IoT は増え続けるのに、なぜセキュリティは追いつかないのか
― 日本国内 IoT 機器調査とオブザベーションセンターの役割 ―

サイバーセキュリティシンポジウム2026

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

高嶋 香織

NICT

NATIONAL CYBER OBSERVATION CENTER

NICT サイバーセキュリティ研究所

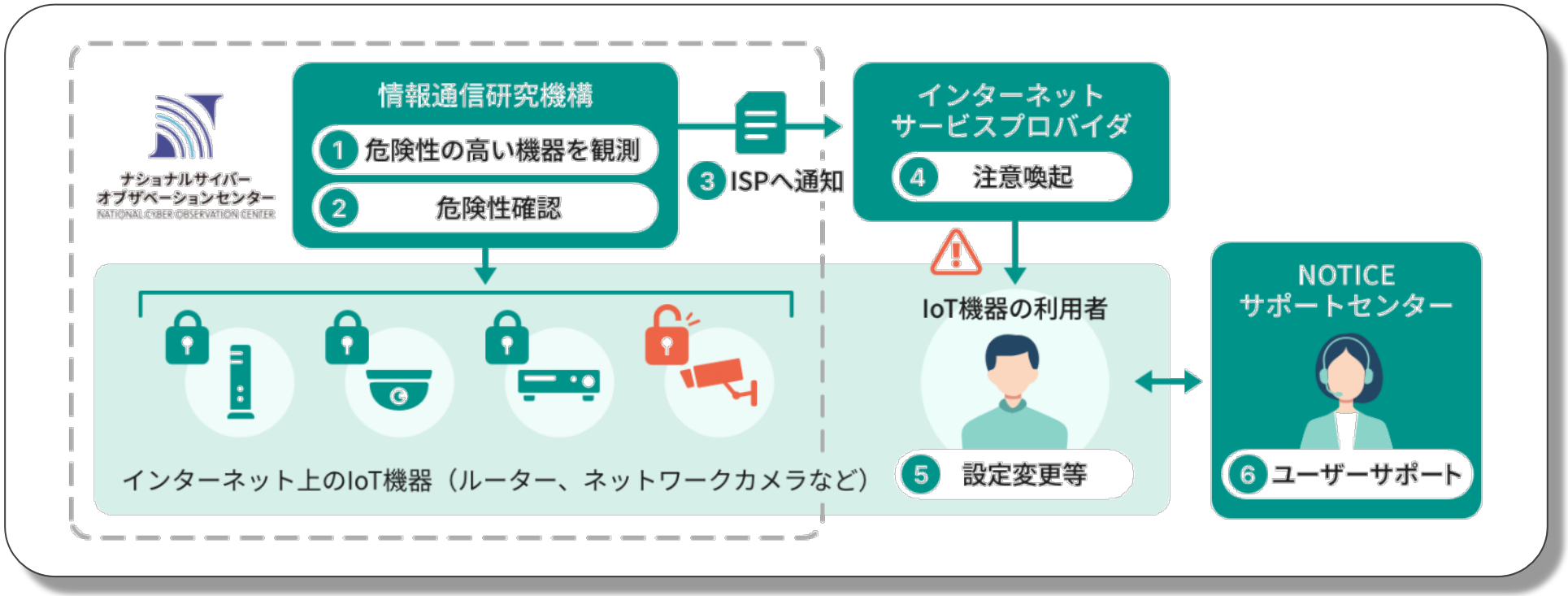
NATIONAL CYBER OBSERVATION CENTER

CYBERSECURITY Research Institute
サイバーセキュリティ研究所
（CSRI）

CYBERSECURITY Laboratory	SECURITY FUNDAMENTALS Laboratory	National Cyber Training Center	NATIONAL CYBER OBSERVATION CENTER	CYNEX CYBERSECURITY NEXUS	CREATE Center for Research on AI Security and Technology Evolution
サイバーセキュリティ研究室（CSL）	セキュリティ基盤研究室（SFL）	ナショナルサイバートレーニングセンター（NCT）	ナショナルサイバーオブザベーションセンター（NCOC）	サイバーセキュリティネクサス（CYNEX）	AIセキュリティ研究センター（CREATE）
攻撃観測分析・対策研究	暗号研究	セキュリティ人材育成	IoT機器セキュリティ対策	産学官連携拠点形成	AIセキュリティ研究

