より安全な IoT 環境の実現に向けて
– NOTICE 事業 5 年間の総括と今後の取り組み –

2024 年 2 月 16 日
NICT サイバーセキュリティシンポジウム 2024

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
研究センター長 衛藤 将史

NATIONAL CYBER
OBSERVATION CENTER

はじめに

NATIONAL CYBER OBSERVATION CENTER

1. NOTICE 事業の紹介と 5 年間の取り組み

- ✓ NOTICE 調査の仕組み
- ✓ 定期的な観測の実施状況
- ✓ 過去の対処事例

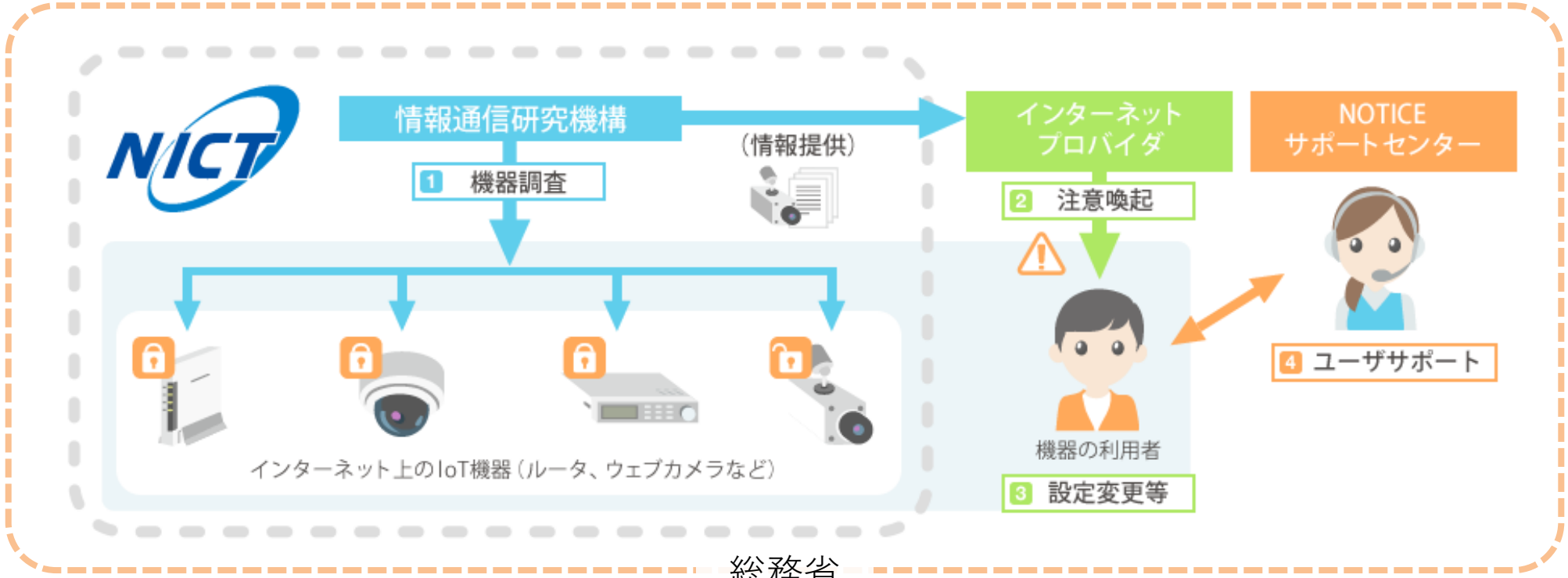
2. NOTICE は新たなフェーズへ

- ✓ 情報通信研究機構法の改正
- ✓ 今後予定されている新たな取り組み等

3. おわりに

NOTICEプロジェクト（2019年２月～）

- NOTICE: National Operation Towards IoT Clean Environment
- 総務省、NICT、ISPが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組



https://notice.go.jp/

NICT法による特定アクセス行為の規定

附則　第八条（業務の特例）

2　機構は、第十四条及び前項に規定する業務のほか、平成三十六年三月三十一日までの間、次に掲げる業務を行う。

一　特定アクセス行為を行い、通信履歴等の電磁的記録を作成すること。

二　特定アクセス行為に係る電気通信の送信先の電気通信設備が次のイ又はロに掲げる者の電気通信設備であるときは、当該イ又はロに定める者に対し、通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと。

