

新しい NOTICE の船出

ー国内の IoT セキュリティの最新状況ー

2025/02/21

NICT サイバーセキュリティシンポジウム 2025



NATIONAL CYBER
OBSERVATION CENTER

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ーベーションセンター (NCO)
研究センター長 衛藤 将史

2024 年 4 月に再出発した**新しい NOTICE** における具体的な取り組みを紹介します。新たに業務として位置づけられたファームウェア脆弱性調査、マルウェア感染端末調査等に触れつつ、それらの調査で明らかになった国内の IoT セキュリティの最新状況を報告します。

1. NOTICE プロジェクトについて

- ✓ NOTICE における NICT の調査業務

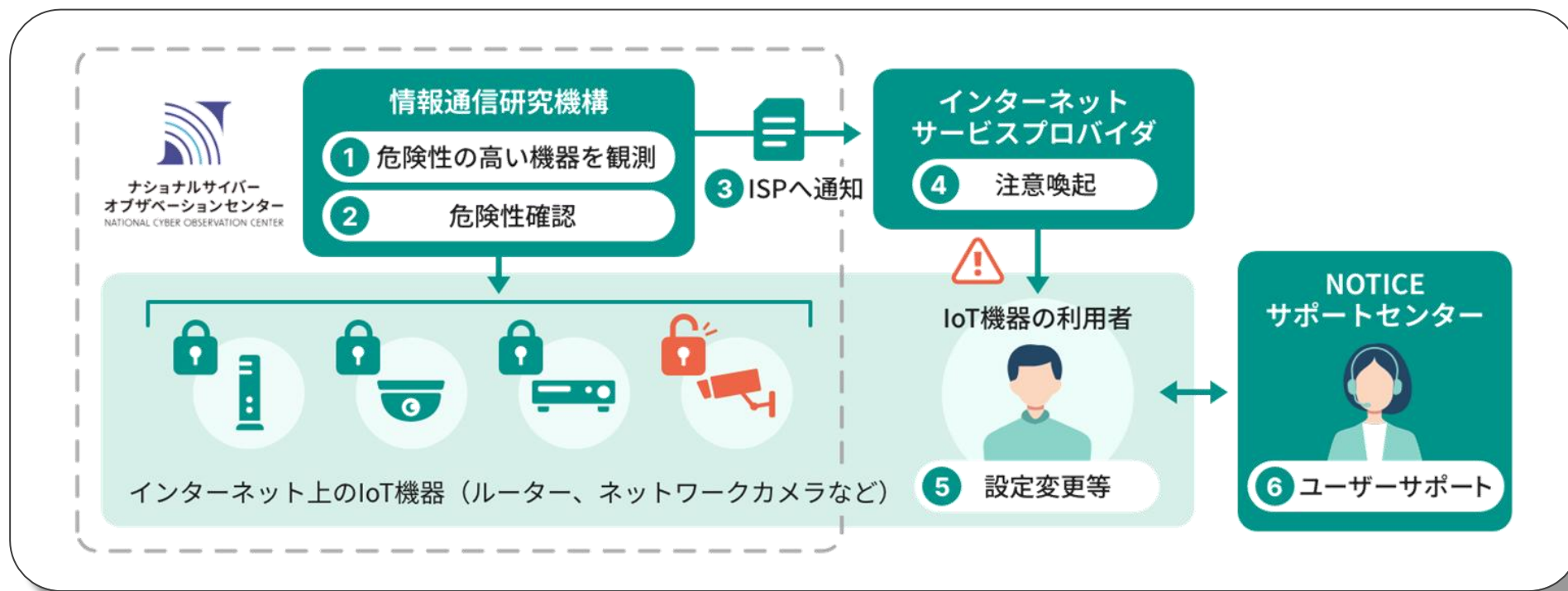
2. NOTICE における調査方法と調査事例

- A) ID・パスワード脆弱性調査
- B) ファームウェア脆弱性調査
- 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機器の調査