NOTICEプロジェクト　第1期　2019.02~

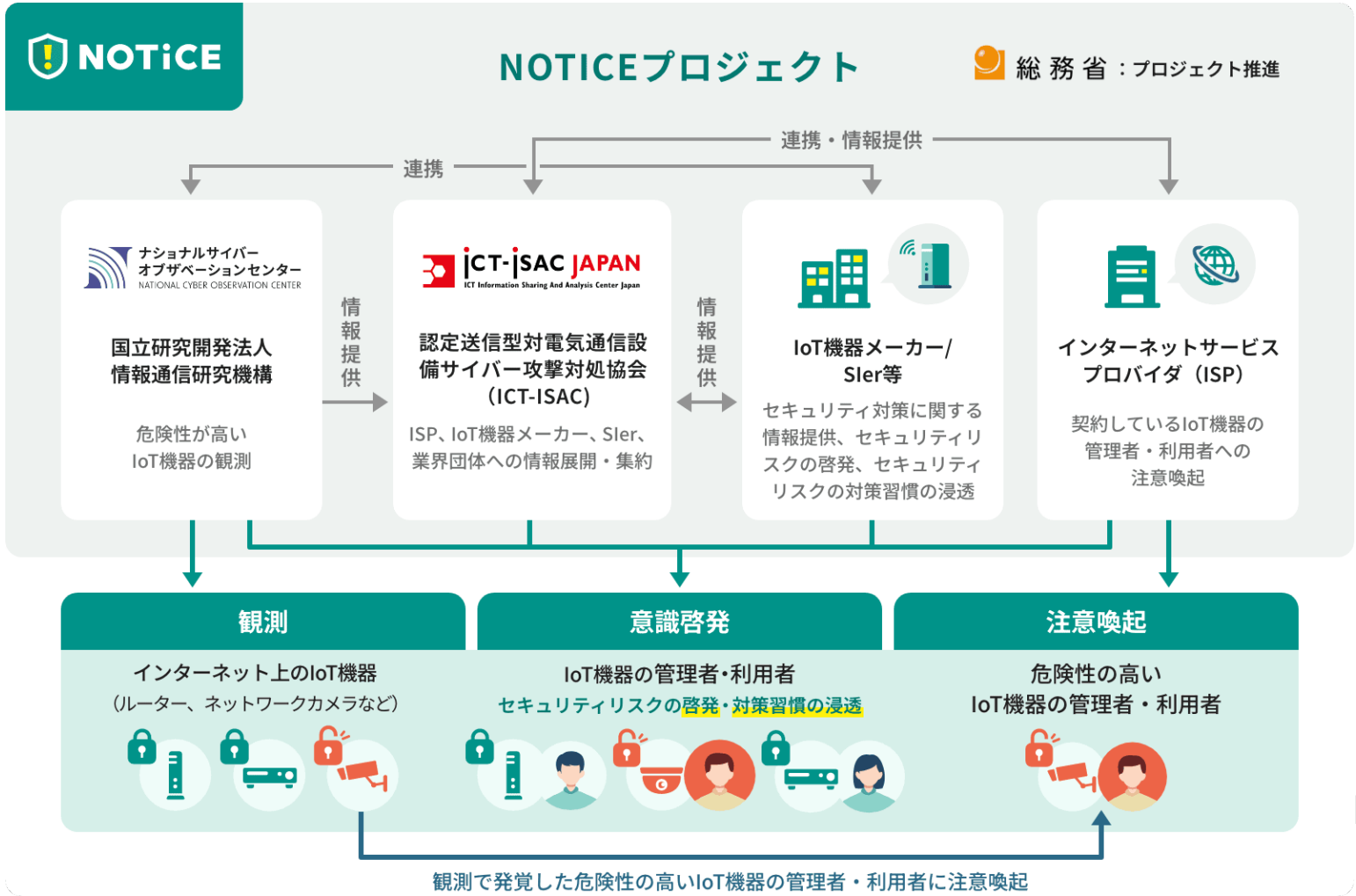
- NOTICE: National Operation Towards IoT Clean Environment
- 総務省、NICT、ISPが連携し、IoT 機器のセキュリティ対策向上を推進することにより、サイバー攻撃の発生や、その被害を未然に防ぐためのプロジェクト



