資料７－３
※一部非公開※

# 新しい NOTICE における調査業務

2024 年 5 月 10 日 (金)
ICTサイバーセキュリティ政策分科会

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

# はじめに

NATIONAL CYBER OBSERVATION CENTER

## 1. 最近の取り組みと事例

- ✓ HTTP(S) フォーム認証への対応
- ✓ 従来の NOTICE における調査事例

## 2. 新しい NOTICE における取り組み

- ✓ 新しい NOTICE における NICT の役割
- ✓ ファームウェア脆弱性調査

## 3. 今後のナショナルサイバーオブザベーションセンター (NCO) の業務の方向性

- ✓ CURE の活用による高度分析情報の提供
- ✓ 重要施設を対象としたアタックサーフェス調査の実施

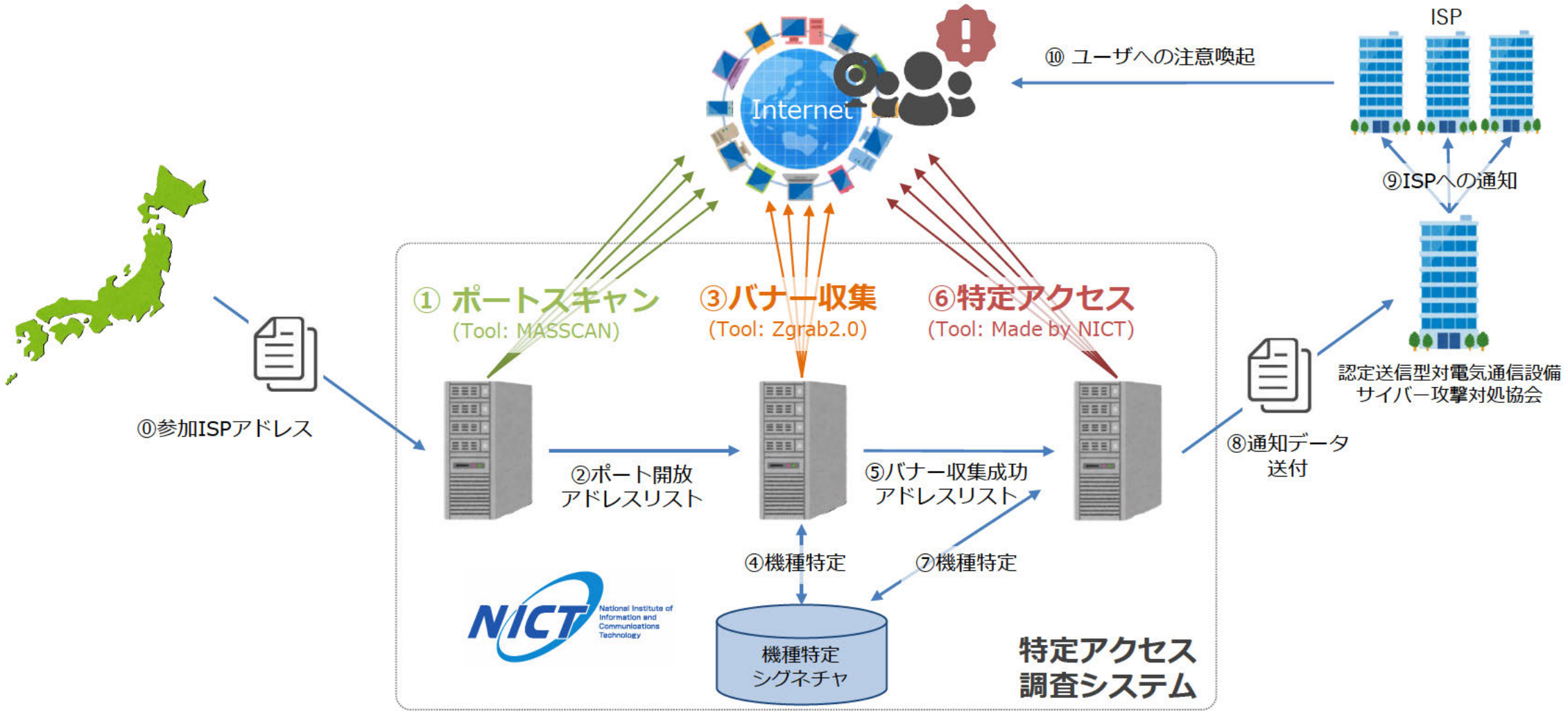