3. おわりに

NOTICE プロジェクトについて

- 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/>

●サイバーセキュリティ対策助言等業務

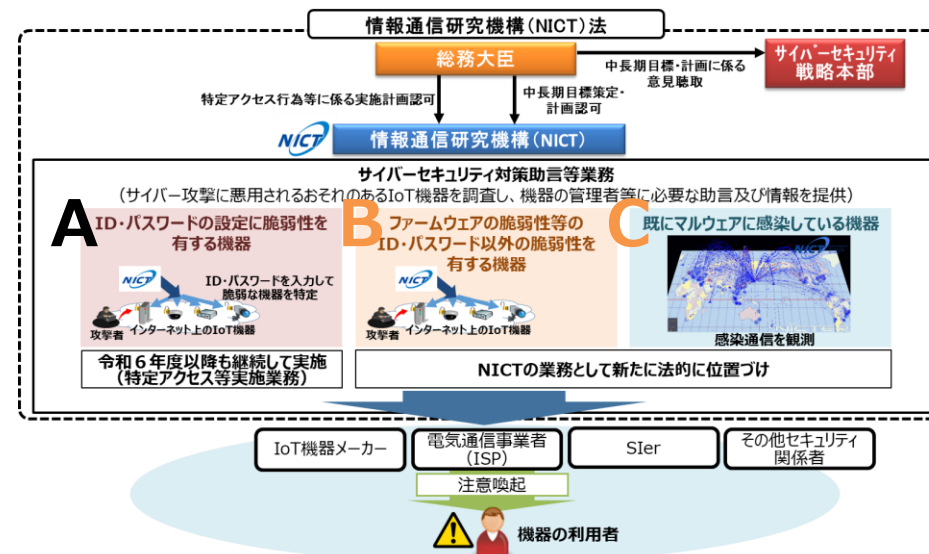
A)ID/パスワード設定の脆弱性の調査 (特定アクセス調査) ← 2019 年度開始

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)



産業界との連携をより一層強化

● 2024 年度よりベンダ部会を立ち上げ、産業界と連携した取り組みを強化

- ✓ 脆弱性情報、攻撃情報等の早期共有による対処の迅速化
- ✓ 機種情報等の共有による調査精度の向上



参加組織

述べ 94 社

NOTICEの取り組みに参加している会社・団体の数

ISP
85 社

IoT 機器メーカー
6 社

Sler
1 社

団体
2 団体

I-O DATA

PRO

Orchestrating a brighter world
NEC

ELECOM

BUFFALO™

YAMAHA

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)