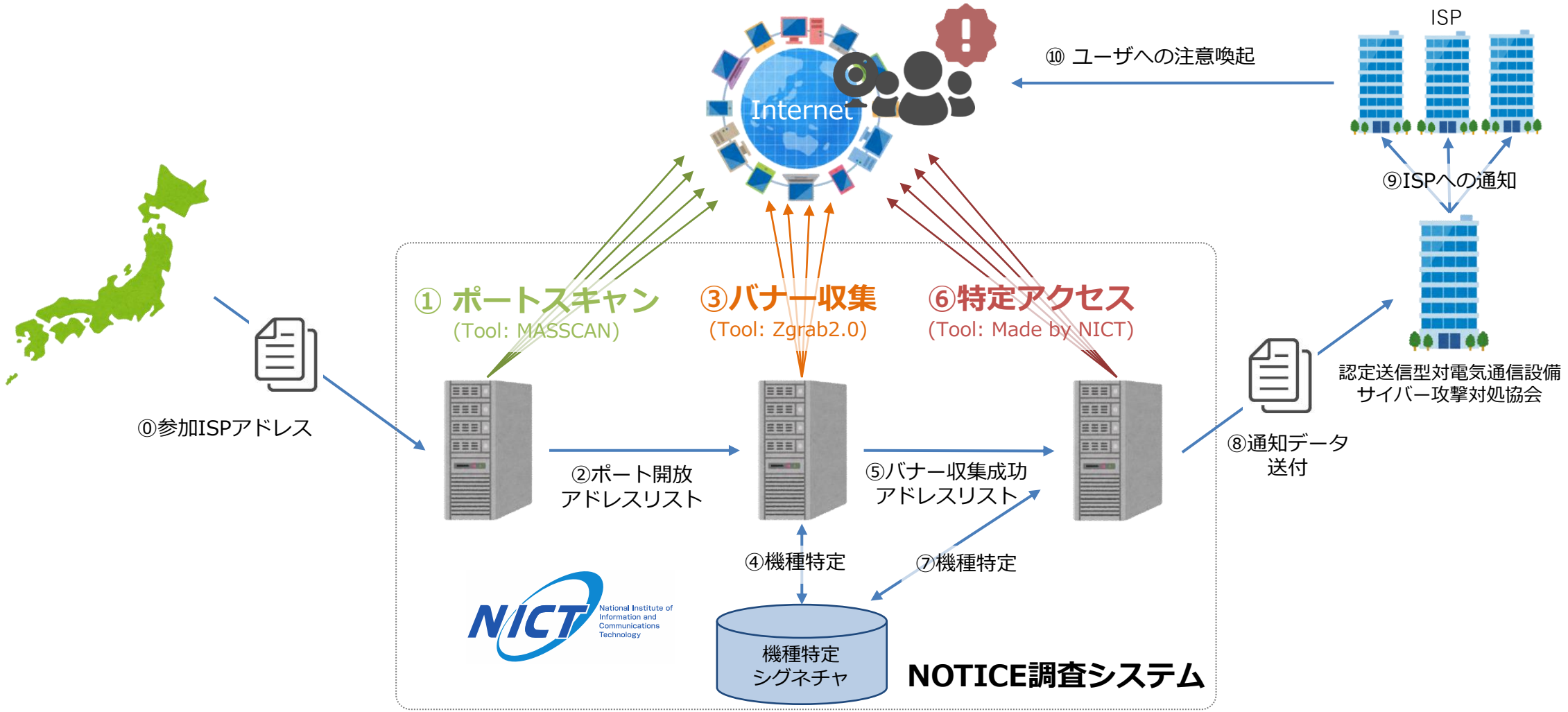
7　第二項から第四項までの規定により機構の業務が行われる場合には、次の表の上欄に掲げる規定中同表の中欄に掲げる字句は、それぞれ同表の下欄に掲げる字句とする。

不正アクセス行為の禁止等に関する法律第二条第四項第一号	及び当該	、当該
	を除く	及び国立研究開発法人情報通信研究機構法（平成十一年法律第百六十二号）附則第九条の認可を受けた同条の計画に基づき同法附則第八条第二項第一号に掲げる業務に従事する者がする同条第四項第一号に規定する特定アクセス行為を除く

