資料88-2

IoT 機器調査から見える 技術基準適合機器のセキュリティ対応状況

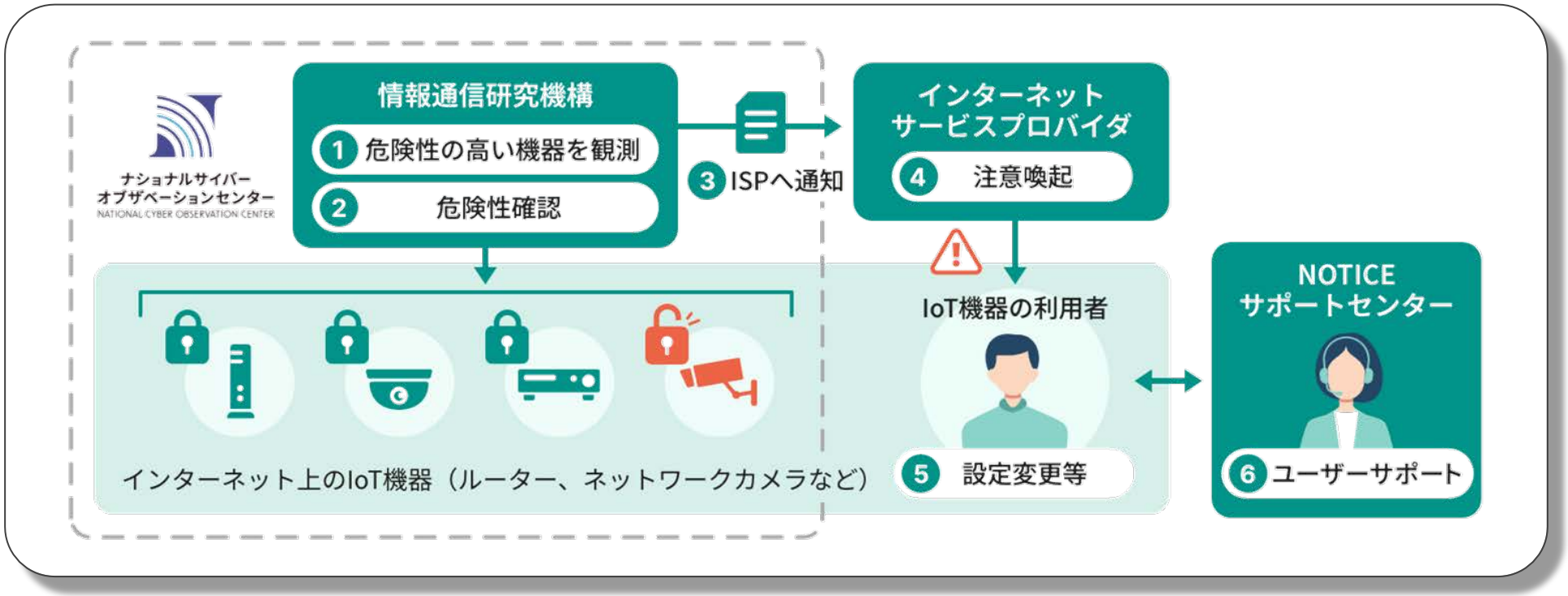
情報通信審議会 IP ネットワーク設備委員会
(2025/6/24)

国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所
ナショナルサイバーオブザベーションセンター (NCO)
研究センター長 衛藤 将史

NATIONAL CYBER OBSERVATION CENTER

NOTICE プロジェクト

- NOTICE: National Operation Towards IoT Clean Environment
- 総務省、NICT、ISP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

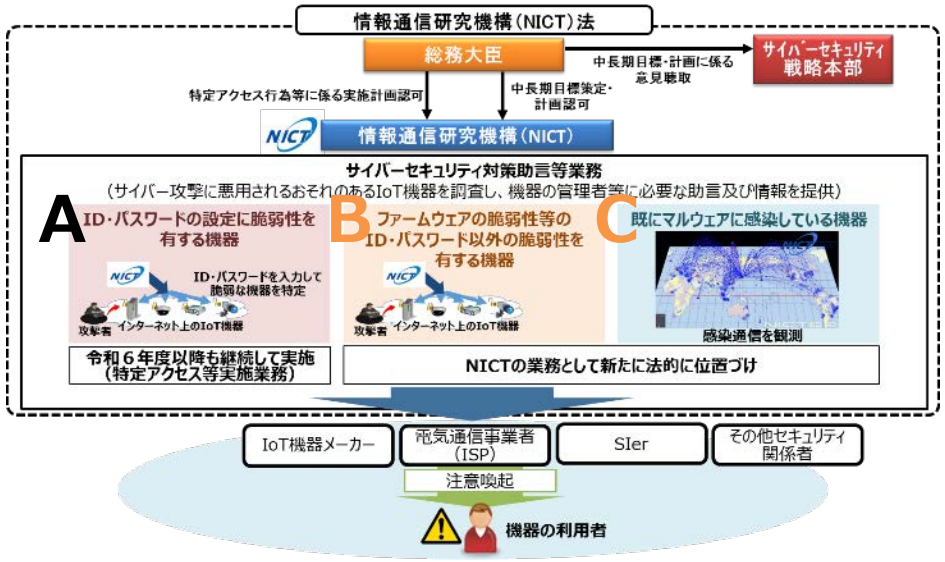


https://notice.go.jp/

NOTICE プロジェクトにおける NICT の役割

- **サイバーセキュリティ対策助言等業務**
  - A)ID/パスワード設定の脆弱性の調査 (特定アクセス調査) ← 2019 年度開始
  - B)ファームウェアの脆弱性を有する機器の調査
  - C)マルウェア感染機器の調査
  - D)リフレクション攻撃の踏み台にされうる機器の調査

