高度で洗練されたマルウェア


ドライブ・バイダウンロード攻撃


ボットネット

## ICT-ISACが進める官民連携プロジェクト

**NOTICE** 2019~
脆弱なIoT機器への注意喚起
（総務省・NICT）

**ACTIVE** 2013~2018
PC等の総合的なマルウェア対策プロジェクト

**PRACTICE** 2011~2016
国際連携による
サイバー攻撃予知即応プロジェクト

**RDB** 2009~2012
悪性サイトの調査研究

**Cyber Clean Center** 2006~2011
ボットネット通信を検知し、対策を促す取り組み

### NOTICE
National Operation Towards IoT Clean Environment

脆弱なID・パスワード設定など、IoT機器の悪用によるサイバー攻撃を防止する取り組み

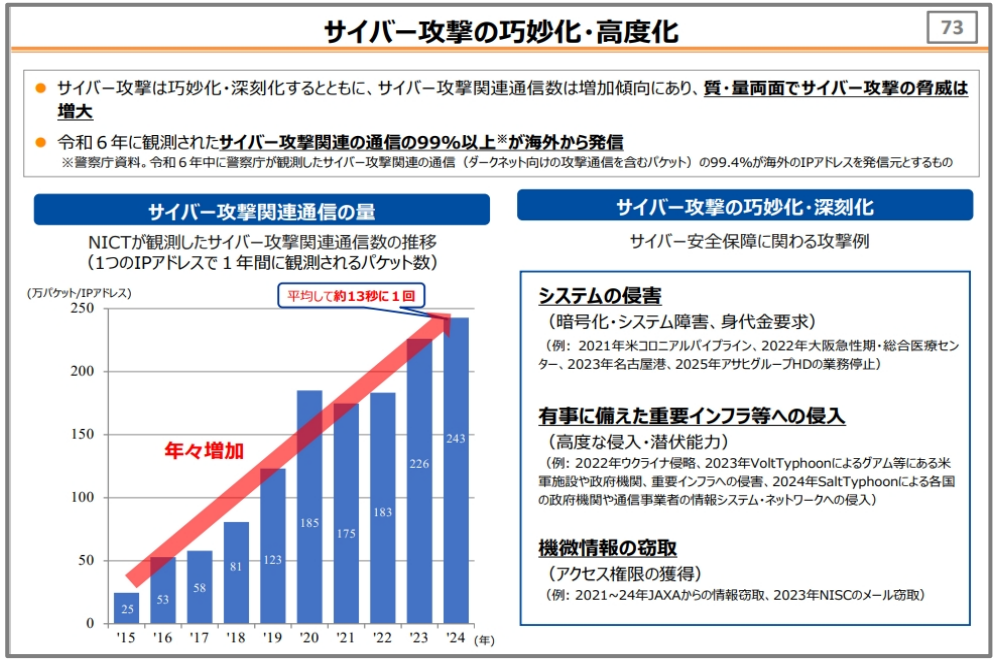
- 観測（NICTが脆弱なIoT機器等を観測）
- 分析（機種メーカに外部攻撃通信可否を調査）
- 特定（当該通信事業者に情報展開しユーザを特定）
- 連絡（IoT機器の利用者にリスクを連絡）
- 対処（ID・パスワード再設定など利用者が対処）

ユーザ特定の結果、法人の場合も多い

# サイバーセキュリティ脅威はデジタルインフラ整備推進の障壁

- **民間だけでは対応できない「犯罪や攻撃に悪用されるIoT機器等のデバイスの撲滅」が喫緊の課題**
  - サイバーセキュリティ上の**脅威は増大の一途**（主体の変化：愉快犯→**金銭目的**→**地政学的・戦略的背景**）
  - インターネットバンキングに係る不正送金事犯の被害総額は令和7年度上半期で約42億2,400万円*1 、また令和7年3月から5月にかけて証券口座への不正アクセスおよび不正取引が急増、1年間のインターネット取引サービスへの不正アクセス・不正取引の金額は約7393億円*2

*1 警察庁サイバー警察局「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」より
*2 金融庁「インターネット取引サービスへの不正アクセス・不正取引の発生状況（R8.1.14）」より