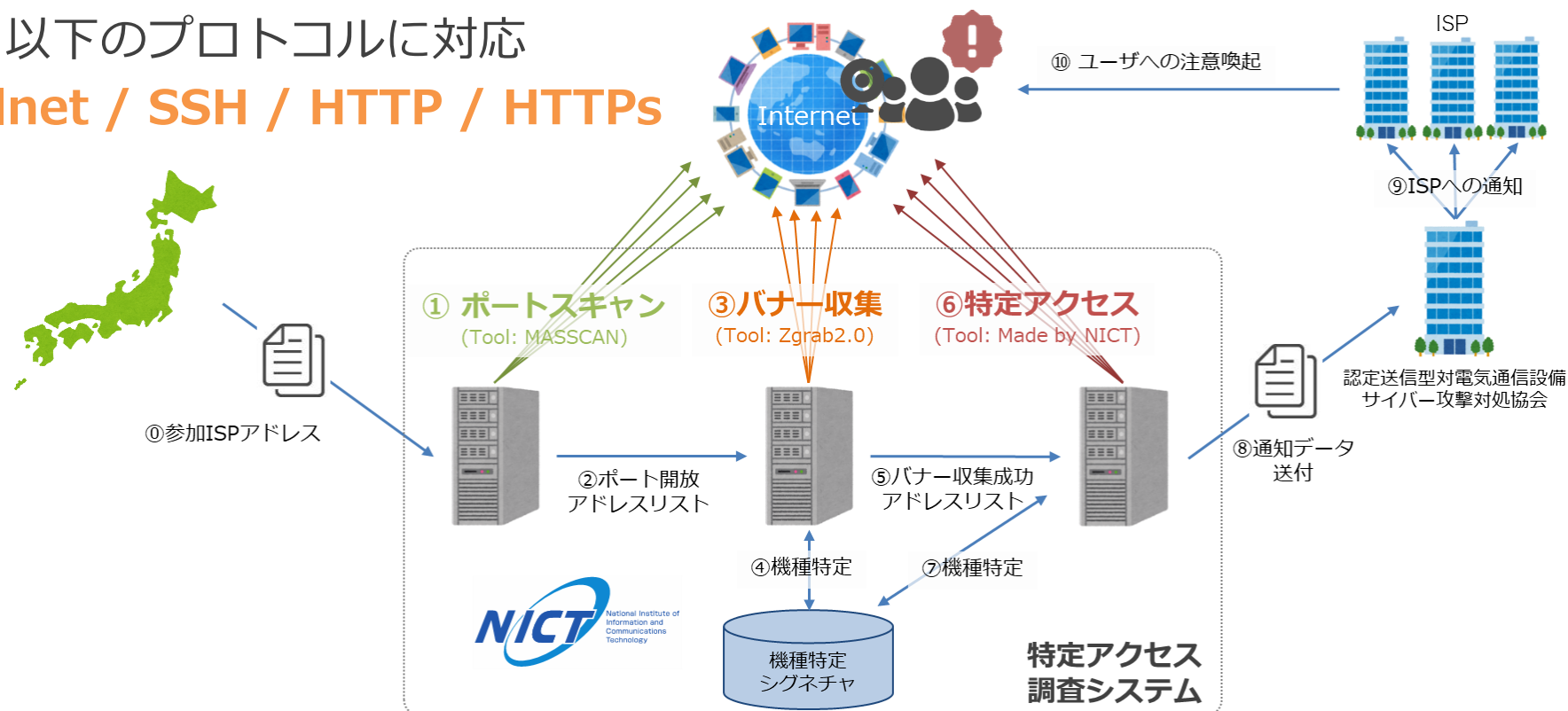
● 2019年2月20日より特定アクセス調査と通知業務を開始

✓ 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**



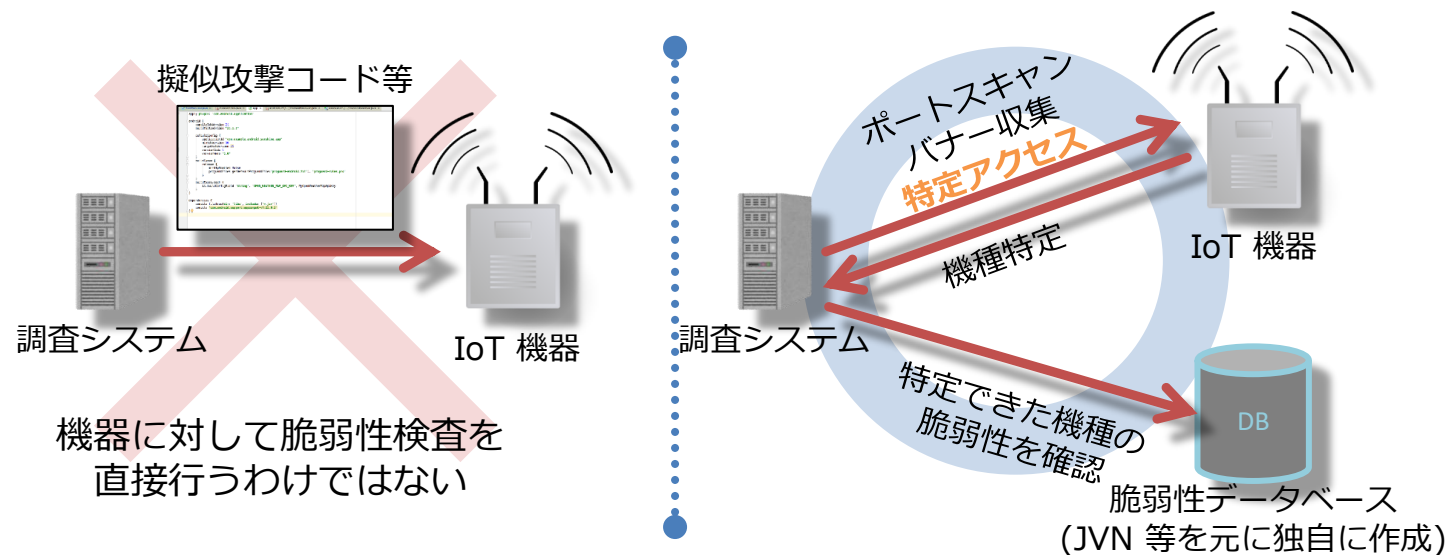