  ← 2024 年度から拡充 (業務として新たに位置づけて実施)



調査事例

IoT 機器調査及び利用者への注意喚起の実施状況 (2025 年 04 月度)

NATIONAL CYBER OBSERVATION CENTER

IoT 機器観測総数

月 1.25 億件

参加インターネットサービスプロバイダ（ISP）の IPアドレスに対して観測している総数

A 容易に推測可能な ID・パスワードであるIoT機器

月 14,667 件※

- 容易に推測可能なIDやパスワードを使用しているため、攻撃者によって管理権限を乗っ取られたり、サイバー攻撃に加担させられる危険性がある機器

B ファームウェアに 高リスク脆弱性を有するIoT機器

月 4,119 件※

- 第三者に不正利用される危険性があるファームウェア脆弱性を有するIoT機器

C マルウェア感染 IoT機器検知数

最大 1,011 件/日※

- Miraiに既に感染していると推定されるIoT機器。サイバー攻撃に加担させられている可能性がある。
- IPアドレスが変動している場合は重複して計上
- 当月1日あたりの最大値を掲載

D リフレクション攻撃の 踏み台にされうるIoT機器数

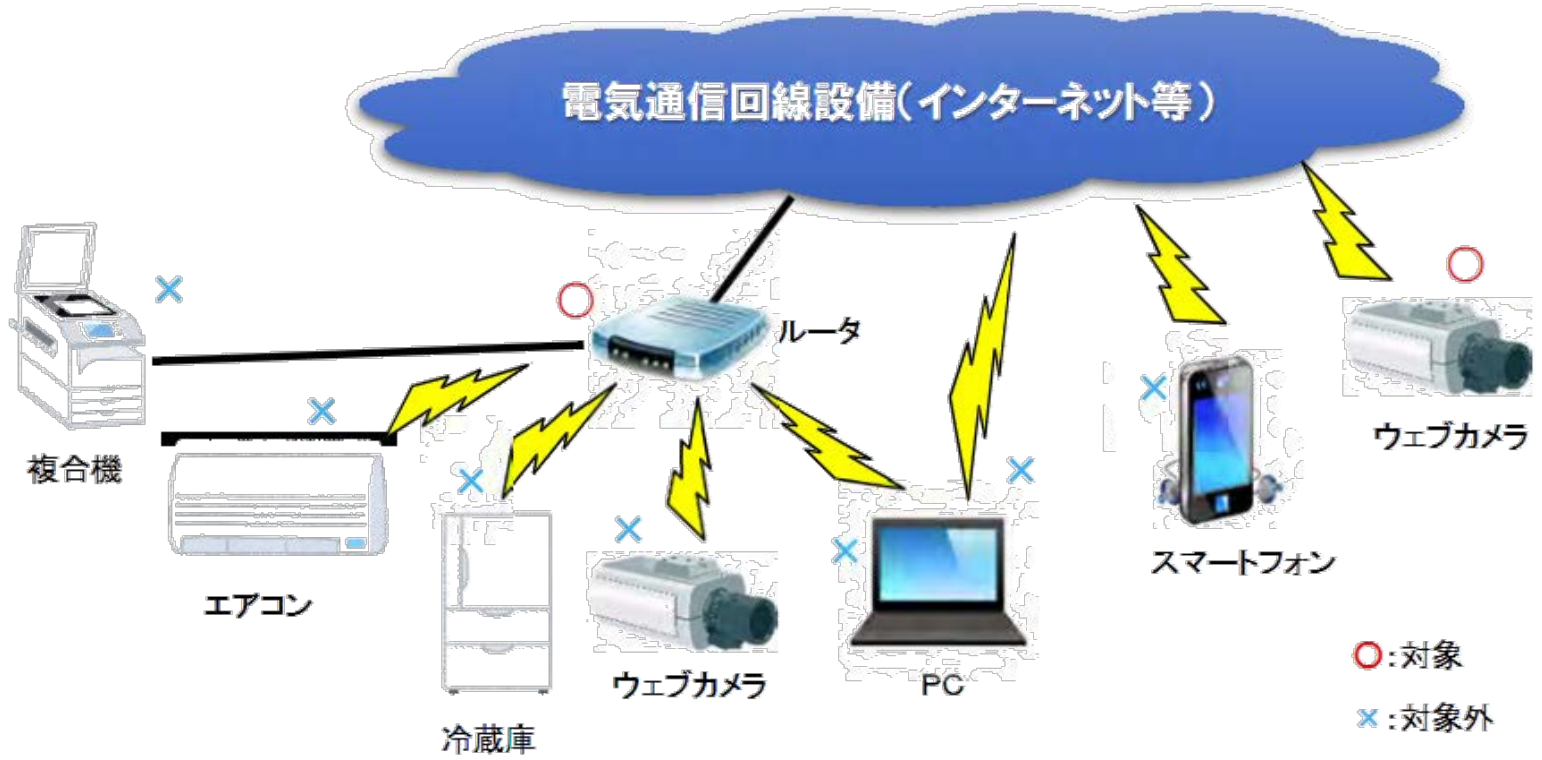
月 15,783 件

- リフレクション攻撃の踏み台にされうる可能性のあるIoT機器として検知した数

※各調査をおおむね月に 1 回 (③のみ毎日)実施し、脆弱性等が確認され、注意喚起対象となったもの (ユニーク IP アドレス数)