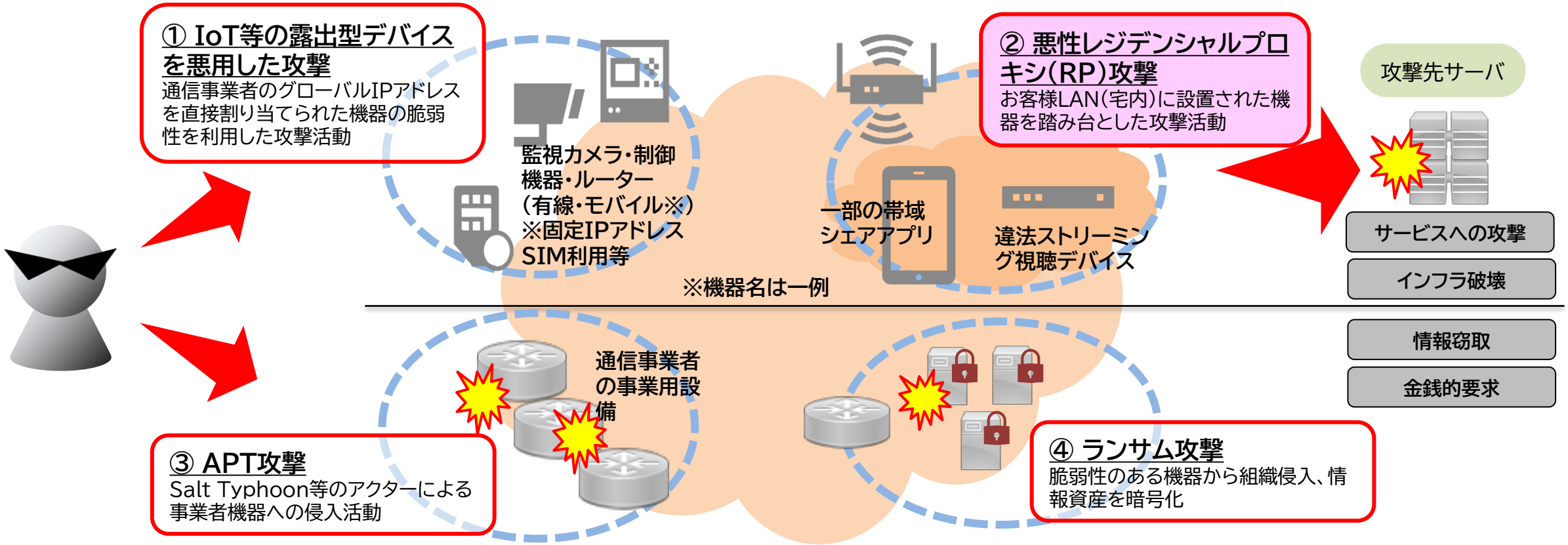




情報通信成長戦略官民協議会（第1回）参考資料3情報通信に関する現状と動向　より引用
https://www.soumu.go.jp/main_content/001053461.pdf

# インターネットを取り巻く足元の脅威 ＜概観＞



- IoT機器等を踏み台にした第三者への攻撃
  - ① IoT機器等の露出型デバイスを悪用した攻撃　IoT機器等の既知脆弱性や設定不備を利用した攻撃（NOTICEで対策実施中）
  - ② 悪性レジデンシャルプロキシ(以下RP)攻撃 宅内に設置した機器(違法ストリーミングデバイス・一部の帯域シェアアプリ)を利用した攻撃
- 通信先の組織自体を狙う攻撃
  - ③ APT攻撃(国家アクター等による攻撃)　特定組織に長期間潜伏、事業者に気づかれないまま内部情報・通信情報を窃取
  - ④ 情報資産を交渉材料にしたランサム攻撃　脆弱なVPN機器・リモートアクセス可能なホストから組織侵入、情報資産を暗号化し身代金交渉