B) ファームウェアの脆弱性を有する機器の調査

● 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



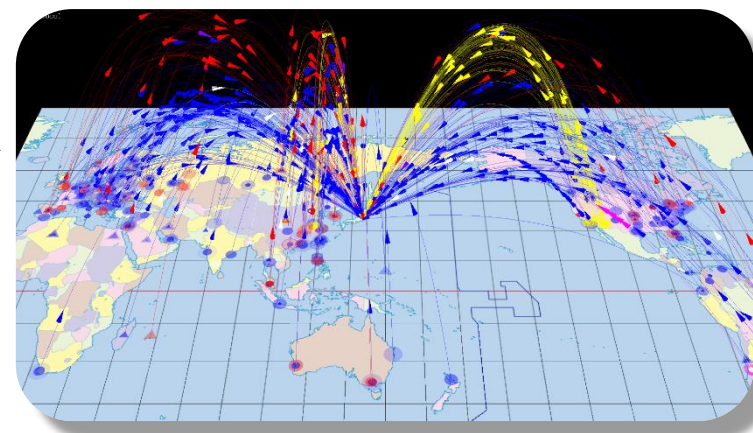
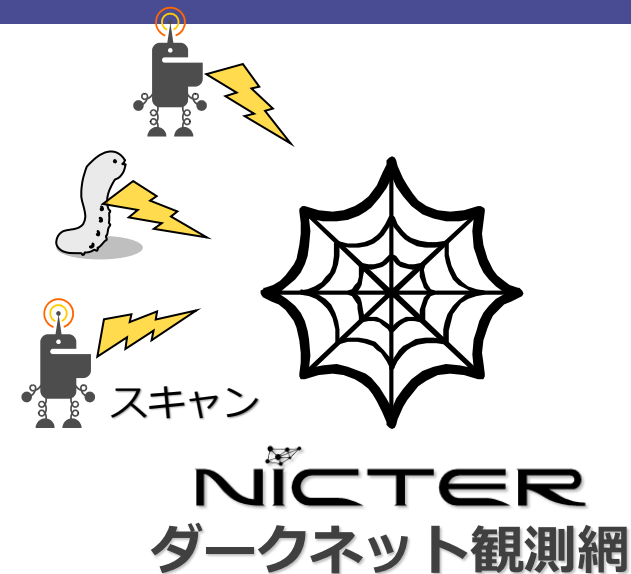
C) マルウェア感染機器の調査