https://notice.go.jp/

NOTICEプロジェクト 第2期 2024.04～

- 新たにIoT機器メーカーやSIerとも連携し、
  意識啓発等のIoT 機器のセキュリティ対策向上を推進



https://notice.go.jp/

NOTICE参加組織数 2025年12月現在

NATIONAL CYBER OBSERVATION CENTER

参加組織

述べ 110 社

NOTICEの取り組みに参加している会社・団体の数

ISP

96 社

IoT 機器メーカー

10 社

SIer

2 社

団体

2 団体

NOTICE プロジェクトにおける NICT の役割

NATIONAL CYBER OBSERVATION CENTER

●サイバーセキュリティ対策助言等業務

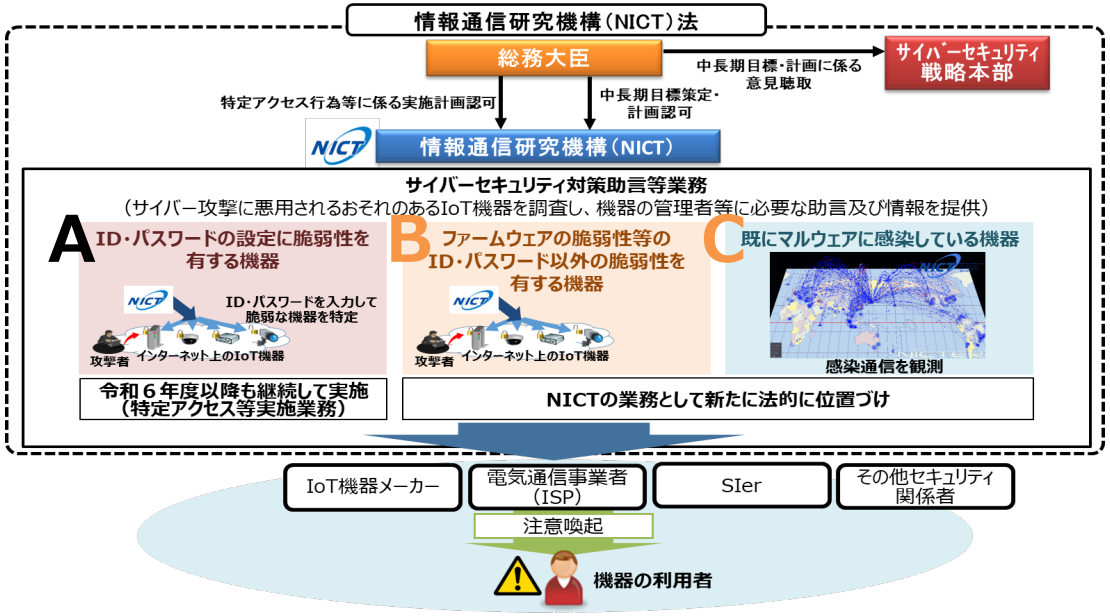
A)ID/パスワード設定に脆弱性を有する調査 (特定アクセス調査) ← 2019 年度開始

B)ファームウェアに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)



IoT 機器調査及び利用者への注意喚起の実施状況 (2025 年 12 月度)

NATIONAL CYBER OBSERVATION CENTER

IoT機器観測総数

月1.17億件

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13,796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2,536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328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。

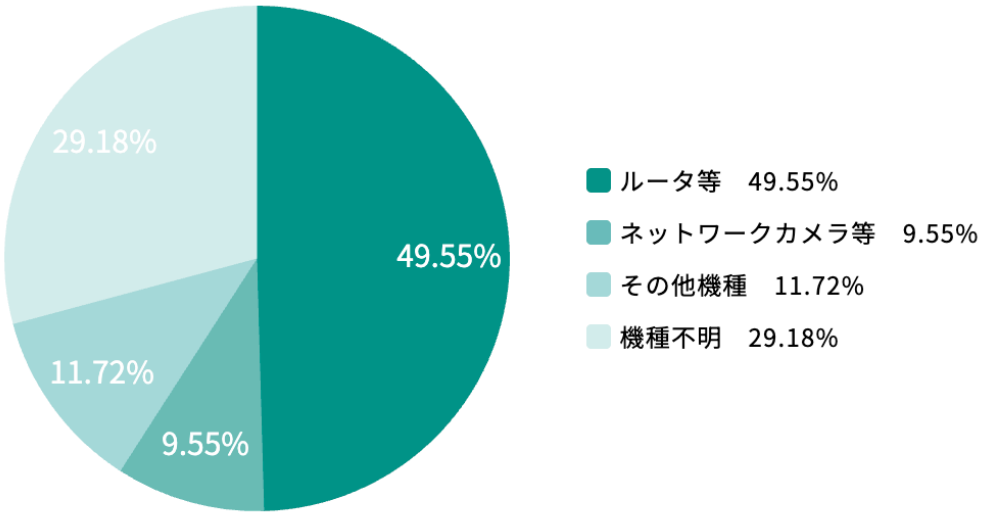
※IPアドレスが変動している場合は、重複して計上している場合があります
※当月1日あたりの最大値を掲載しています