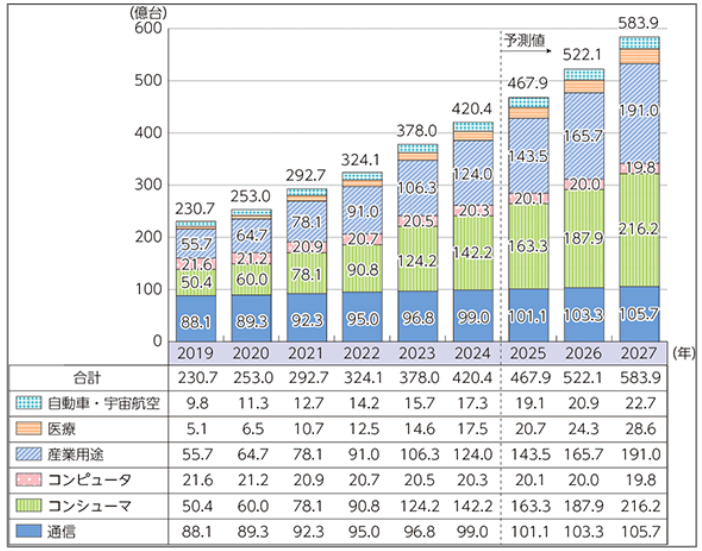
# ネットワークに接続される機器の増加によるリスクの上昇



- **ネットワークに接続されるIoT機器は増大の一途で、リスク上昇**
  - EOL/サービス終了等で、**適切なアップデートがされずに放置**されている機器が存在
  - パスワードの脆弱性を持つ機器の多くは、すでに発売から**10年以上を経過しサポート終了**した機器

## 世界のIoTデバイス数の推移及び予測

過去5年平均年率12%以上で増加、今後も台数増は継続



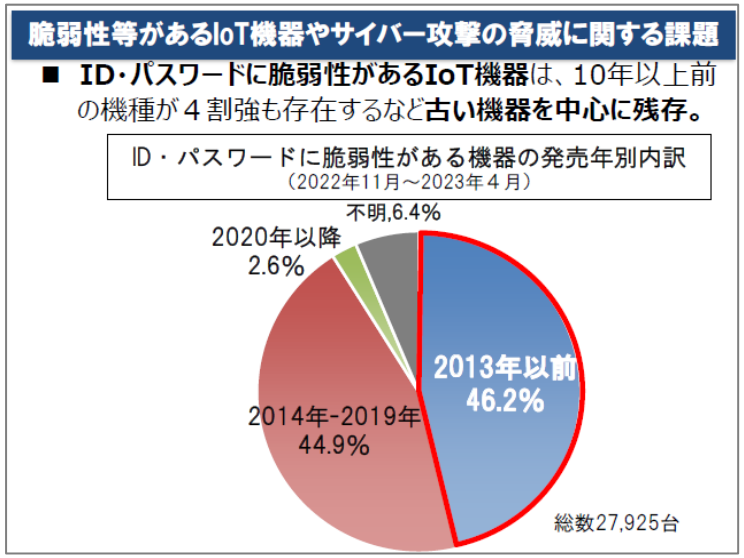

| | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 |
|---|---|---|---|---|---|---|---|---|---|
| 合計 | 230.7 | 253.0 | 292.7 | 324.1 | 378.0 | 420.4 | 467.9 | 522.1 | 583.9 |
| 自動車・宇宙航空 | 9.8 | 11.3 | 12.7 | 14.2 | 15.7 | 17.3 | 19.1 | 20.9 | 22.7 |
| 医療 | 5.1 | 6.5 | 10.7 | 12.5 | 14.6 | 17.5 | 20.7 | 24.3 | 28.6 |
| 産業用途 | 55.7 | 64.7 | 78.1 | 91.0 | 106.3 | 124.0 | 143.5 | 165.7 | 191.0 |
| コンピュータ | 21.6 | 21.2 | 20.9 | 20.7 | 20.5 | 20.3 | 20.1 | 20.0 | 19.8 |
| コンシューマ | 50.4 | 60.0 | 78.1 | 90.8 | 124.2 | 142.2 | 163.3 | 187.9 | 216.2 |
| 通信 | 88.1 | 89.3 | 92.3 | 95.0 | 96.8 | 99.0 | 101.1 | 103.3 | 105.7 |

(年)

令和7年版 情報通信白書
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html


## パスワード脆弱性を持つ機器

パスワード脆弱性を持つ機器の多くは、アップデートが提供されなくなった経年機




総務省のサイバーセキュリティ政策の動向
https://www.telesa.or.jp/vc-files/kantou/20250228telecomlec_2_MIC.pdf