端末設備等規則の対象機器

- **セキュリティ基準（新規則第 34 条の 10）に係る技術基準適合認定等の対象機器の範囲のイメージ**
  - ✓ インターネットに直接接続される**ルータ、ウェブカメラ等が主な対象**
  - ✓ PC、スマートフォンは利用者が任意のソフトウェアにより随時かつ容易に変更できるため**対象外**



端末設備等規則のセキュリティ基準の改定 (2019 年)

NATIONAL CYBER OBSERVATION CENTER

一. アクセス制御

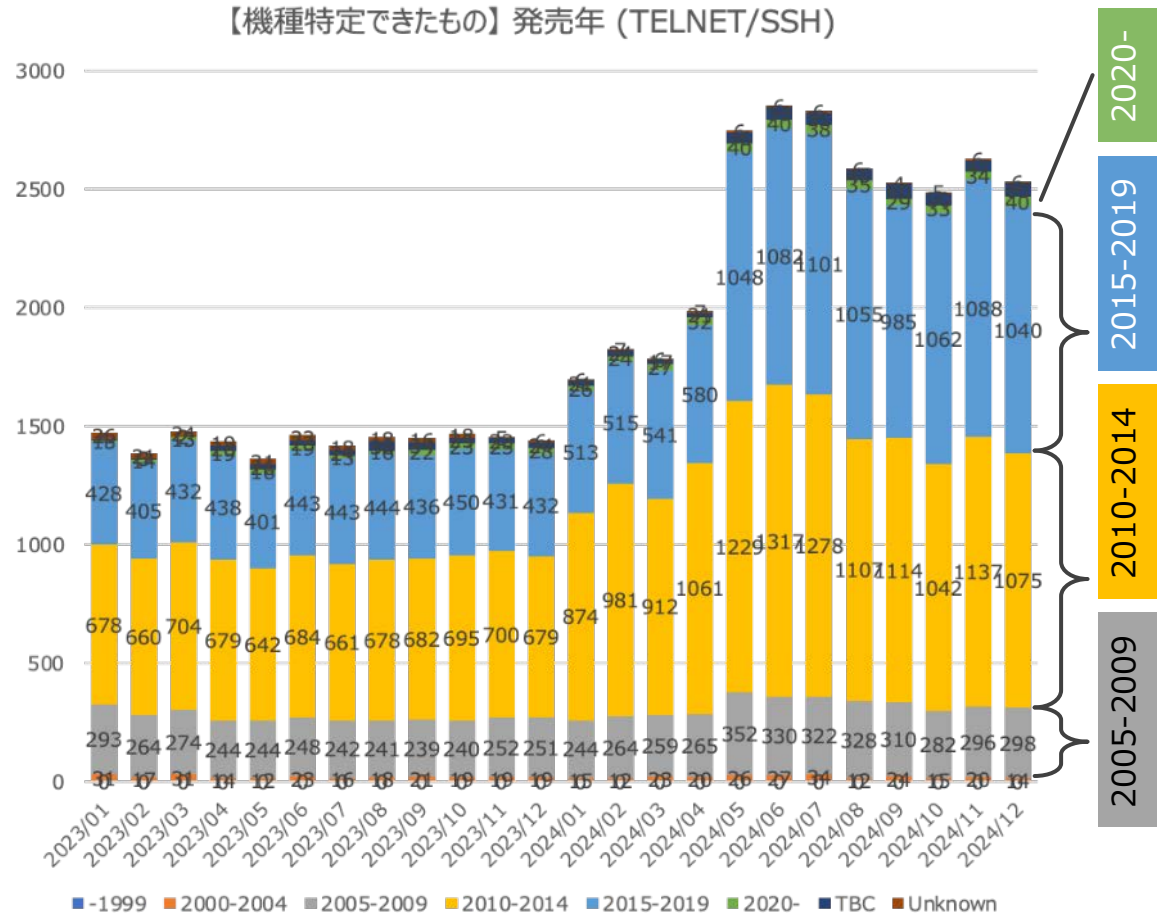
二. アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能