D リフレクション攻撃の踏み台にされうるIoT機器

月15,077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機器だと検知した数

A 容易に推測可能なID・パスワードであるIoT機器の種類



ISP・ベンダ等との連携による対処

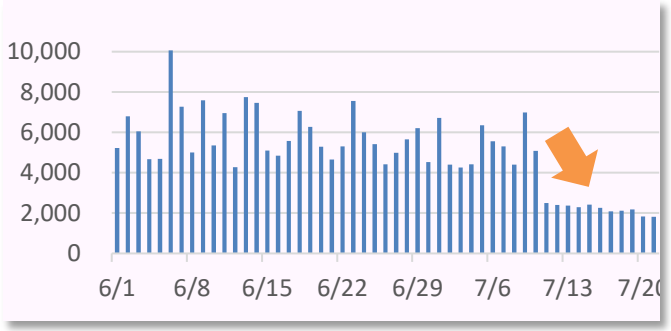
NATIONAL CYBER OBSERVATION CENTER

- **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**

C 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**

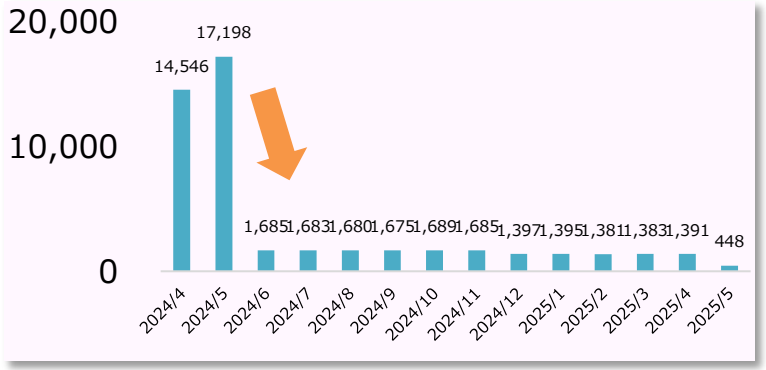


マルウェアからの感染拡大通信の観測数（NICTERによる観測）

B 海外ベンダ製壁埋め込み型ルータ

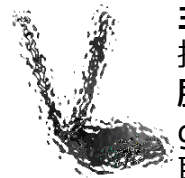
主な用途：家庭等において、インターネットに接続し、無線LAN等を提供するための機器
脆弱性詳細：脆弱性を有する管理画面がインターネットからアクセス可能な場合、管理画面に攻撃を行うことでルーターの悪用が可能になる。

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**



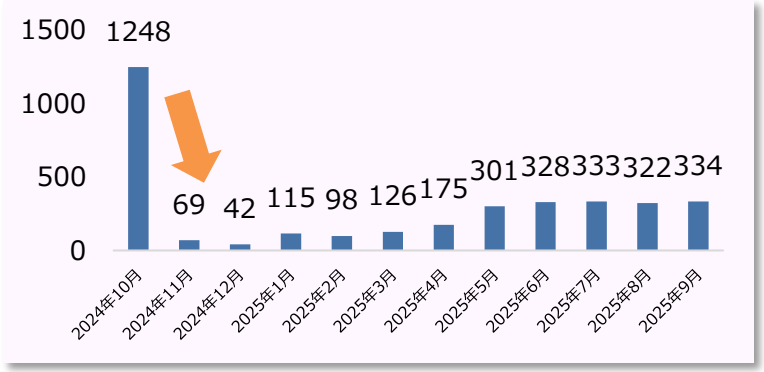
NOTICE による当該ルータの観測数

A&B&C 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 ユーザでのログイン後に管理者権限を取得し、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 の登録を行うと共に NOTICE での注意喚起を開始。



NOTICE による当該ルータの観測数

IoT機器調査におけるニーズ把握

NATIONAL CYBER OBSERVATION CENTER

- **NOTICE注意喚起から得た知見**
  - ✓ 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
- **観測数減少の主な理由**
  - 注意喚起によるユーザ対処
  - 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
- **ISPを通じたフィードバック**
  1. 法人ユーザは対応が早い。個人ユーザへは通知を届ける事が難しい
  2. 通知対象が何かわからないとユーザは対応出来ない
  3. ユーザは自宅の機器が脆弱だとは考えていない
  4. 対処方法が無い機器への通知は出来ない