NOTICE 調査の概要

NATIONAL CYBER OBSERVATION CENTER

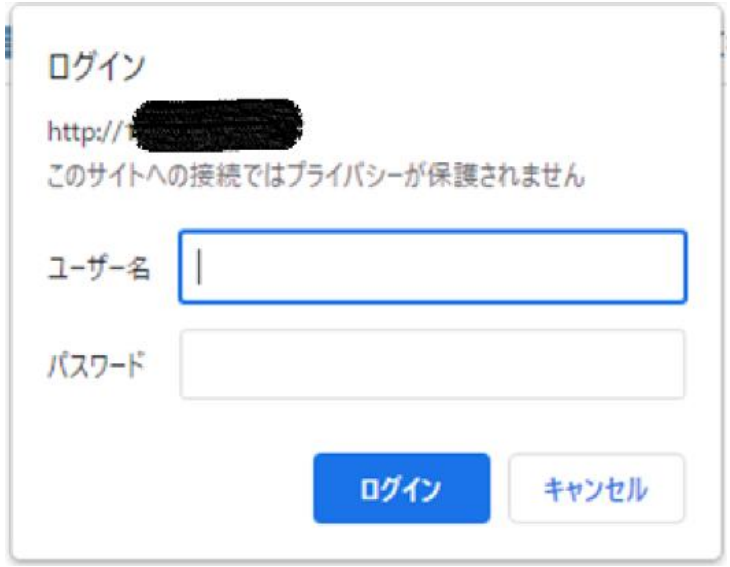
● 2019 (R1) 年4月：NOTICE調査＋ISP通知の開始



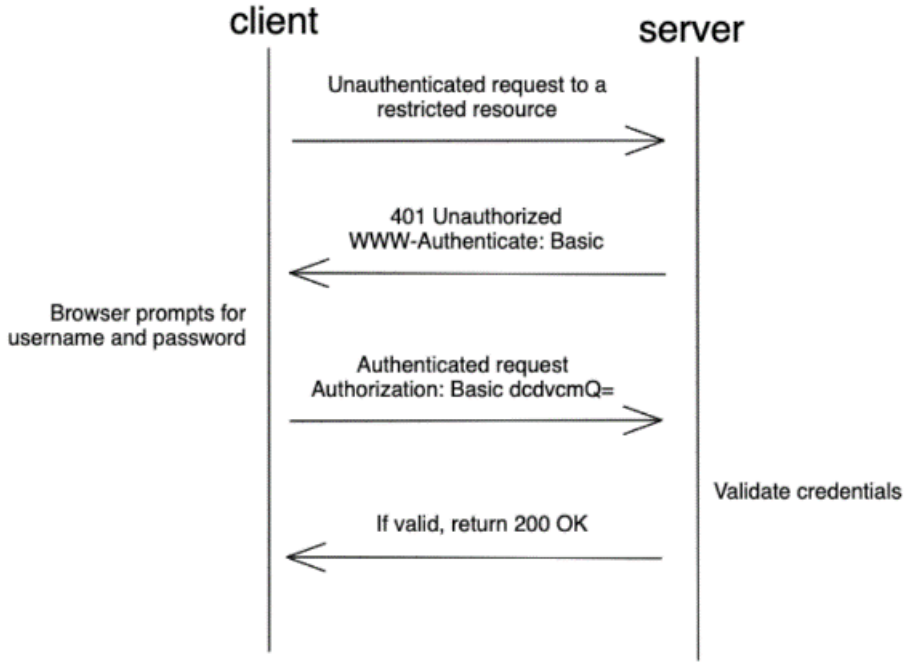
HTTP(S) Basic認証/Digest認証の調査開始 (R4)

NATIONAL CYBER OBSERVATION CENTER

- IoT 機器の Web 管理画面への攻撃活動も多数発生



Basic認証が要求されるWebサイトへアクセスした際に
Webブラウザに表示されるダイアログ例



Basic認証のフロー
[出典] https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication

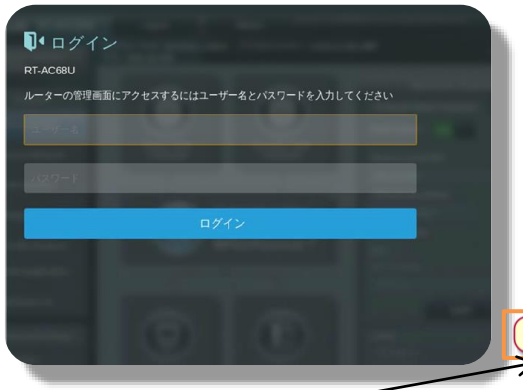
HTTP(S) のフォーム認証への対応 (R5)