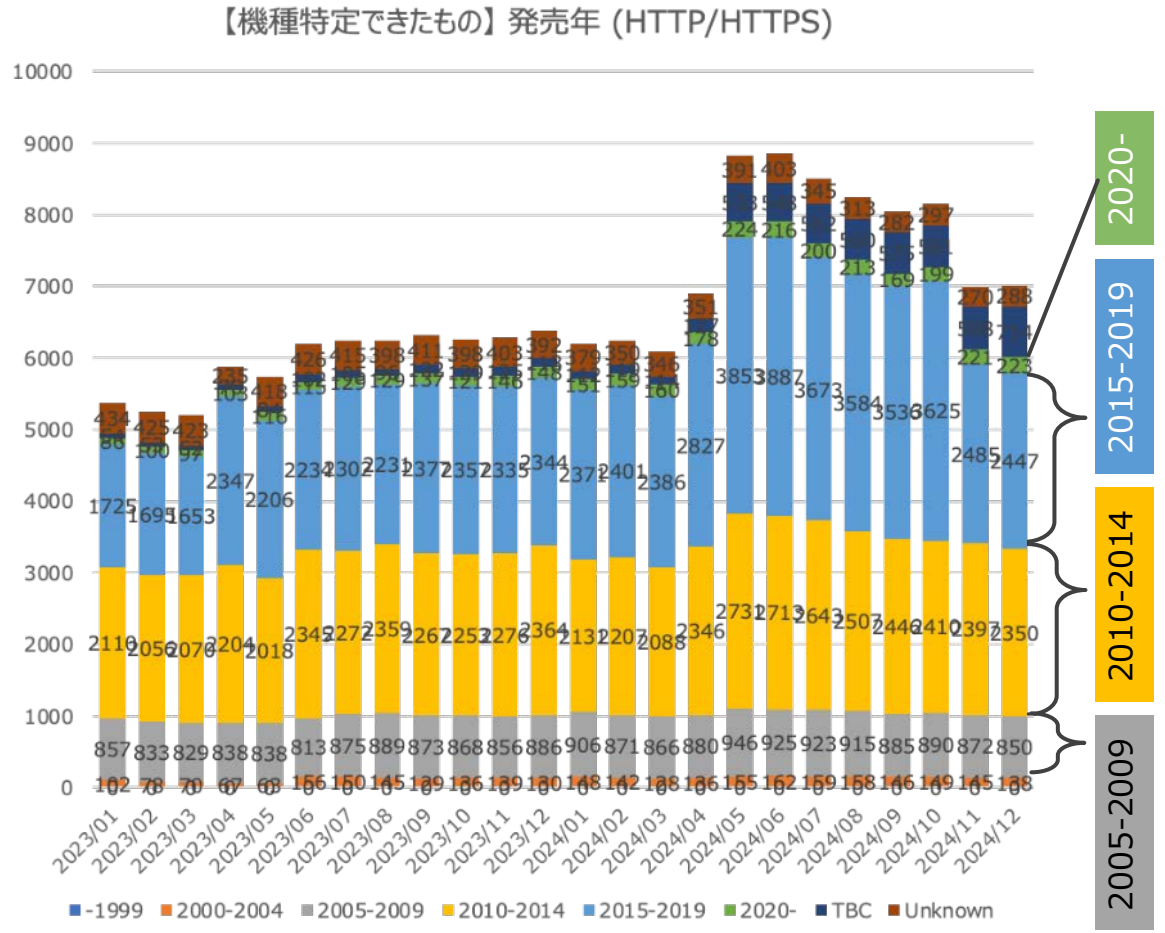
三. ファームウェアの更新機能

四. 端末への電力共有が停止した場合でも、更新されたソフトウェアや変更されたアクセス制御の設定内容を維持

脆弱な機器と発売年度の関係

- ID/パスワード設定の脆弱性の調査で発見された脆弱な機器のうち、端末設備等規則改訂前にあたる 2019 年以前に発売されたものが全体の 83~96% 程度





脆弱な機器と認証取得状況の関係

- **2025 年 1 月までに検知された 2020 年以降発売 57 機種の特徴**
  - ✓**セキュリティ基準の認証取得状況**
    - **取得済：45 機種**
    - 未取得：11 機種
    - 不明：1 機種

- **取得済み機器における検知の理由 (一部)**
  - ✓ **ID、パスワードがデフォルトのまま使用されていた**
    - パスワード変更に関して**【後で変更】する機能が用意**されていた 等
  - ✓ **ユーザーによって脆弱なパスワードが設定されていた**
    - 複雑性を強要していない、8文字以下のパスワードを許容するなど、**機器側のパスワードルールが厳しくない** 等

まとめ

NATIONAL CYBER OBSERVATION CENTER

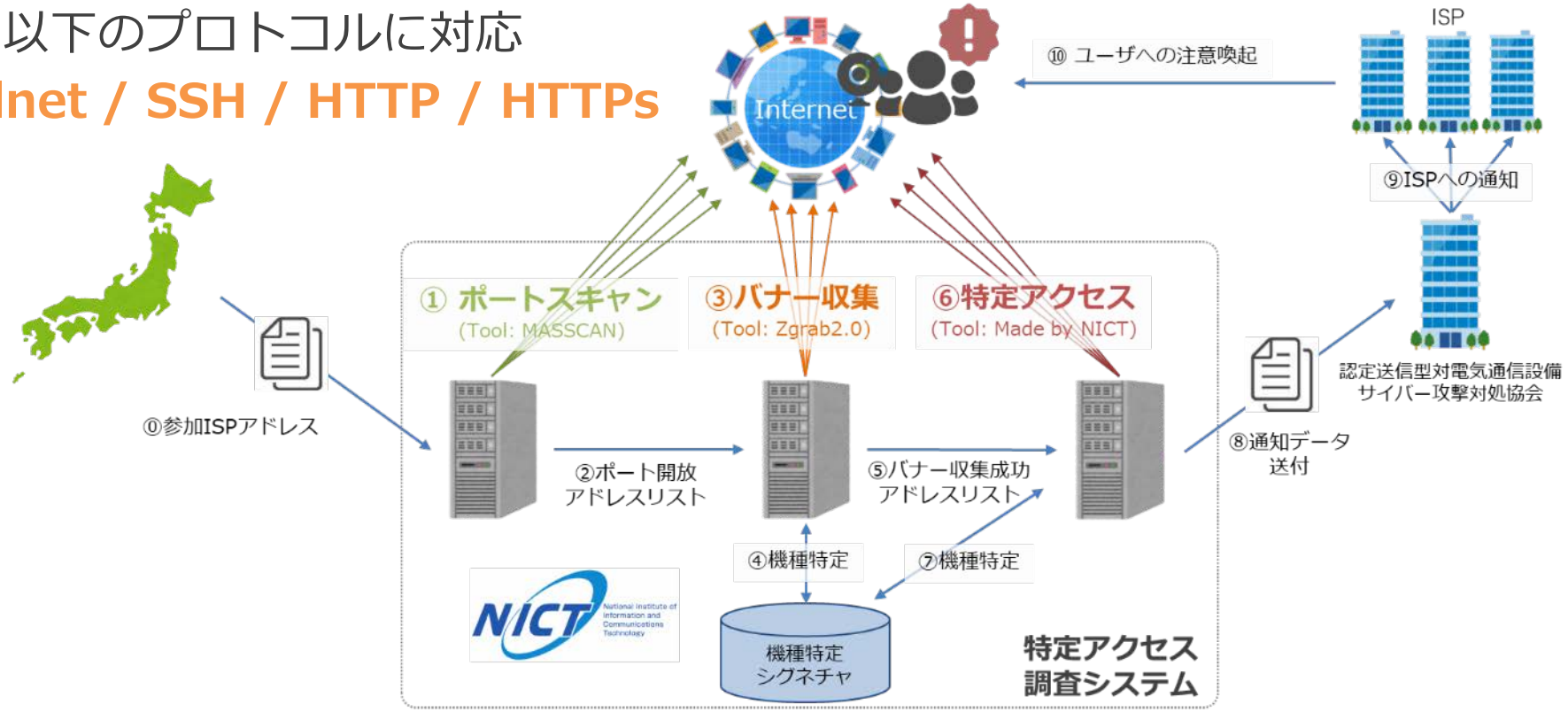
- **調査を通じて得られた主な知見**
  - ✓ 注意喚起を通じて脆弱な機器が**有意な件数減少**することを確認
    - ISP 等を通じた**調査と通知に一定の効果**があることは明白
    - 減少の主な理由
      - ➢ ベンダによるファームウェアアップデートの配布
      - ➢ 通信事業者による対処 (フィルタ設定等) 等
  - ✓ 一方で、**一定期間後に減少幅が縮小**する (下げ止まる) 傾向も
    - いわゆる「根雪」のように残り続ける脆弱機器への対処が課題
  - ✓ ID/パスワード設定の脆弱性の調査で発見された脆弱な機器のうち、**端末設備等規則改訂前にあたる 2019 年以前に発売**されたものは全体の 83~96% 程度