## 4. おわりに

# 最近の取り組みと事例

# これまでの NOTICE (特定アクセス調査)

NATIONAL CYBER OBSERVATION CENTER

- 2019 (R1) 年4月以降の特定アクセス調査と通知業務



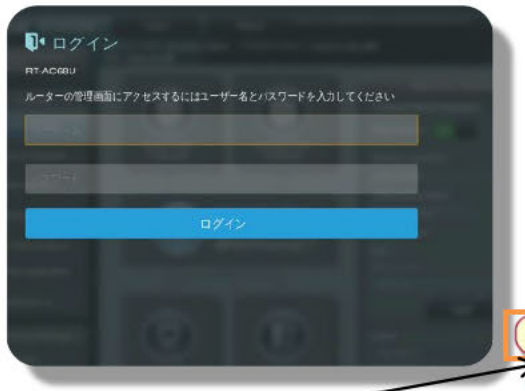
# HTTP(S) のフォーム認証への対応 (R5)

NATIONAL CYBER OBSERVATION CENTER

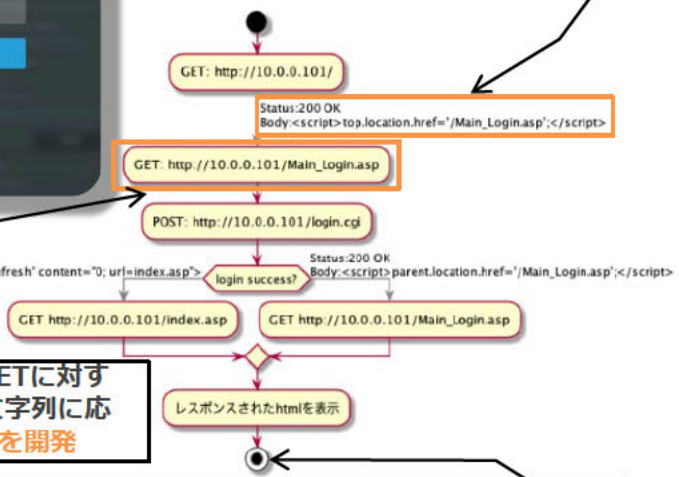
**40機種のフォーム認証に対応したシステムを開発し、2023 (R5) 年6月から本調査開始**

a. HTTP(S)のリダイレクト遷移機能を開発
b. 使用するログイン用スクリプトを決定するため、特定のキーワードやパス情報をキーとする機種特定機能を開発
c. 機種毎に個別のログイン用スクリプト、特定のキーワードやパス情報をキーとするログイン成功判定ロジックを開発