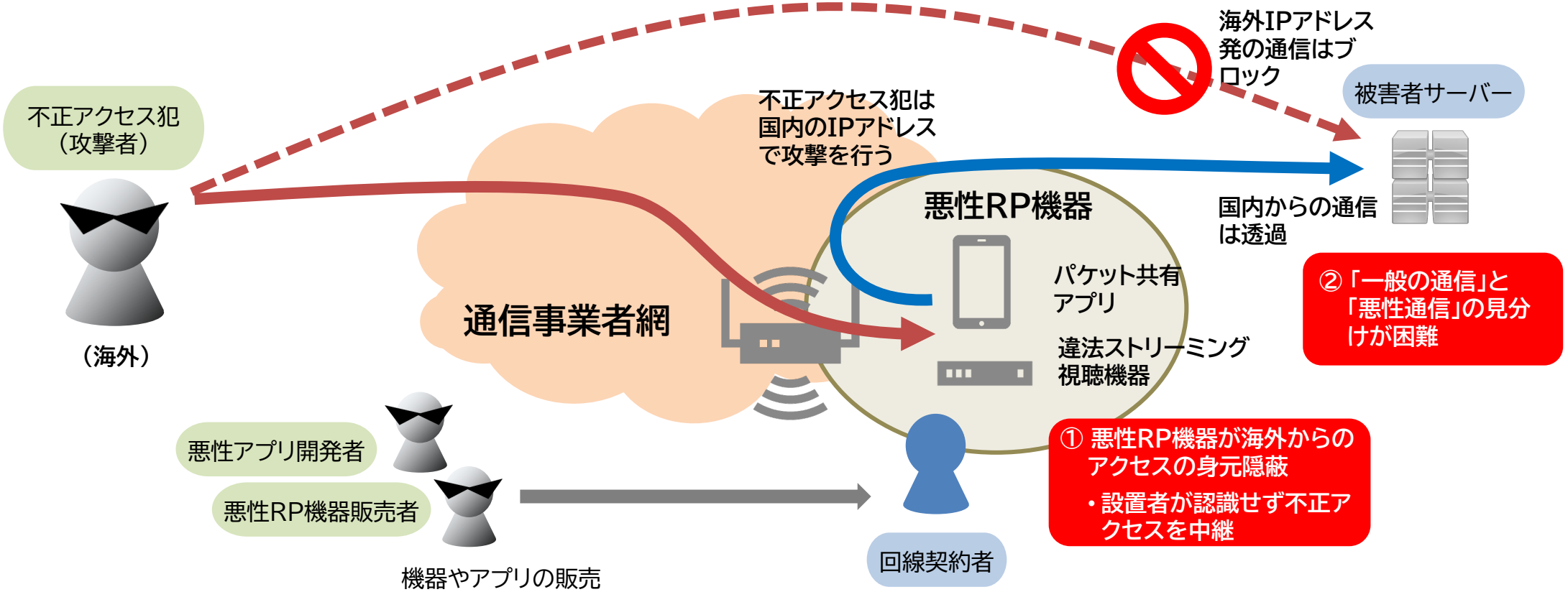
# 悪性レジデンシャルプロキシ(RP)による攻撃のイメージ



**近年金融機関への不正アクセスに、悪性レジデンシャルプロキシ(RP)機器が利用されるケースが多発**

① 家庭内に設置された悪性RP機器が**海外からのアクセスを中継、身元を隠蔽**
- **ユーザが機器設置・アプリインストール**しているが**ユーザ自身は悪性通信を中継していると認識**せず
- 機器やアプリの販売事業者は、多くの場合、表向きは正規の事業を装い、外形的には見分けが困難