調査方法

A) ID/パスワード設定の脆弱性の調査 (特定アクセス調査)

NATIONAL CYBER OBSERVATION CENTER

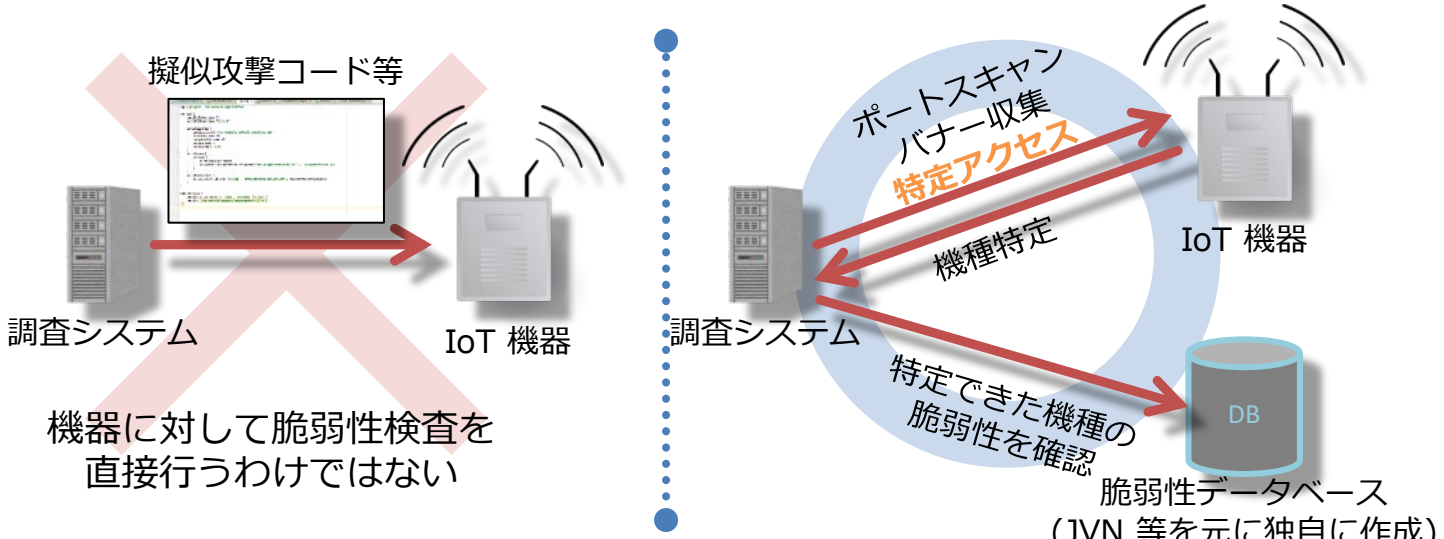
- **2019年2月20日より特定アクセス調査と通知業務を開始**
  - ✓ 特定アクセス行為
    - サイバー攻撃に悪用される危険性があるかを観測するために、インターネット上の IoT 機器に**容易に推測される ID 及びパスワードを入力**
  - ✓ 現在、以下のプロトコルに対応
    - **Telnet / SSH / HTTP / HTTPs**