## 機種 A のログイン画面とフォーム認証の全体フロー



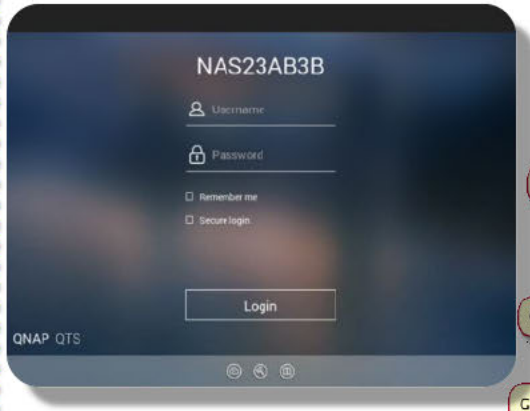

a. location.hrefのパスを検出する機能を開発・実装。/Main_Login.aspの検出によりログイン画面へのアクセスを実現




b. /Main_Login.aspへのGETに対するレスポンスに含まれる文字列に応じて機種Aを特定する機能を開発

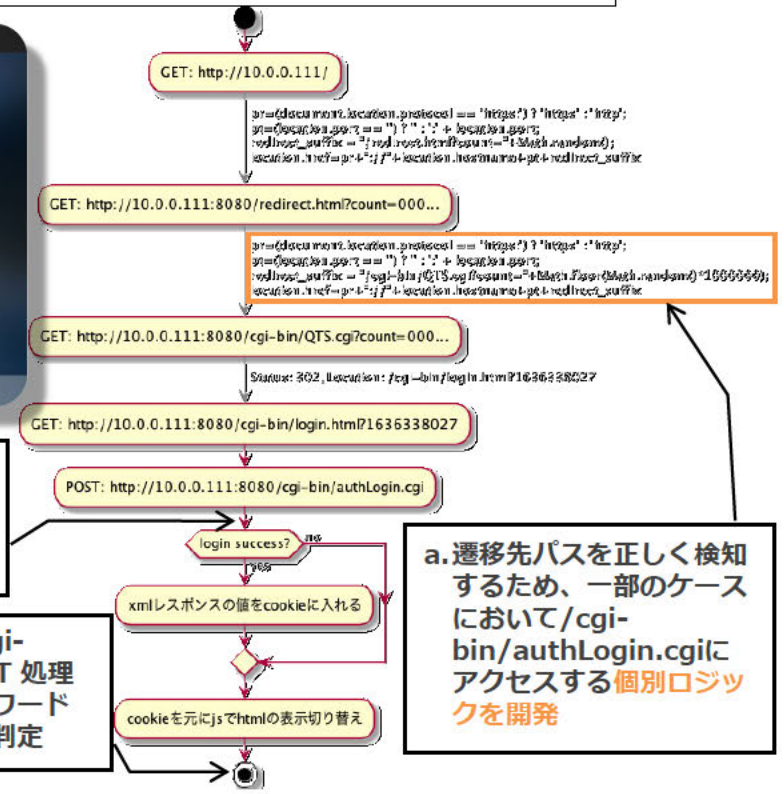
c. 機種Aと特定した機器について /login.cgi に別途 POST 処理を行い、レスポンスに “url=index.asp“が含まれていればログイン成功と判定

## 機種 B のログイン画面とフォーム認証の全体フロー




b. /cgi-bin/authLogin.cgiからのレスポンスに機種Bの型番名が含まれていれば機種Bと機種特定する機能を開発

c. 機種Bと特定した機器について/cgi-bin/authLogin.cgi に別途 POST 処理を行い、レスポンスに所定のキーワードが含まれていればログイン成功と判定




a. 遷移先パスを正しく検知するため、一部のケースにおいて/cgi-bin/authLogin.cgiにアクセスする個別ロジックを開発

# NICTER との連携による NOTICE の調査能力の向上

NATIONAL CYBER OBSERVATION CENTER

- **NICTER 解析チームとの相互連携**
  - ✓ これまで NOTICE では、主に特定アクセス調査に注力
  - ✓ 今般、新しい NOTICE の推進のため、**NICTER との情報共有体制**を強化
    - NICTER 解析チームとの連携で、より多面的な分析が可能となり NOTICE の調査能力が向上
    - 一方、NICTER においても NOTICE からの提供情報を解析業務に活用

# [redacted] モバイルルータ [redacted] 宛の攻撃

NATIONAL CYBER OBSERVATION CENTER

- **攻撃の観測 (2023 年 7 月下旬)**
  - ✓ NICTER のハニーポットにおいて、当該機種を標的にしたと思われる TELNET 通信のパケットを観測