  ✓ 番外として
  - インターネット側だけでなく、組織（家庭）の内側に対しての調査は可能か

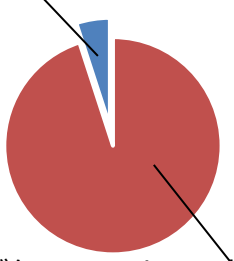
NOTICE 注意喚起を受領したユーザの認知・行動に関する調査

NATIONAL CYBER OBSERVATION CENTER

- **ユーザの行動調査を通じて、NOTICE注意喚起へのフィードバックを実施**

1. 注意喚起メール (NM) が気になった

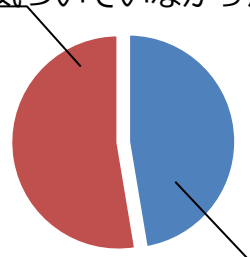
NMが気になった: **5%**



NM**以外**が気になった or 特に気になるメールがなかった: **95%**

2. 1. の 95% の内で NM に気づいてはいた

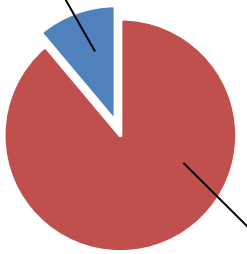
NMに気づいていなかった: **53%**



NMに気づいてはいた: **47%**

3. 2. の 47% 中、NMを迷惑メール/スパム or 自分に無関係なメールと思った

そうは思わなかった: **11%**

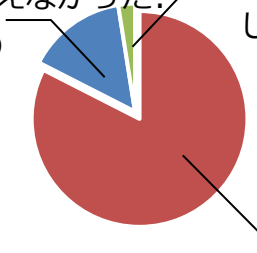


迷惑メール/スパム/無関係のいずれかと思った: **89%**

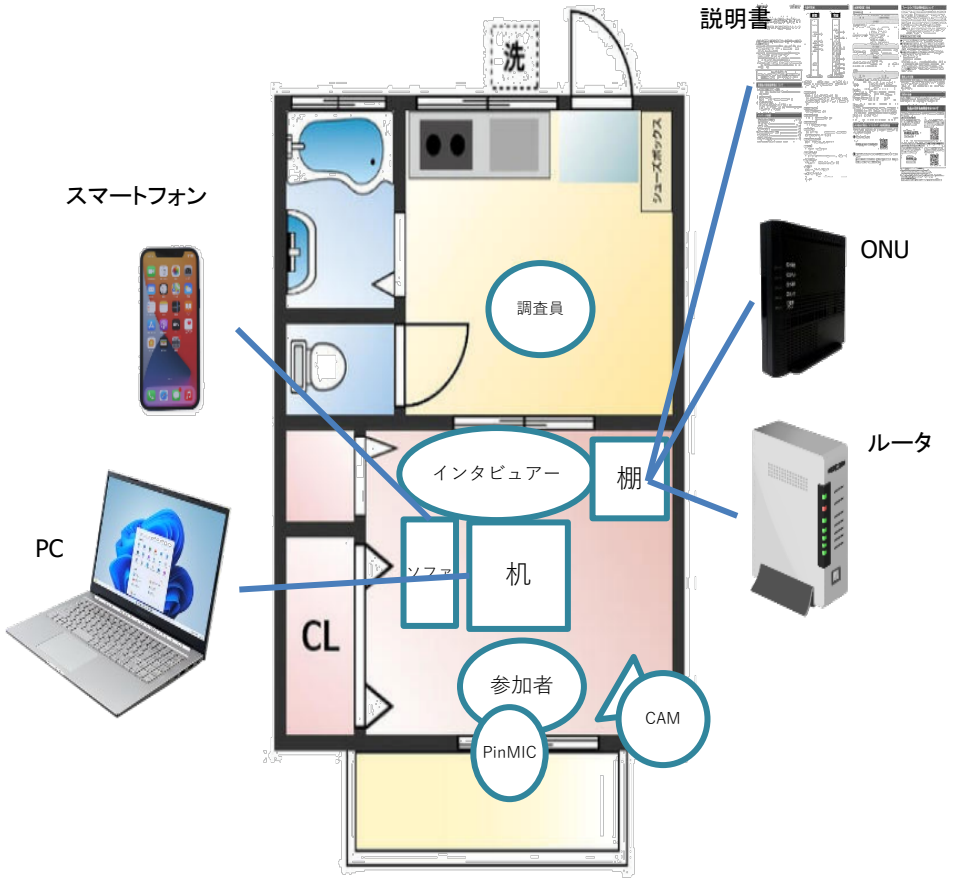