B) ファームウェアの脆弱性を有する機器の調査

NATIONAL CYBER OBSERVATION CENTER

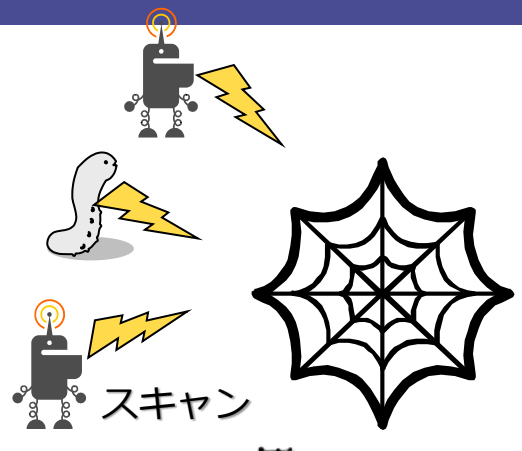
- **概要**
  - ✓ 外部から攻撃可能なセキュリティホール等の**ファームウェアの脆弱性を有する機器**を注意喚起の対象として調査
  - ✓ IoT 機器の脆弱性の中から**脆弱性の深刻度**、**普及台数**、**社会的な影響**、**攻撃への悪用可能性**をはじめとする様々な観点から評価
- **調査方法**
  - ✓ 機器に対して**脆弱性検査を直接行うわけではない**
  - ✓ ポートスキャン、バナー収集等の調査により**機種が特定できた機器の情報**を用いて、独自に整備した脆弱性データベースと照合し、合致する脆弱性があれば通知を実施



C) マルウェア感染機器の調査

●概要

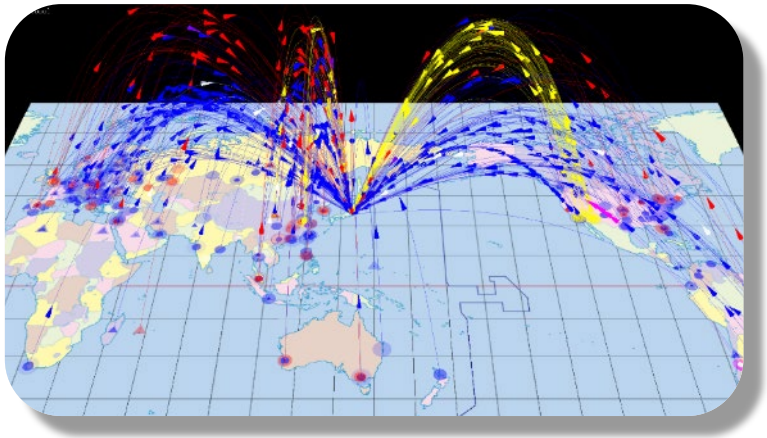
- ✓観測対象ネットワークにおいて**マルウェアに感染した端末**からの攻撃が NICTER で観測された場合に通知
- ✓現状では **MIRAI 感染端末**を対象として調査を実施



ダークネット観測網

●NICTER とは

- ✓サイバー攻撃リアルタイム大規模観測・分析システム
- ✓国内外で30万の未使用 IP アドレス "**ダークネット**" を観測
- ✓無差別型サイバー攻撃の大局的な傾向把握に有効



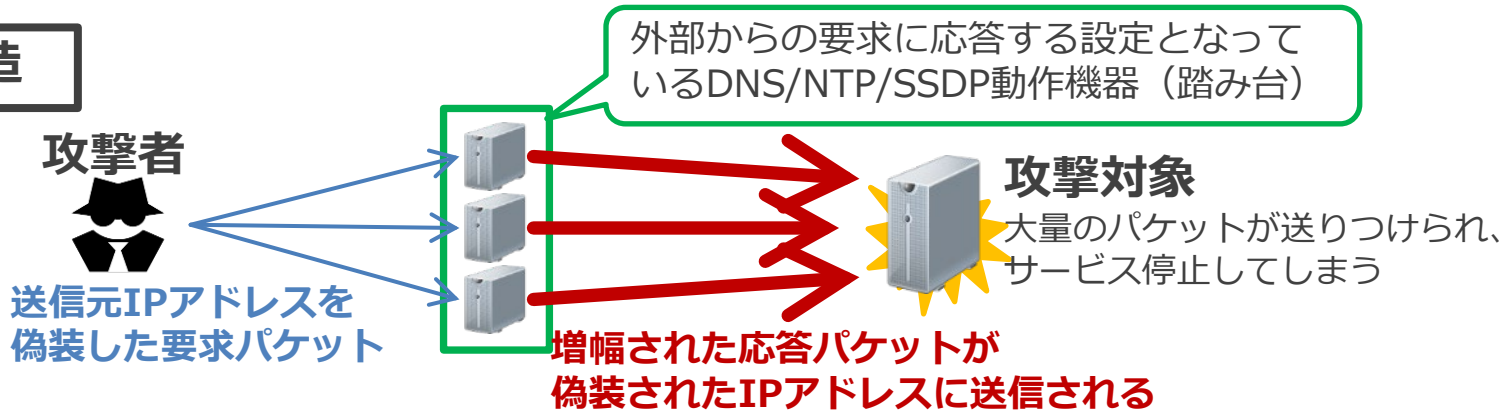
NICTER における
ダークネット観測のイメージ

D) リフレクション攻撃の踏み台にされうる機器の調査

●概要

✓リフレクション攻撃 (下図) への対策のため、**脆弱性を有するDNS/NTP/SSDPサービスが動作する機器** (ブロードバンドルータ、レコーダー、カメラ、その他IoT機器) を調査