●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

●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



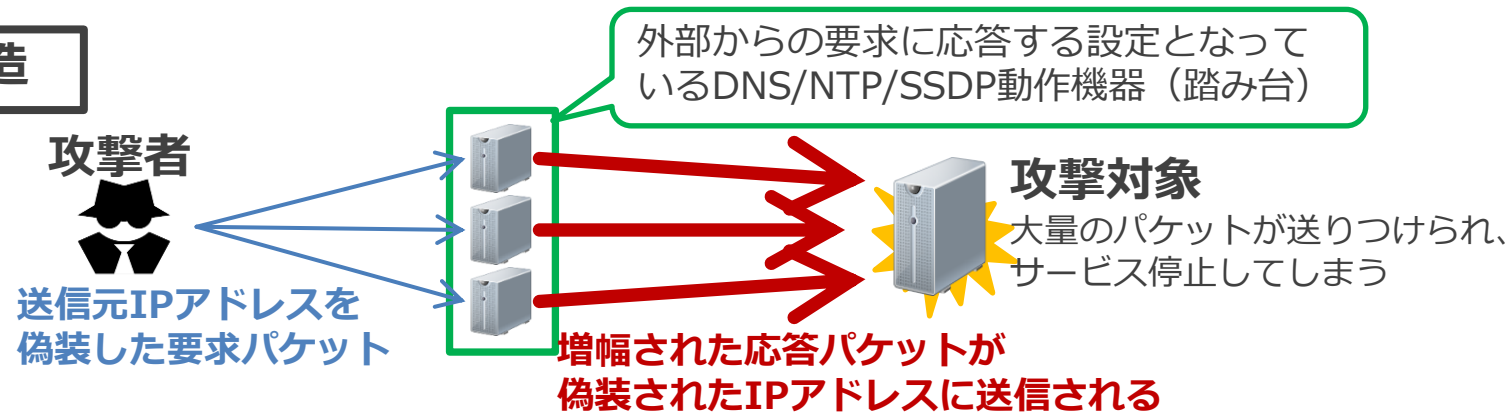
NICTER における
ダークネット観測のイメージ

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

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 (2024 年 12 月度)



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

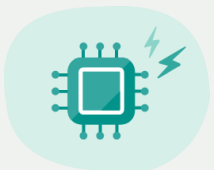
月 14,665 件※



- ・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 4,399 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 1,929 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 16,097 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)

某社製モバイルルータ宛の攻撃

● 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、当該ルータか判定
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**