4. NMを読んでみて怪しいもしくはスパムと捉えた

怪しいもしくはスパムとは捉えなかった: **15%**

特に言及なし: **3%**



怪しいもしくはスパムと捉えた: **83%**

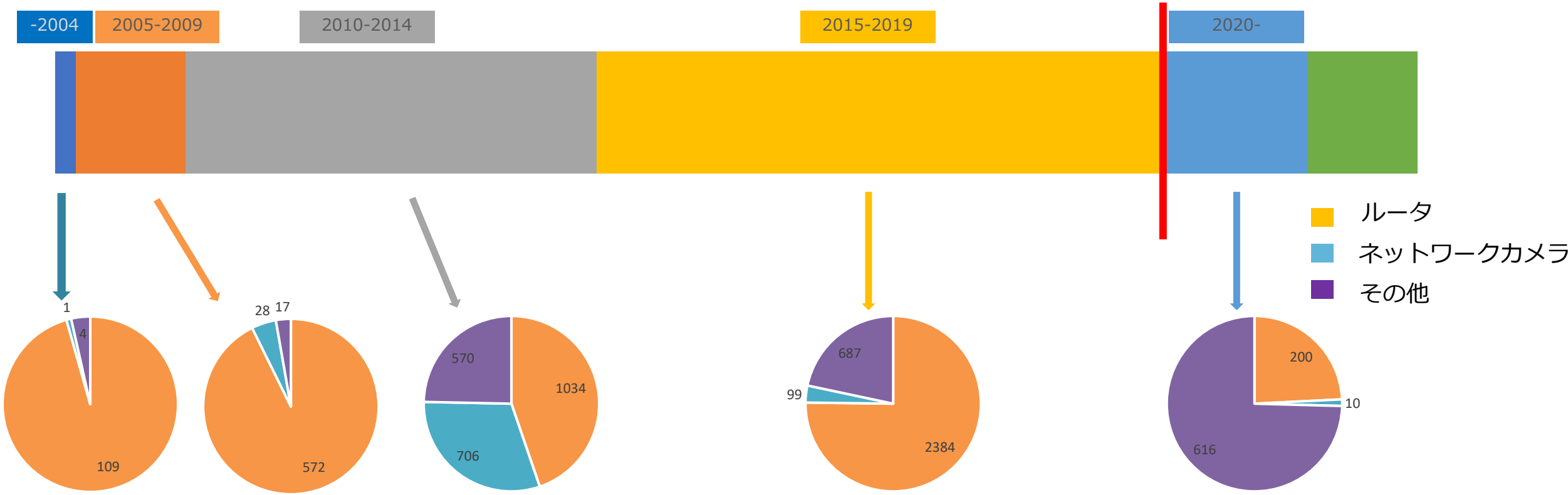


調査環境のイメージ

端末設備等規則のセキュリティ基準の実効性を証明

NATIONAL CYBER OBSERVATION CENTER

- 端末設備等規則のセキュリティ基準が令和元年 (2019 年) 施行
  (アクセス制御、ID・パスワードの適切な設定の促進、F/W の更新機能等)
- セキュリティ基準施行後の発売機器は10%未満



特定アクセス成功機器の発売年とそのカテゴリー一覧(2025/12データ, HTTP/HTTPS)

セキュリティ基準の見直しへの貢献

- **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**
  - ✓ **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

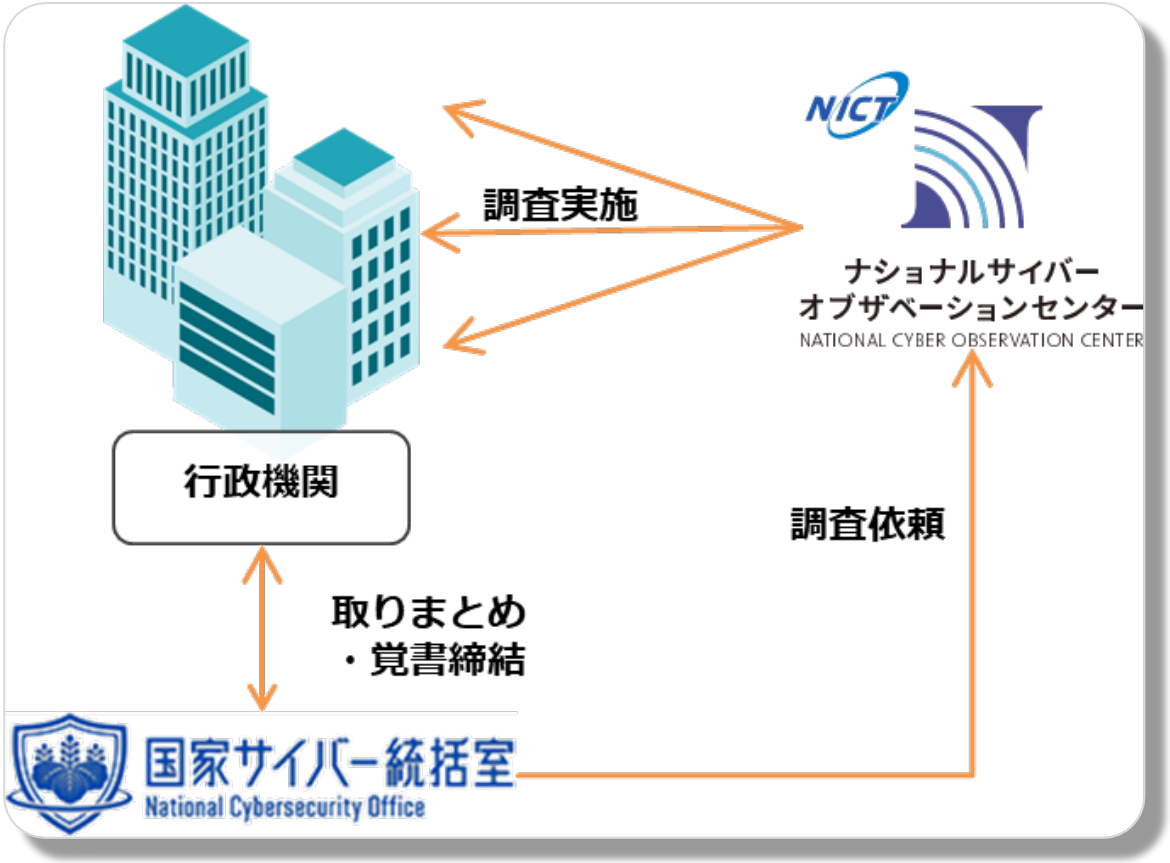
- **NICT からのセキュリティ基準の見直し案に基づく省令の改正に向けた作業を総務省において推進中**
  (IP ネットワーク設備委員会の報告書のとりまとめ)