リフレクション攻撃の構造



●調査対象プロトコル及び調査方法

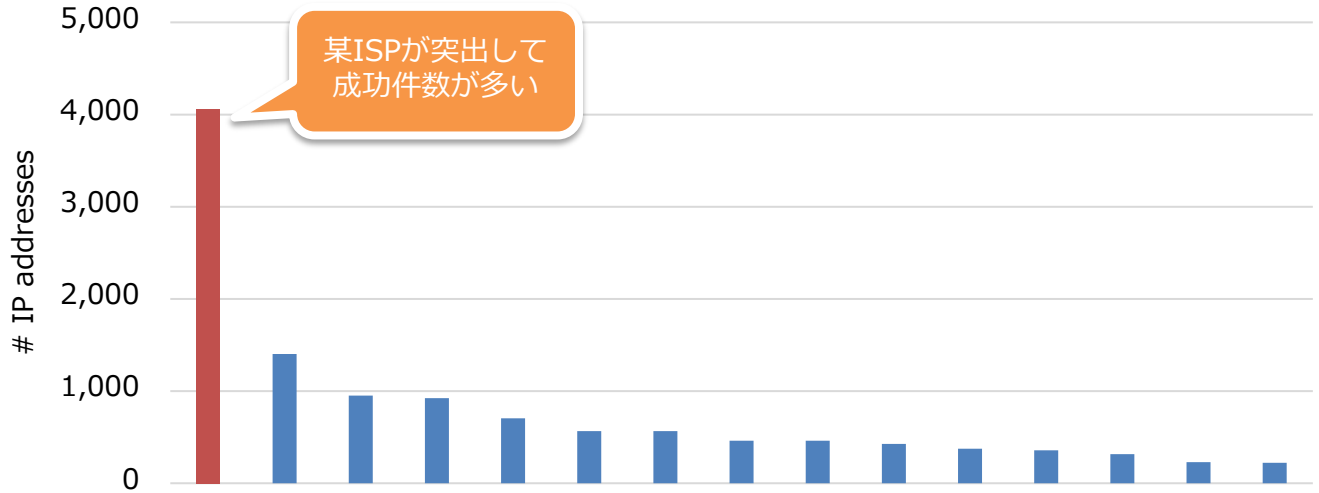
✓攻撃に悪用されやすい、**増幅率が高く踏み台の数が多い**3種のプロトコルを調査

✓調査サーバより該当のポートが開いている機器に対してクエリを送信し、応答を確認することで踏み台となり得る機器を検出

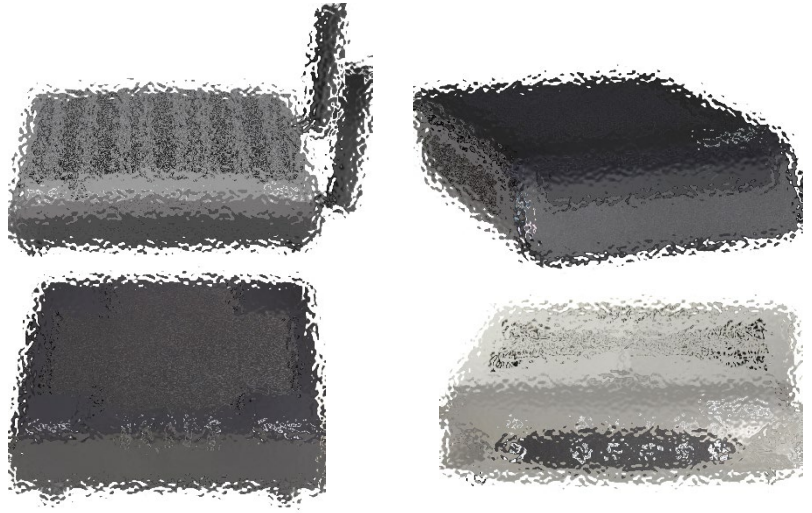
事例 (A：ID/パスワード設定の脆弱性の調査 (特定アクセス調査))

ISP配布ルータのID/PW設定不備を発見

- **2022 (R4) 年3月：HTTP予備調査時に某ISP内で大量の機器にログイン成功**
  - ✓ バナー情報から4000台以上は全て同一機器だと推測し、ISPに通知
- **同月：当該ISPが調査した結果、ISP管理ルータ(顧客配布モデム)と判明**
  - ✓ 全て特定ベンダの機種(バージョン違い含む)であったため、ISPからベンダに修正を依頼
- **～2022 (R4) 年5月頭：ISPで修正ファームウェアの適用を実施し、対処完了**



予備調査時(2022 (R4) 年3月)のISP別のhttp(s) 特定アクセス成功数



特定されたISP配布のルータシリーズ

脆弱な流量計機器の発見と対処

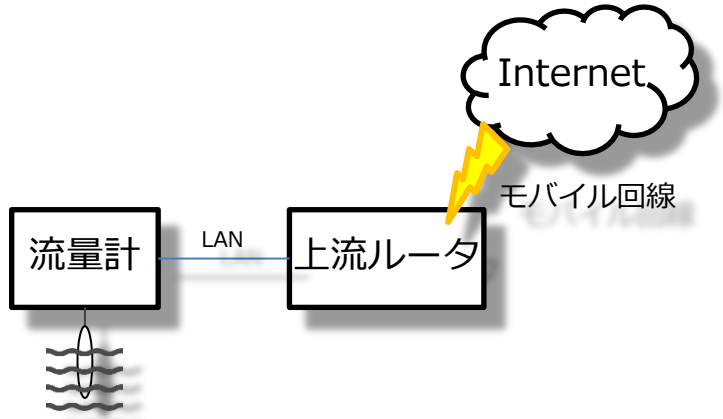
NATIONAL CYBER OBSERVATION CENTER

- **発見から対処完了までの経緯**

1. NOTICE の**調査開始初期より、TELNET での特定アクセスに成功**する特徴的な機器を発見。
   - 機種特定が困難であったため注意喚起対象とならず、その時点では対処出来ず。

2. その後、**NICTER の観測において当該機器のマルウェア感染を確認。**
   - **調査**の結果、設置業者の特定に成功。
   - 設置業者にヒアリングを行う事で、**機種を特定**。

3. 設置業者にて、対処を行った結果、2024 年 3 月時点での特定アクセス調査による**検知数は 0 件まで低減**。



1. で想定された機器構成のイメージ

2. で特定可能となった該当機器
(手前が上流ルータ、奥が流量計本体)