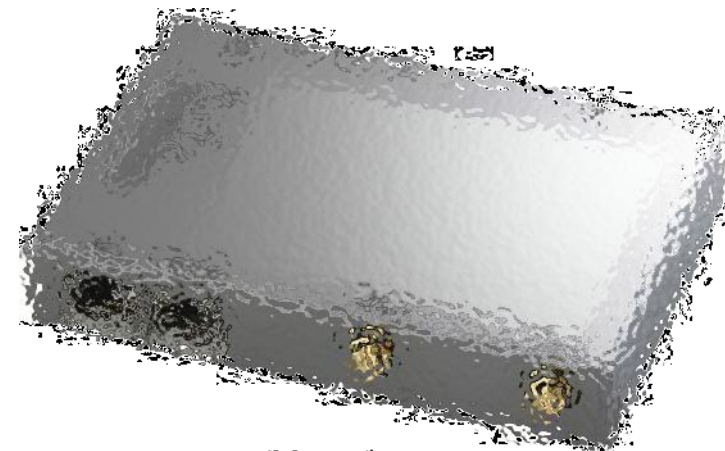
● 特定アクセス調査による当該端末の特定

- ✓ 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同社製モバイルルータを多数検知※ (右表)。

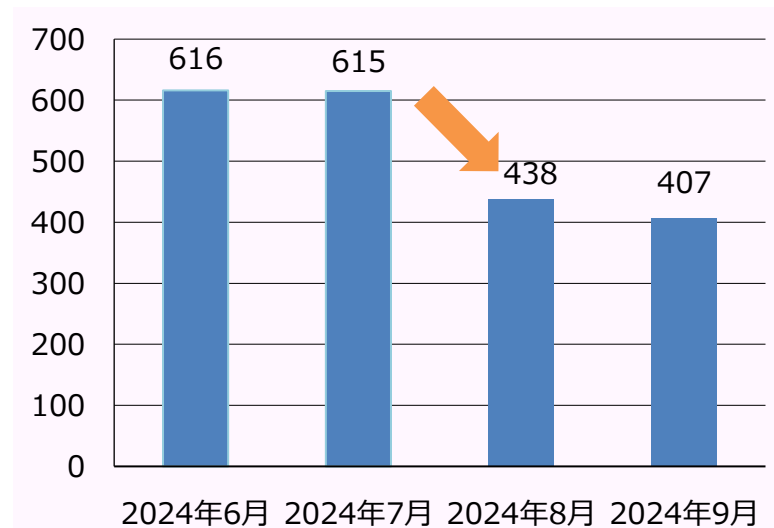
※HTTP での検知数



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



某社製モバイルルータ

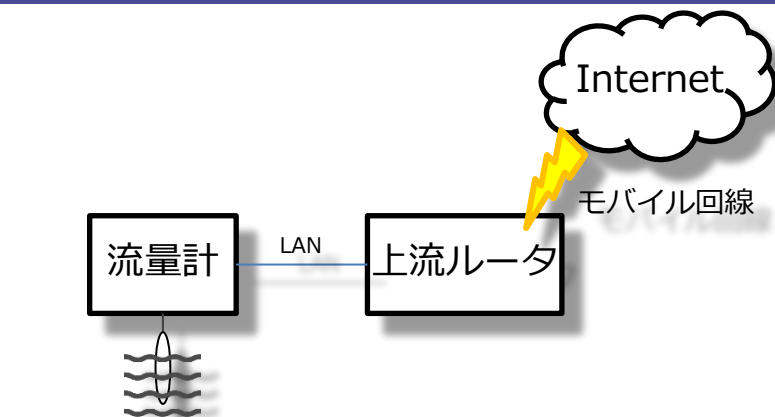


攻撃観測当初における同社製機器への
特定アクセスの成功件数 (HTTP)

脆弱な流量計機器の発見と対処

● 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

ISP・ベンダ等との連携による対処

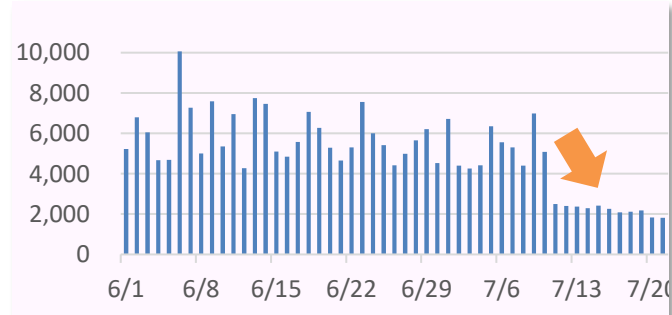
- ISP や製品ベンダと連携した対処により、**新たな脆弱性の発見や、対象とする脆弱性に関して顕著な観測数の減少を確認**

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**



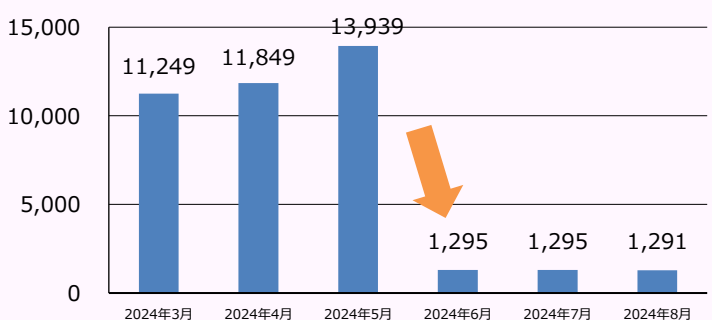
マルウェアからの感染拡大通信の観測数 (NICTERによる観測)

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**



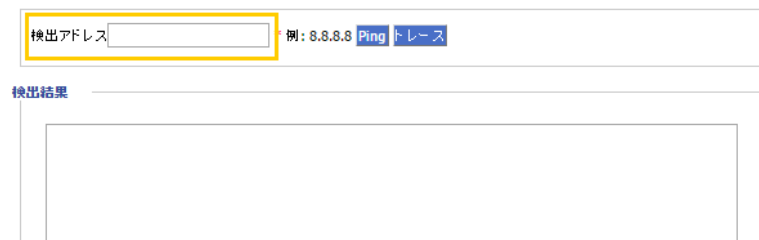
NOTICE による当該ルータの観測数

国内ベンダ製モバイルルータ

主な用途：業務用機器をインターネットに接続するための法人向け装置

脆弱性詳細：標準で guest ユーザーが存在。guest ユーザーでのログイン後に**ネットワークテスト機能**からコマンドインジェクション攻撃を実施可能

NICTER での攻撃観測を起点として当該ベンダとの連携の下、実機の挙動解析を行い**新たな脆弱性を発見**。CVE の登録を行うとともに NOTICE での注意喚起を開始。