- **NICTER 解析チームの分析により判明した攻撃の流れ (攻撃者視点)**
  1. 事前にサーバヘッダの情報を確認し、[redacted]ルータか判定
  2. TELNET へアクセスの確認 (アクセスできれば 4 へ)
  3. HTTP から**脆弱なパスワードでログイン**して TELNET を有効化
  4. TELNET へアクセスし、**任意のコマンドやマルウェアを実行**

- **特定アクセス調査による当該端末の特定**
  - ✓ 同時期の特定アクセス調査においても、脆弱なパスワードにより ログイン可能な[redacted]モバイルルータを多数検知※ (右表)。
    ※HTTP での検知数

**ID／パスワードの脆弱性により侵入された後に実際に機器が悪用された事例の一つ**

[redacted]

| 観測月 (2023年) | 特定アクセス成功件数 |
|---|---|
| 6月 | 409 |
| 7月 | 390 |
| 8月 | 485 |
| 9月 | 436 |
| 10月 | 439 |
| 11月 | 454 |
| 12月 | 483 |

攻撃観測当初における[redacted]
特定アクセスの成功件数 (HTTP)

# 脆弱な流量計機器の発見と対処

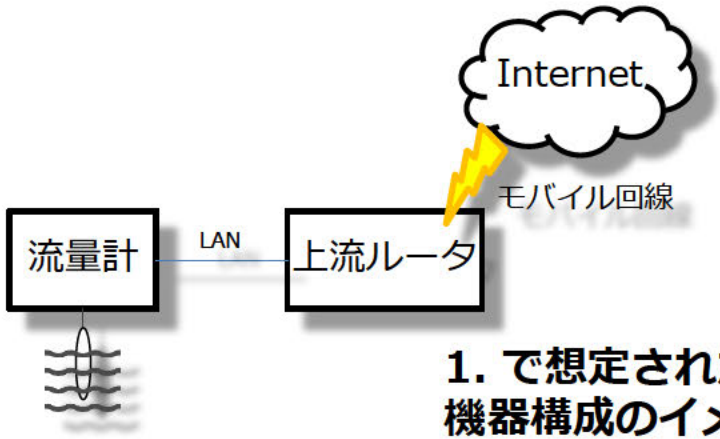
NATIONAL CYBER OBSERVATION CENTER

- **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。（ルータの下に流量計が接続されている構成が想定されたが、いずれも機種特定できず）

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。**
   - **NICTER 解析チームによる調査**の結果、設置業者の特定に成功。
   - NICTER 解析チームが設置業者にヒアリングを行う事で、**機種の特定が可能となった**。

3. 設置業者にて、以下の対処を行った結果、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**。
   - 管理者権限にて再起動 (マルウェアの削除)
   - 各ユーザのパスワードを複雑なものに変更 (再侵入の阻止)
   - 不審なユーザが存在しないか確認 (バックドアユーザを確認)
   - 流量計の WebUI アクセスポートの変更 (念のための対策)