NCO と連携し NOTICE をベースとした行政機関向け ASM の本格運用を開始

- **NCO による横断的 ASM 事業の一環として、NICT において NOTICE をベースとした行政機関向けASM サービス (NOTICE ASM) を令和 7 年度より正式サービスとして実施**
  - ✓ 各機関が保有する IP アドレスリストの提出を受け、NICT からスキャン調査を実施
  - ✓ 特定アクセス調査のノウハウ活用により、ASM 事業としては他にはない高精度な調査を実施

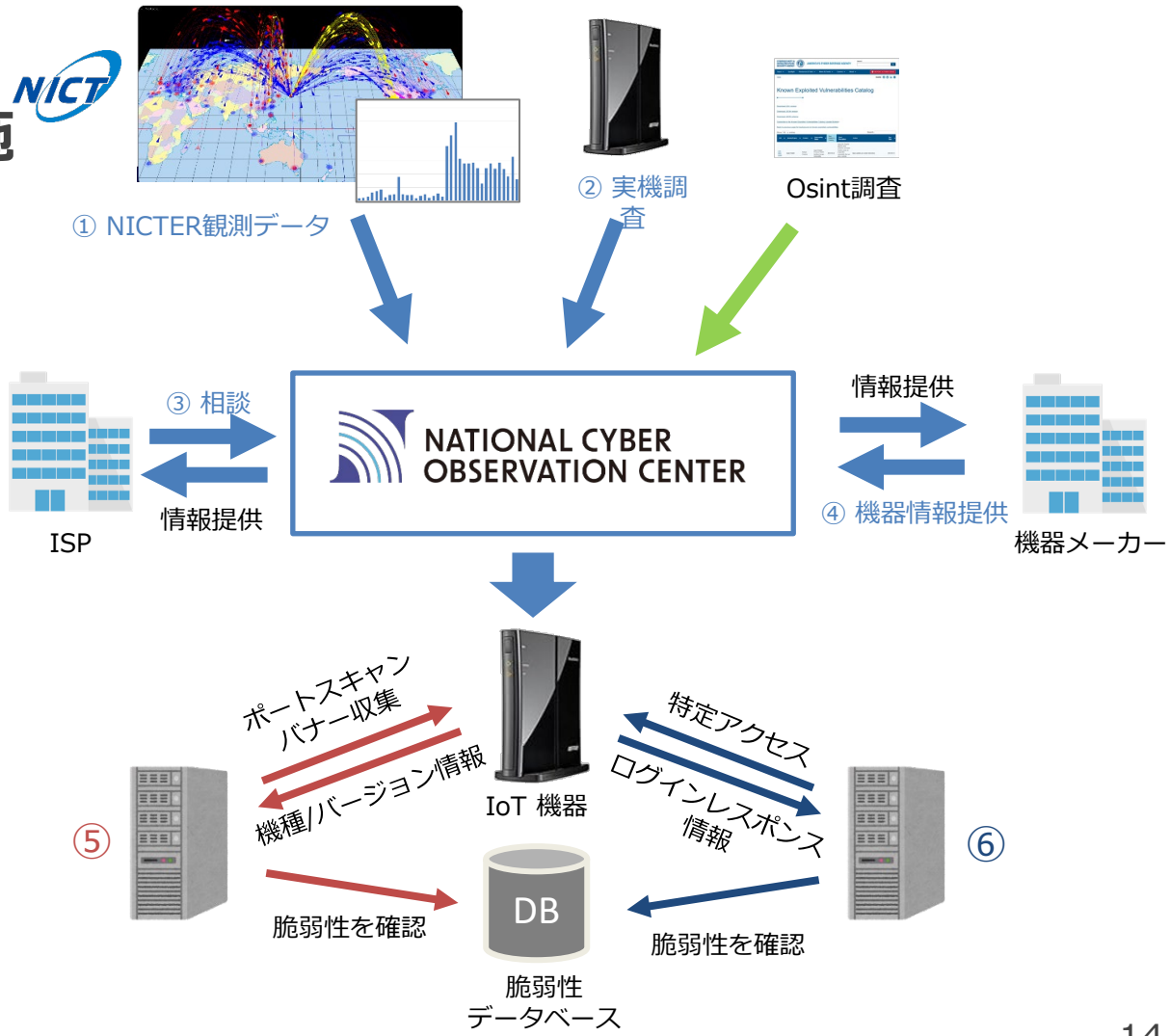
- **ASM調査では**
  - ✓ 調査対象との合意に基づく調査
  - ✓ 新たな脆弱性に関する試験的な調査を実施
  - ✓ 調査対象機関からのフィードバックに基づき機種情報等を収集