② 受信側(被害サーバ)では**正常通信との見分けが困難**



# 想定される「違法ストリーミング視聴機器」「パケット共有アプリ」

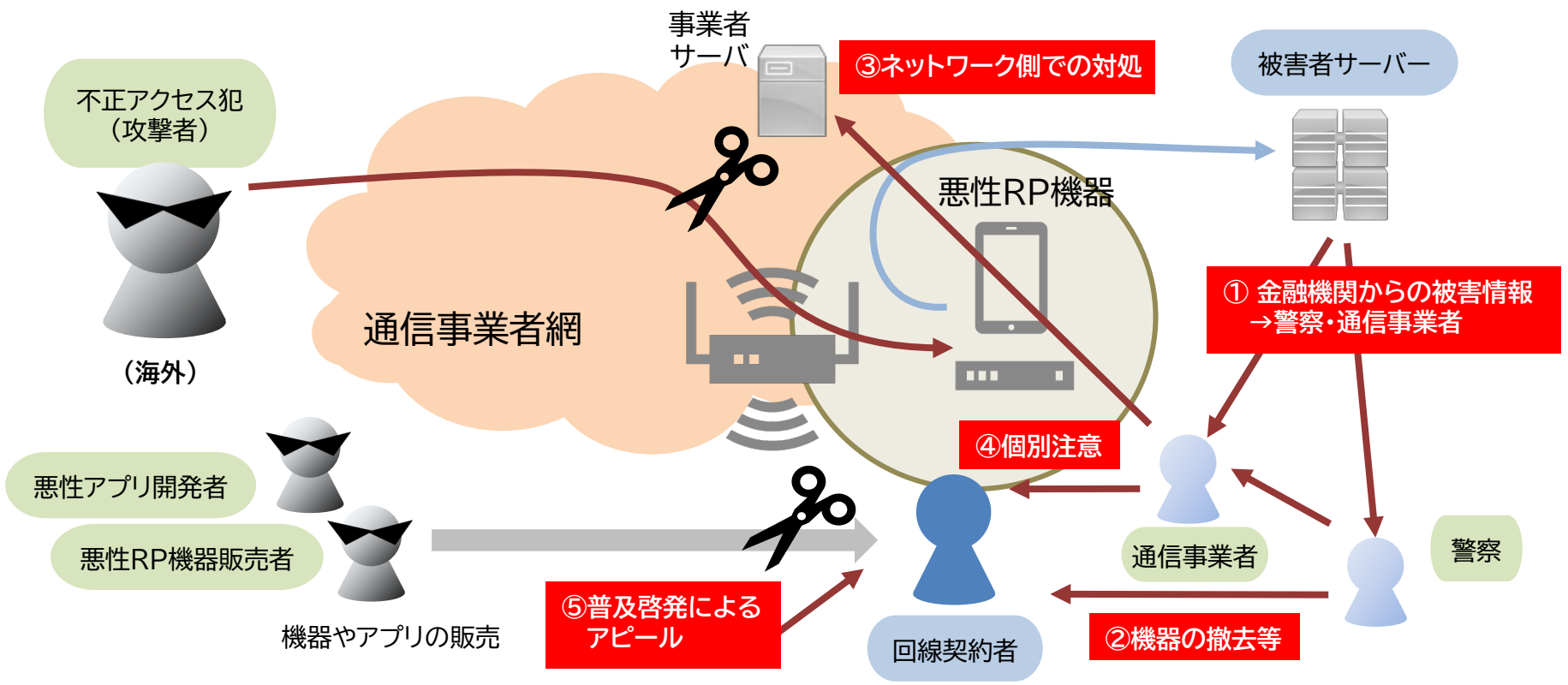


構成員限り

# 悪性レジデンシャルプロキシへの対抗（対症療法と根治対策）



- 問題解決のためには、官民が連携し**「根治対策・対症療法・普及啓発」**の効果的な組み合わせが肝要
  - **根治対策**：悪性RP機器の**撤去や取り換え**、ユーザ端末からのパケットシェアアプリの**アンインストール【②】**
  - **対症療法**：**回線契約者への個別注意**等のネットワークオペレータとしての対処**【③④】**
  - **普及啓発**：NHK等マスメディアやネットメディアでの特集を通し、**社会全体へ危険性・違法性アピール【⑤】**
- ICT-ISACが進めた過去の対策でも、**根治対策を行わないと短期間で脅威が再発**