**1. で想定された機器構成のイメージ**

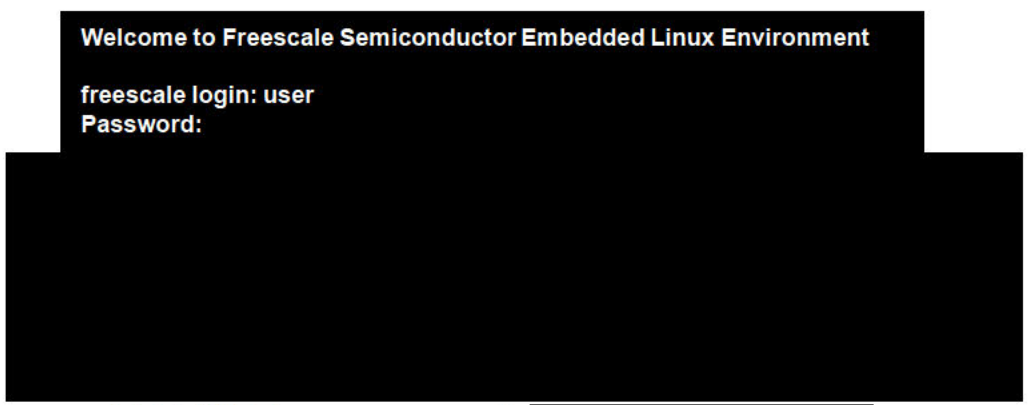
**2. で特定可能となった該当機器 (手前が上流ルータ、奥が流量計本体)**

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

# [参考] 経緯①：特定アクセス調査における流量計の発見

NATIONAL CYBER OBSERVATION CENTER

- [redacted](モバイルレンジ) で特定アクセスに成功する特徴的な機器を認識
  - ✓ 23/TELNET で特定アクセスに成功 (ID/Password は全て同一)
  - ✓ 特定アクセス調査の開始当時 (2019 年前半) から数十台規模で観測 (調査月によって変動)
    - 参考：75 アドレス (2020 年 7 月調査時)、63 アドレス (2024 年 1 月調査時) *TELNET での検知数のみ
  - ✓ 特定が困難な機種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
- **バナー調査によって、流量計の上流ルータに特定アクセス成功していると推測**
  - ✓ Telnet バナー情報から、組み込み機器用チップ搭載機器と推定 (**機種特定不可のため注意喚起対象外**)
  - ✓ HTTP (80/TCP) で Web UI にアクセスするとタイトルに製品名と施設名らしき文字列が含まれる
    - [redacted]観測された通信経路の長さの違いから、Telnet が上流ルータの UI で、Web UI はその配下に接続された装置のものと推測された



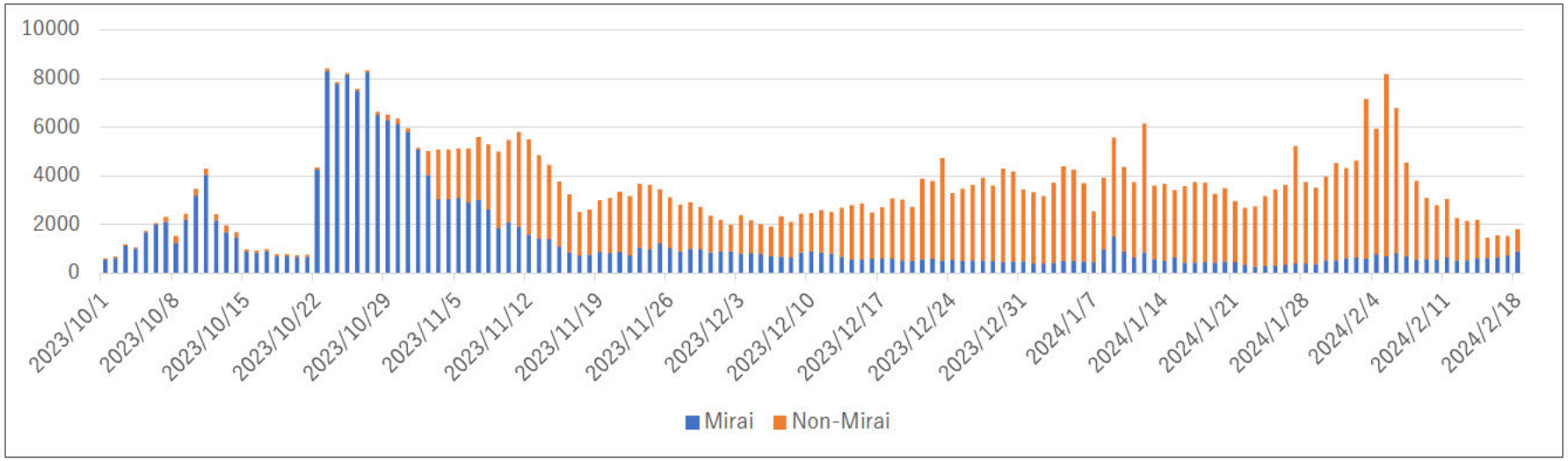

対象機器のHTTP Title[redacted]