検索アドレス 例: 8.8.8.8 Ping トレース

検索結果

ネットワークテスト機能

● NOTICE の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」のようにロングテール**で残り続ける脆弱機器への対処が課題

セキュリティ対策を行わずに
IoT機器を放置すると
気づかぬうちに乗っ取られること



適切に定期的にIoT機器を管理すれば
ボットネットによる被害は予防できる

安全な管理ができているかのチェック項目

設置時



1 推測されにくい複雑な管理者パスワードに変更してください



2 ファームウェアが最新版でない場合はアップデートしてください



3 使用しない機能や設定は無効にしてください

定期的



4 ファームウェアが最新版でない場合はアップデートしてください



5 サポートが終了したルーターやネットワークカメラは
買い替えをご検討ください

推測されにくい複雑な管理者パスワードに変更してください

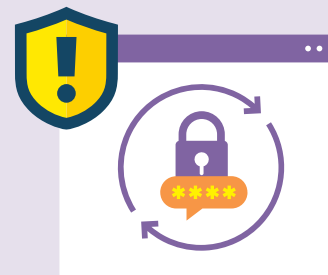
IoT機器に設定されている初期管理者パスワード情報は、マニュアルなどに記載され、
またインターネット上にも公開されていることがあります。

以下の例を参考に、管理者パスワードを変更しましょう。

管理者パスワードは、10桁以上で英大文字小文字、数字、記号を含み、名前や誕生日
などを避けた他人に推測されにくいものにしてください。

推測されにくい強い管理者パスワードの3つの条件

- ① 英大文字小文字、数字、記号を含む
- ② 10桁以上
- ③ 推測されにくいフレーズ



引用元：NISC「インターネットの安全・安心ハンドブックVer 5.00」

ファームウェアが最新版でない場合はアップデートしてください

装置を制御する内蔵プログラムのことを「ファームウェア」と呼びます。
ファームウェアに脆弱性が発見されると、修正プログラムがメーカーのウェブサイトで公開されることがあります。IoT機器の説明書などを参考に、
メーカーのウェブサイトにファームウェアの最新版があるかを確認し、
常に最新の状態を保ってください。

アップデート方法は一般的に以下があります。

- | | |
|-------------|--------------------------|
| ① ウェブサイトを確認 | ③ (1)アップデートツールを利用する場合 |
| ② マニュアルを参照 | ③ (2)ネットワーク経由でアップデートする場合 |
| ③ アップデートの実施 | |

ファームウェアの「自動アップデート」が可能なルーターや
ネットワークカメラを購入することを推奨します。
自動アップデート機能は、必ず「有効」にしてください。

使用しない機能や設定は無効にしてください

スマホやパソコンを使用して、**外出先からインターネットを経由して管理機能**を操作できるルーターやネットワークカメラがあります。これらの機能を普段使用しない場合は、第三者から操作されることが起きないようにその機能を無効にするなどの対策が必要です。具体的には、ルーターやネットワークカメラの設定で使用していない機能が有効になっていないかをマニュアルや管理画面で確認し、もし有効であればその機能を無効にしてください。

設定の変更方法

1. 使用しない機能の無効化（SSH/Telnet接続等の無効化）

マニュアルを参照して、ルーターやネットワークカメラの管理画面を確認してください。インターネットから設定変更を行うことができる機能や、動作状況を確認できる機能が有効になっていることがあります。これらの機能を使う必要がない場合は、設定を変更して無効化しておきましょう。

2. 使用する機能のアクセス制限

インターネット側から管理機能を利用する必要がある場合は、これらの機能を第三者に利用されないよう、対策してください。アクセス元を必要最小限に制限する、推測されにくい管理者パスワードに設定するなどの対策をしておきましょう。

万が一、不審な設定があった場合は、第三者がルーターやネットワークカメラに侵入している可能性があるため、直ちに初期化を行い、**ファームウェアを最新版にアップデートし、管理者パスワード変更を実施**しましょう。

ご清聴ありがとうございました

詳細はNOTICE Web サイトへ :
<https://notice.go.jp/>