- **機種情報等の調査結果をNOTICE側にも反映**



調査手法の改良・拡大による調査能力の向上への取り組み

- **IoT機器の機種・バージョン情報等の特定が脆弱な機器対処への近道となる。**
- **調査能力の向上のために様々な調査を実施**
  - ✓ 実機を使用した調査
  - ✓ Osint情報を活用した調査
  - ✓ ステークホルダー/セキュリティ関連組織との連携による対策の促進



高度なセキュリティ助言・情報提供の推進を通じた、安心・安全な IoT 利用環境の実現

NATIONAL CYBER OBSERVATION CENTER

NOTICE
調査対象の拡大と円滑な調査実施

脆弱性を有する機器

サポート終了機器 等

NOTICE ASM

調査実施

ナショナルサイバーオブザベーションセンター
NATIONAL CYBER OBSERVATION CENTER

行政機関

調査依頼

取りまとめ・覚書締結

国家サイバー統括室 National Cybersecurity Office

事業成果向上のための実態把握・研究

注意喚起を受けたユーザの認知行動調査 等

ステークホルダーとの連携による対処能力の強化

JPCERT CC　IPA

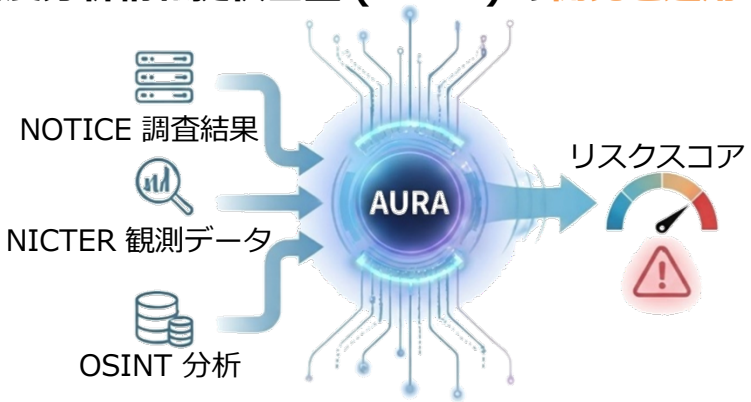
NICT NATIONAL CYBER OBSERVATION CENTER

脆弱性情報の共有
調査結果の共有 等

民間企業 (ISP 等)

総務省　国家サイバー統括室 National Cybersecurity Office

高度分析情報提供基盤 (AURA) の開発と運用



新たな調査分析手法 (SONAR) の研究開発と実用

- 機器の脆弱性調査
- 機器の設定状況の確認
- 製品サポート状況の確認
- マルウェア感染状況の確認

etc.

NOTICE ヘルスチェックサービス
(ネットワーク内部からの調査)

高度なセキュリティ助言・情報提供の推進を通じた、安心・安全な IoT 利用環境の実現

NATIONAL CYBER OBSERVATION CENTER

NOTICE
調査対象の拡大と円滑な調査実施

脆弱性を有する機器

サポート終了機器 等

NOTICE ASM

調査実施

ナショナルサイバーオブザベーションセンター
NATIONAL CYBER OBSERVATION CENTER

行政機関

調査依頼

取りまとめ・覚書締結

国家サイバー統括室 National Cybersecurity Office

ステークホルダーとの連携による対処能力の強化

JPCERT CC

IPA

NICT NATIONAL CYBER OBSERVATION CENTER

脆弱性情報の共有
調査結果の共有 等

民間企業 (ISP 等)

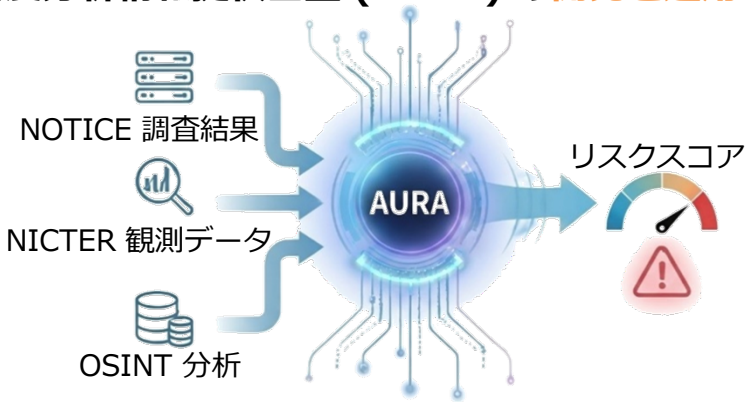
総務省

国家サイバー統括室 National Cybersecurity Office

事業成果向上のための実態把握・研究

注意喚起を受けたユーザの認知行動調査 等

高度分析情報提供基盤 (AURA) の開発と運用



新たな調査分析手法 (SONAR) の研究開発と実用

- 機器の脆弱性調査
- 機器の設定状況の確認
- 製品サポート状況の確認
- マルウェア感染状況の確認

etc.

NOTICE ヘルスチェックサービス
(ネットワーク内部からの調査)