NATIONAL CYBER OBSERVATION CENTER

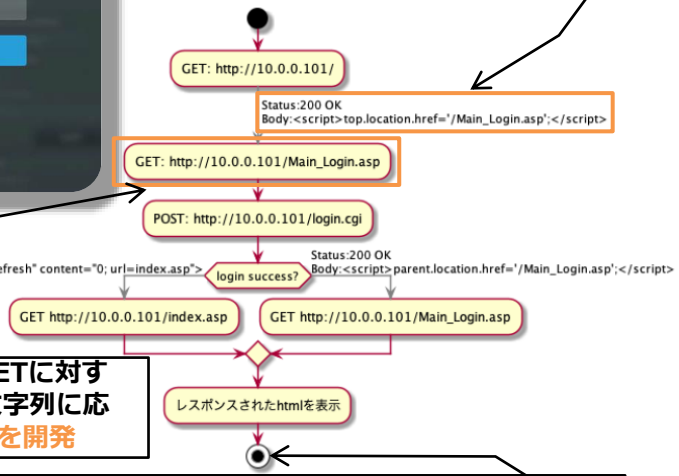
40機種のフォーム認証に対応したシステムを開発し、2023 (R5) 年6月から本調査開始

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



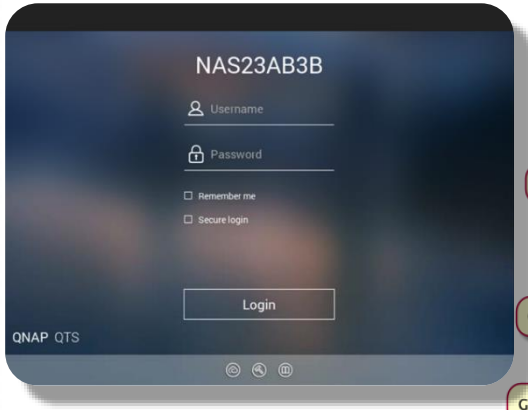
a. location.hrefのパスを検出する機能を開発・実装。/Main_Login.aspの検出によりログイン画面へのアクセスを実現