[redacted]WebUI

# [参考] 経緯②：NICTER での当該機器のスキャンの観測

NATIONAL CYBER OBSERVATION CENTER

- **2023 年 10 月に NICTER において国内のマルウェア感染ホストの急増を発見**




23/TCP 宛の NICTER 観測アドレス数の推移

- ✓ 調査を進めたところ、感染端末の中に**本流量計が含まれていることが判明**

- **NICTER 解析チームにおいて、これらの感染ホストに対する機器調査を実施**
  - ✓ 結果として、2024 年 2 月 5 日時点で**流量計の WebUI にアクセスできる約 230 アドレス**を発見
  - ✓ 23/TCPへのスキャン(Miraiの特徴は持たない)
  - ✓ [redacted]観測したスキャンパケット数は多くは無い

# 新しい NOTICE における取り組み

# 新しい NOTICE 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**
  - ① ID/パスワード設定の脆弱性の調査 (特定アクセス調査)
  - ② **ファームウェアの脆弱性を有する機器の調査**
  - ③ **マルウェア感染機器の調査**

**[参考] 情報通信研究機構法の改正**
**(令和 6 年 4 月 1 日施行)**

- ✓ 時限設定の解除によるNOTICE 事業の継続的実施へ
- ✓ ファームウェアの脆弱性等が調査対象に
- ✓ 特定アクセス等実施業務の一部の外部委託が可能に