ISP 等を通じた利用者への注意喚起だけでなく、
ベンダー、設置業者等の関係者への直接の働きかけも有効であることを示す事例

ソフトウェア脆弱性調査

NATIONAL CYBER OBSERVATION CENTER

- **外部から攻撃可能なセキュリティホール等の<u>ソフトウェアの脆弱性を有する機器</u>を注意喚起の対象として調査を実施**
  - ✓ 国内外のメーカーが製造するルータやネットワークカメラ (デジタルビデオレコーダー (DVR) を含む)、VPN 機器やゲートウェイなどを脆弱性調査の対象機器として想定。
  - ✓ IoT 機器の脆弱性の中から**<u>脆弱性の深刻度</u>**、**<u>普及台数</u>**、**<u>社会的な影響</u>**、**<u>攻撃への悪用可能性</u>**をはじめとする様々な観点から評価

#	選定基準の例
1	JVNで緊急とされているもの
2	CVSS値が高いもの
3	通信サービスへの影響が懸念されるもの • OSコマンドインジェクションの脆弱性を有するもの • 検知数が多いもの
4	当該機器による攻撃を観測しているもの • NICTER のハニーポット等で検知 • CISA KEV (Known Exploited Vulnerabilities Catalog) 等に掲載されているもの
5	NICT によるソフトウェア脆弱性調査によって検知可能なもの
6	ゼロデイ脆弱性であるもの (→ ベンダーへの働きかけへ)
7	NICT の外部機関から協力依頼のあったもの
8	当該機器のベンダから使用中止勧告が出ていたり、後継機種への乗り換えが推奨されているもの
9	当該機器の悪用事例が世間に認知されていると思われるもの

ソフトウェア脆弱性調査

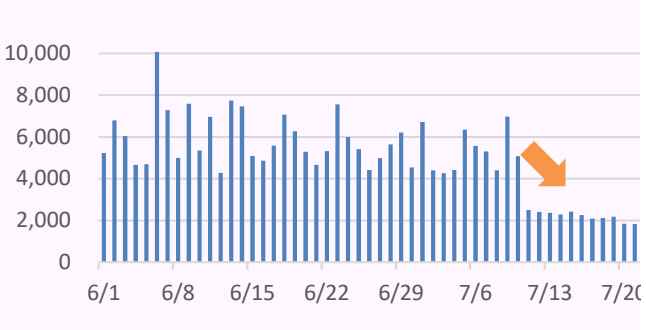
NATIONAL CYBER OBSERVATION CENTER

- 3 件のファームウェア脆弱性の調査を開始し、計 60,155 件の通知を実施
- その後の製品ベンダと連携した対処により対象とする脆弱性に関して顕著な観測数の減少を確認

国内ベンダ製無線ルータ

主な用途：家庭等において、インターネットに接続し、無線LAN等を提供するための機器
脆弱性詳細：Web設定画面がインターネット上からアクセス可能かつ、Web設定画面の脆弱性を用いて任意のコマンドが実行可能。

ベンダから対策済みファームウェアの配信とNOTICE による注意喚起が始まると、
平均6,000ホストから2,000ホストまで減少

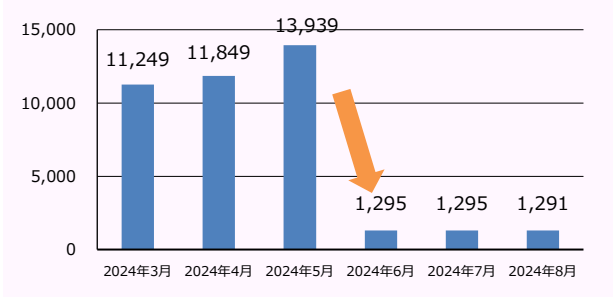


マルウェアからの感染拡大通信の観測数
（NICTERによる観測）

海外ベンダ製壁埋め込み型ルータ

主な用途：家庭等において、インターネットに接続し、無線LAN等を提供するための機器
脆弱性詳細：脆弱性を有する管理画面がインターネットからアクセス可能な場合、管理画面に攻撃を行うことでルーターの悪用が可能になる。

当該機器を導入しているマンション向け ISP がインターネットからのアクセス制御を実施したことで、6月から検知数が**約 1/10 に減少**

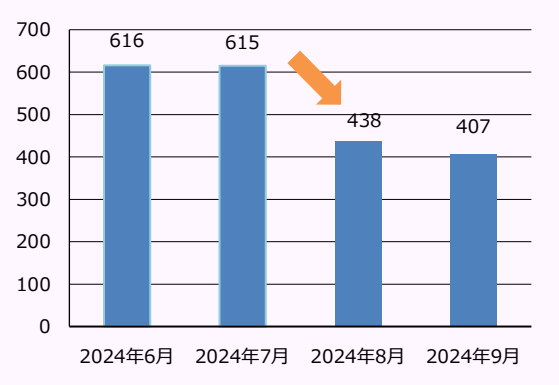


脆弱性のあるD-Link社製壁埋め込み型ルータの観測数
(NOTICEによる観測)

国内ベンダ製モバイルルータ

主な用途：
IoT機器等をインターネットに接続し、機器を遠隔で保守するための装置

実機の挙動解析により侵入経路を明らかにし、該当するポート番号 (6666/tcp) を NOTICE の調査対象に追加して注意喚起を行った結果、脆弱性のある当該国内ベンダ製モバイルルータの観測数が減少。



脆弱性のある国内ベンダ製モバイルルータの観測数
（NOTICEによる観測）