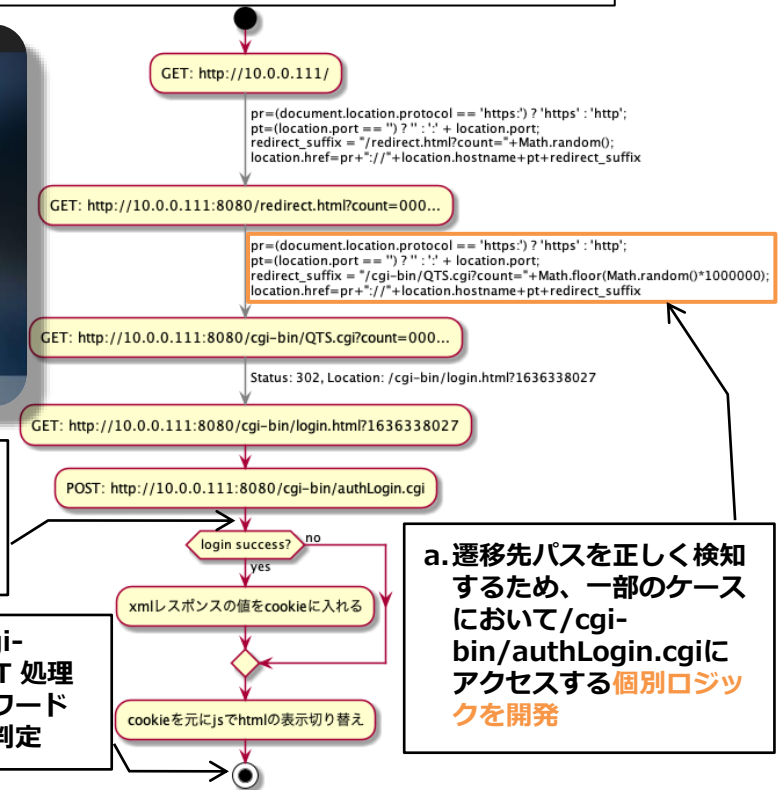


b. /Main_Login.aspへのGETに対するレスポンスに含まれる文字列に応じて機種Aを特定する機能を開発

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

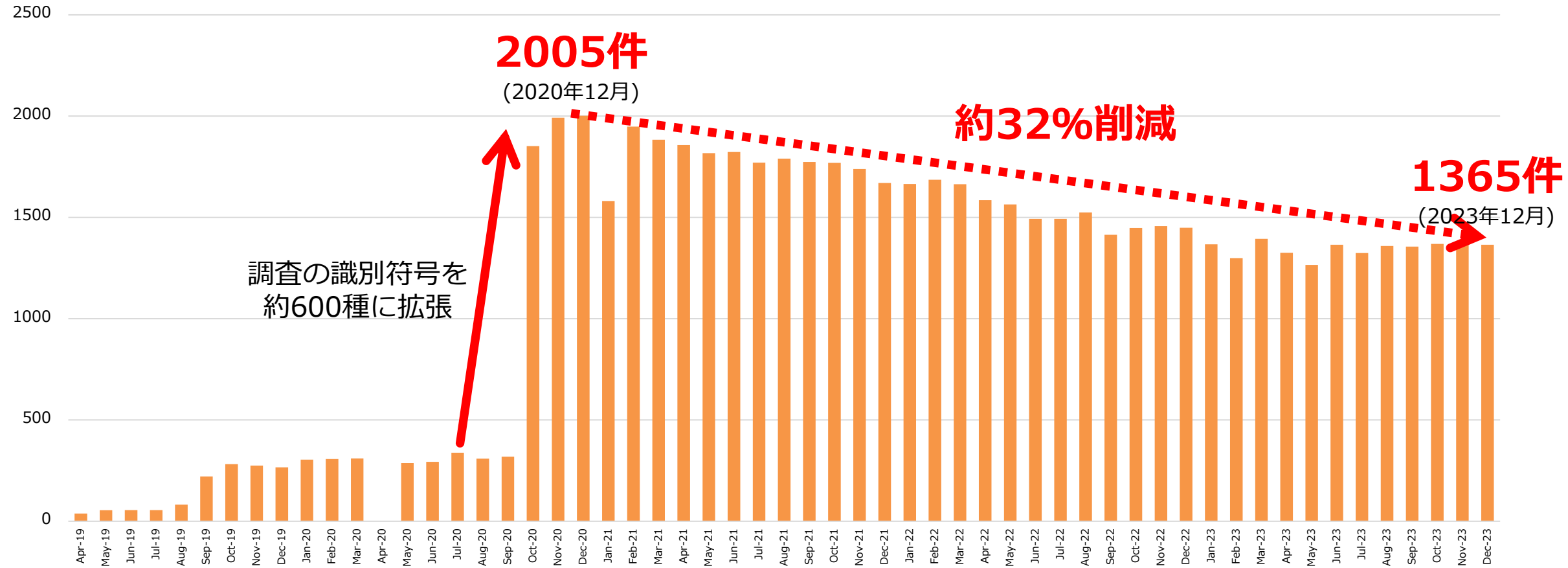
c. 機種Bと特定した機器について/cgi-bin/authLogin.cgi に別途 POST 処理を行い、レスポンスに所定のキーワードが含まれていればログイン成功と判定

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

月1回の継続的な調査とISPへの通知

NATIONAL CYBER OBSERVATION CENTER

✓Telnet/SSH/HTTP(S)におけるID/パスワード設定不備の国内機器として**10,000台以上を発見** (R5年度)
✓注意喚起対象としてR5年度に**計45,508件をISPへ通知** (R5年度)
✓継続的な通知によりTelnet/SSHの注意喚起対象機器をピーク時から**約32%削減**