対処後、短期間で再発した例

**構成員限り**

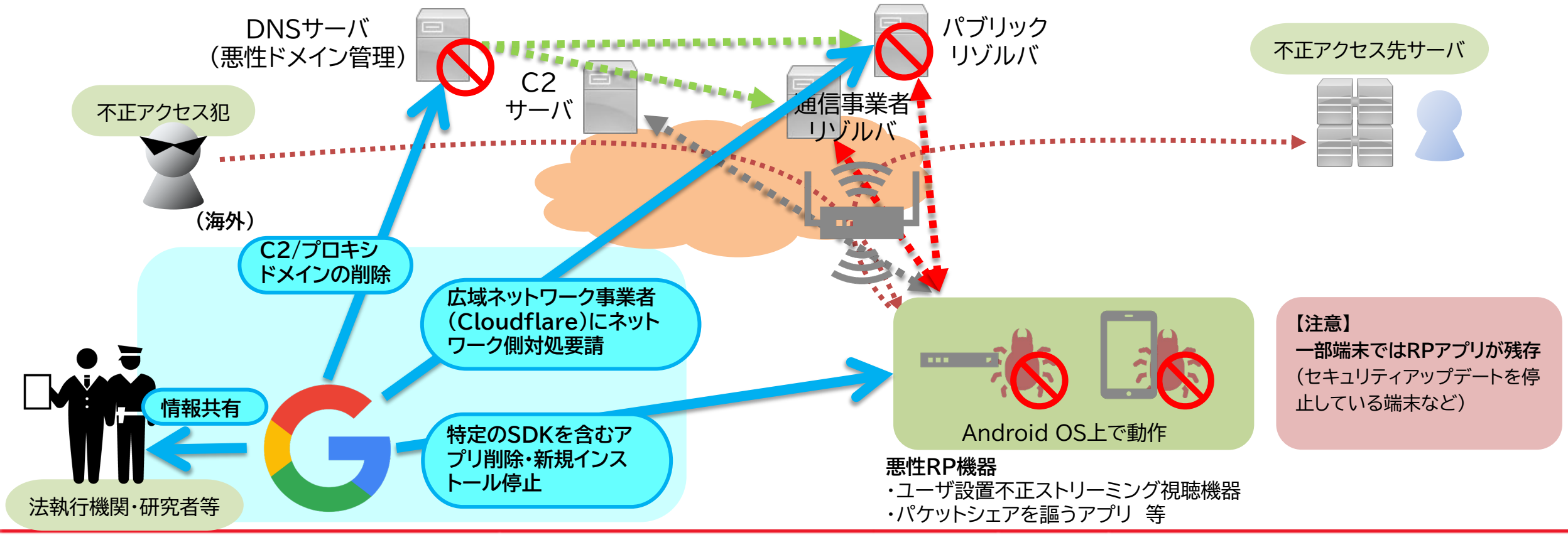
警察摘発による高効果の例

**構成員限り**

# 【参考】1/28 Google発表 「RPネットワーク遮断」対応



- 2026/1/28 Googleが自社ブログで**「IPIDEA proxy network」を遮断**したと発表
  (https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network)
  - 「法的措置でデバイスコントロール・プロキシトラフィックに利用されている**ドメインを削除、広域ネットワーク事業者へのネットワーク側対処要請**」
  - 「IPIDEAソフトウェア開発キット(SDK) に関して研究者・法執行機関・調査会社と**情報共有**」
  - 「IPIDEA SDKを**Android OS上から削除**・今後の**インストールの技術的禁止**」
- プロキシデバイスを**数百万台単位で減少**と発表、対症療法(ネットワーク側対処)・根治対策(SDK削除・ドメイン削除)の**好事例**



# まとめ



- APT攻撃・IoT等の露出型デバイス脆弱性・悪性RP機器攻撃などによりデジタルインフラ整備推進の障壁と認識
- 脆弱なIoT機器はセキュアなものに置き換えていく必要
- 様々なステークホルダーが複雑に関与して生み出される現代のサイバー脅威に対抗するには、「根治対策」・「対症療法」・「普及啓発」を適切に組み合わせて実効性を高めることが鍵
  - 対症療法については、その効果の測定も必要
- 対策には通信事業者だけでなく、総務省・警察庁とも連携のうえ社会全体での取り組みが必要

ご清聴ありがとうございました。