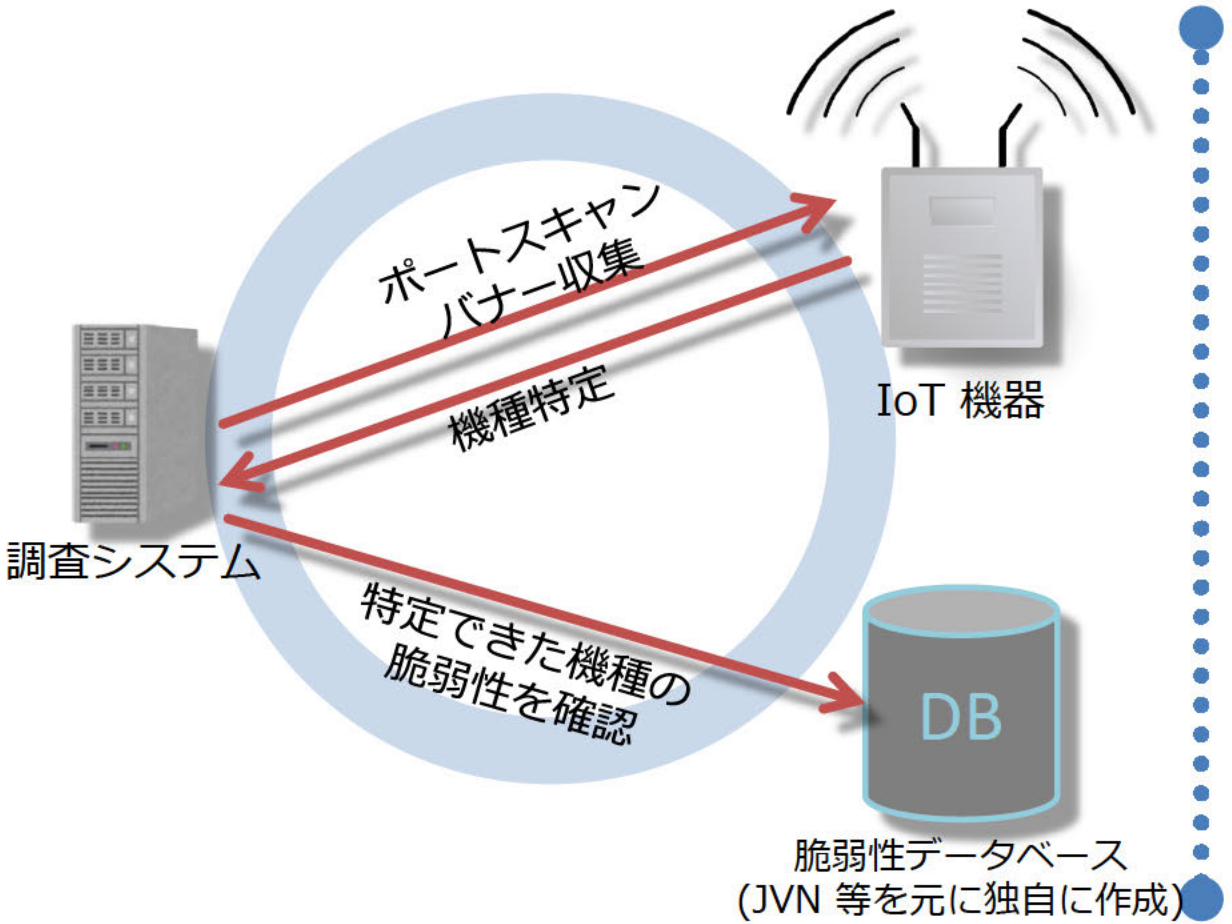
# ファームウェア脆弱性調査

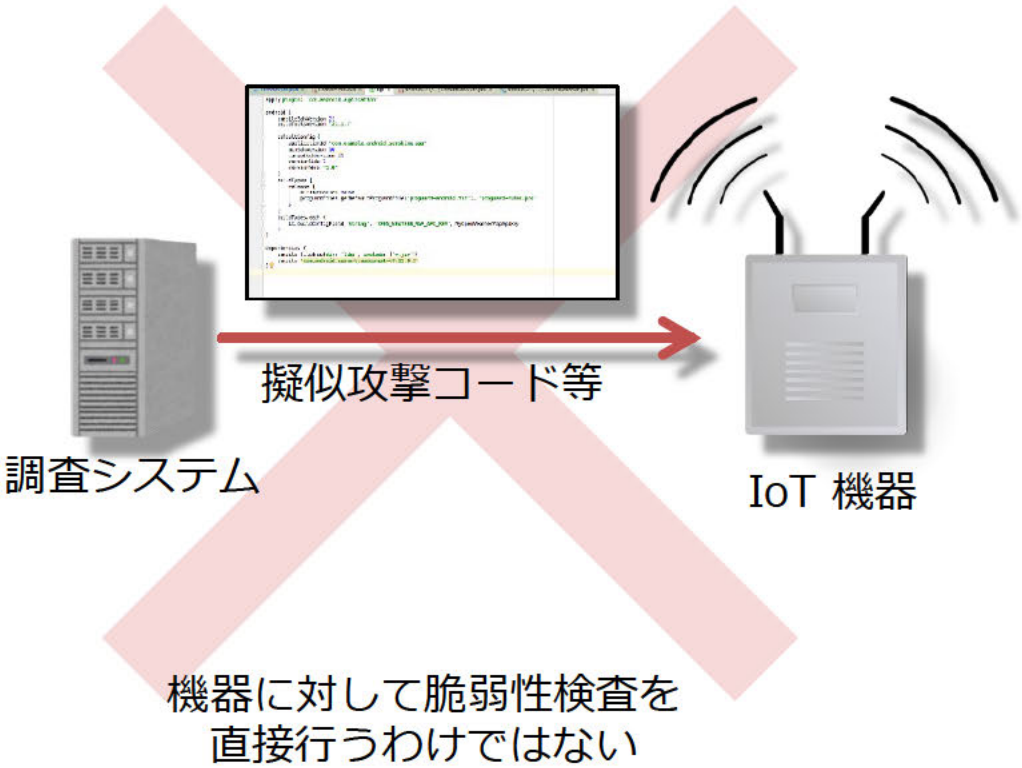
NATIONAL CYBER OBSERVATION CENTER

- **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を実施**
  - ✓ 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
  - ✓ 優先的に対処すべき脆弱性を抽出した上で調査を実施