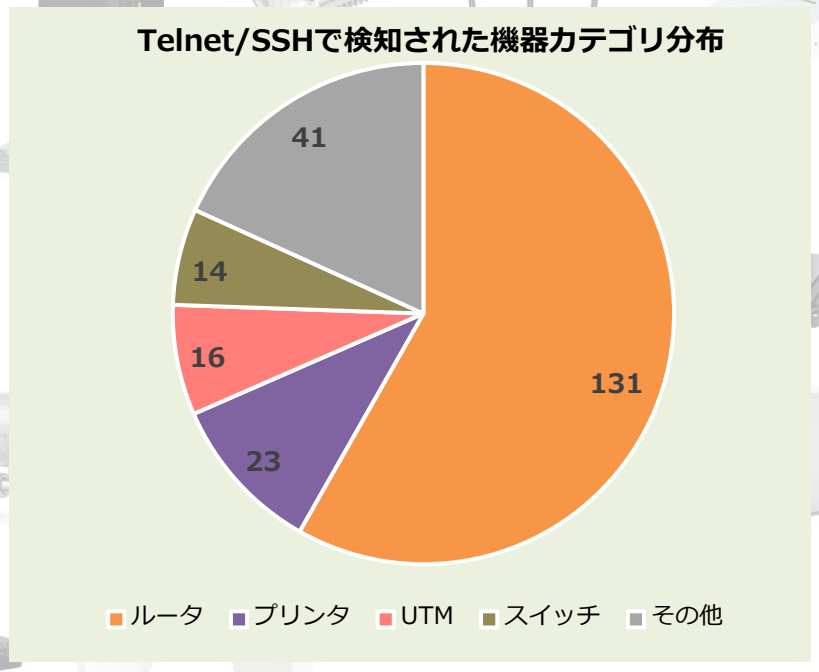


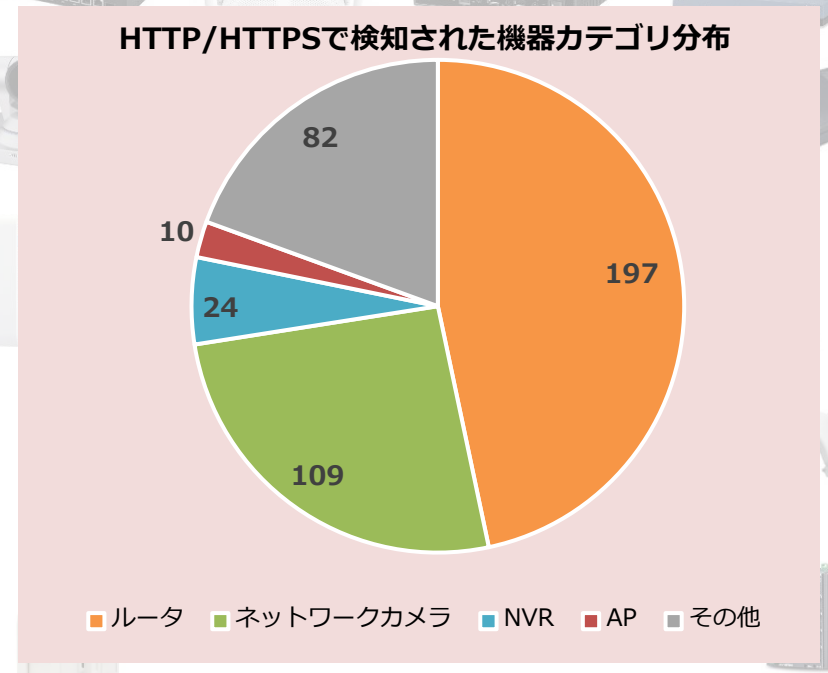
Telnet/SSHの注意喚起対象数の推移(月毎)

調査結果の分析により延べ600機種以上の脆弱な機種の特定に成功

NATIONAL CYBER OBSERVATION CENTER

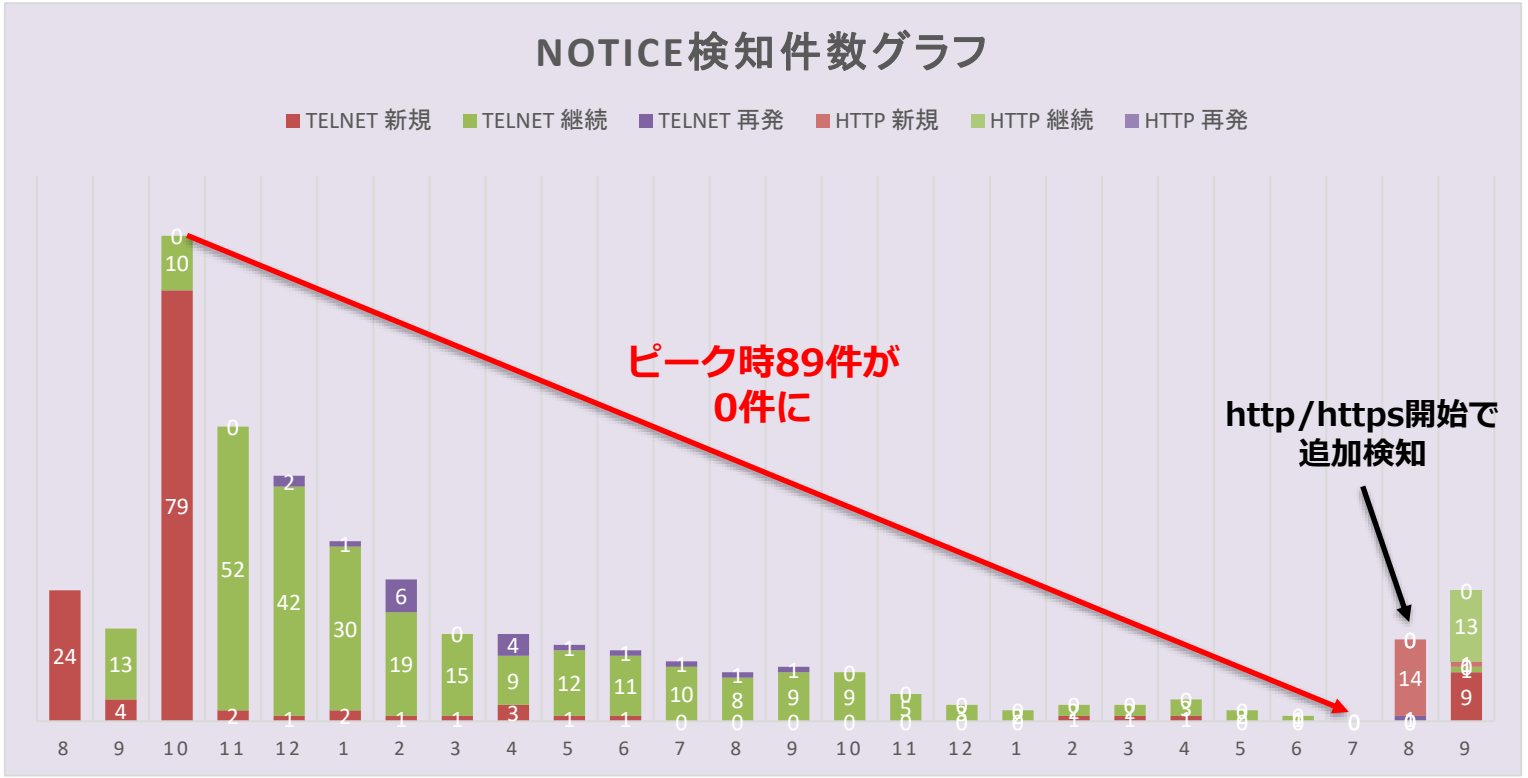
Telnet/SSH：　50ベンダ、計225機種
HTTP/HTTPS：83ベンダ、計422機種
を特定





注意喚起対象数が0件まで減少したISP

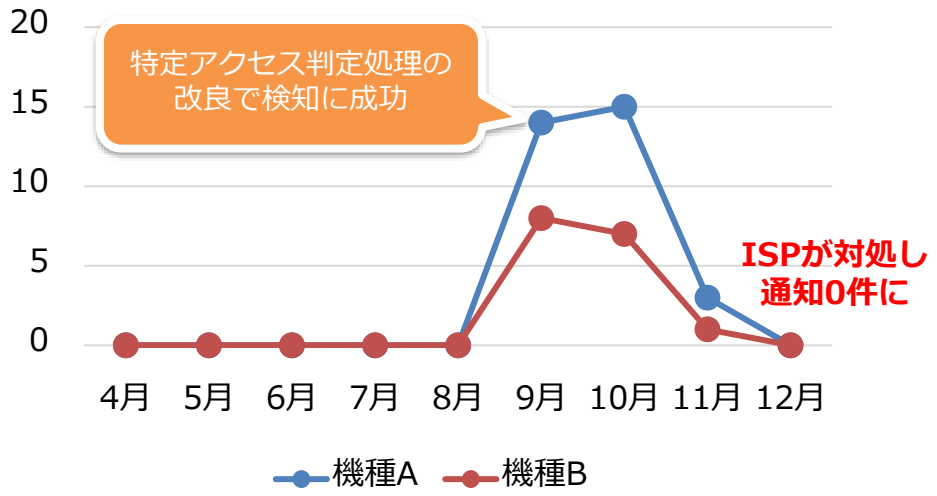
- **某ISP：Telnet/SSHに関してはほぼ全件対処完了**
  - ✓ 検知された契約者は全て法人顧客。メールでの注意喚起を実施
  - ✓ ISP内で通知データを顧客単位で紐づけて暦月管理し、対処状況を把握