# ファームウェア脆弱性の調査とは

- 機器に対して**脆弱性検査を直接行うわけではない**
- 調査により機種が特定できた機器について、**既知の脆弱性があれば通知**を実施



# 脆弱性の選定基準

- 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。
- 以下で例示する選定基準に基づいて、脆弱性を選定。
  - 選定基準の順番は目安。優先順位を示すものではない。
  - 以下はあくまで例示であり、ISP 等からのフィードバックや、社会情勢の変化等に応じて適宜見直す。

| # | 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<br>• OSコマンドインジェクションの脆弱性を有するもの<br>• 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<br>• NICTER のハニーポットで検知<br>• CISA KEV (Known Exploited Vulnerabilities Catalog) 等に掲載されているもの |
| 5 | NICT によるファーム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 |

# 今後の NCO の業務の方向性

# CURE の活用による高度分析情報の提供

NATIONAL CYBER OBSERVATION CENTER

**通知対象組織 (通信、重要インフラ事業者等) 向けの高度分析情報提供基盤を構築**

- ✓ 特定アクセス調査、ファームウェアの脆弱性調査等によって得られた情報に加え、サイバーセキュリティ研究所が運用するセキュリティ情報融合基盤 “CURE” を活用
- ✓ 各組織が管理する IP アドレスにおける攻撃関連情報や、機器が保有する脆弱性情報等、各組織におけるセキュリティ対応に資する情報をリアルタイムに提供

**イメージ図**

- ✓通知対象組織の IP アドレス帯に限定して情報提供
- ✓個別の IP アドレスについて、設定期間におけるイベント情報 (次頁) を提供

# 重要施設を対象としたアタックサーフェス調査の実施

NATIONAL CYBER OBSERVATION CENTER

- **国内の重要施設に設置されている IoT 機器を対象とした調査と注意喚起**
  - ✓ NOTICE における ISP 等との既存の連携に加えて、特に**社会的な影響の大きい重要施設の管理組織**と連携することで、調査の精度や注意喚起の効果の向上を期待
  - ✓ 重要施設の管理組織における IoT 機器に関する情報に基づき、**外部から攻撃可能な脆弱性や ID／パスワード脆弱性等のアタックサーフェス調査**を行い、注意喚起を実施
- **重要施設における IoT 機器を対象とした調査の実施に向けて**
  - ✓ 総務省をはじめ各セクターの情報共有分析センター (ISAC) 等との連携を前提として、情報共有や注意喚起の流れの整理等、事業の**体制づくりから推進することが必要**
  - ✓ 調査対象の拡大により調査・分析に係る業務の増加が見込まれることから、**NICT の人員体制の強化**をより一層進めることが必要

# おわりに

NATIONAL CYBER OBSERVATION CENTER

- **NOTICE 事業のこれまで**
  - ✓ HTTP(S) フォーム認証を新たに追加し、各種プロトコルでの調査を実施
  - ✓ 複数の事例を通じて本取り組みの有効性を確認
    - 脆弱な機器の発見を通じてサイバー攻撃の発生を未然に抑制
  - ✓ 機器ベンダーとの直接の連携による対処を実施

- **NOTICE 事業は新たなフェーズへ**
  - ✓ 脆弱なパスワードが設定された機器の調査 (特定アクセス調査) は継続
  - ＋ ファームウェアの脆弱性を有する機器の調査
  - ＋ NICTER を活用した**既感染端末**の探索
  - ＋ 調査依頼に基づく調査

- **より安全な IoT 環境の実現に向けて**
  - ✓ 日本国内におけるサイバー攻撃に悪用されるおそれのある機器の低減
  - ✓ NCO の観測体制と情報発信力の強化