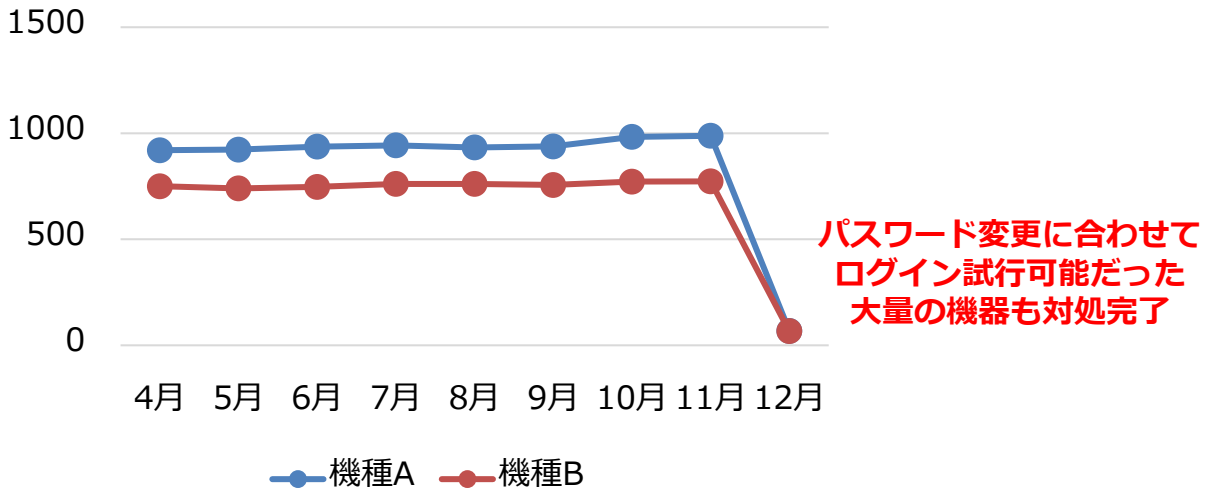
某ISPのNOTICE通知グラフ

ユーザ注意喚起無しでISPが直接対処

- **2019年9月：某ISPにある某社製ルータに特定アクセス成功・通知**
  - ✓ 通知数は約20件だが、ログイン試行が可能な機器が1700台以上、当該ISP内に存在
- **同月：当該ISPが調査した結果、ISP管理ルータ(マンション設置機器)と判明**
  - ✓ 管理用にOpen。設置時のパスワード変更の作業漏れで一部のルータがデフォルトで放置
- **～2019年11月：ISPでパスワード変更した結果、通知数0件に減少**
  - ✓ パスワード変更に合わせてログイン試行可能な機器1700台も設定変更され、悪用リスクを軽減



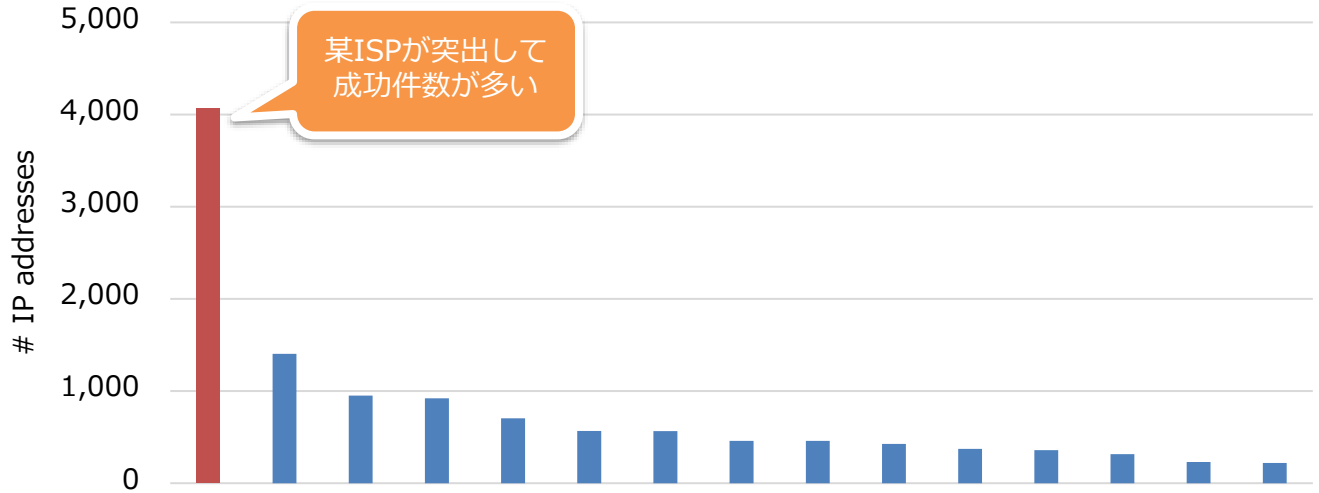
某社製ルータの注意喚起対象数の推移(月毎)



某社製ルータのログイン試行可能な機器数の推移(月毎)

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**



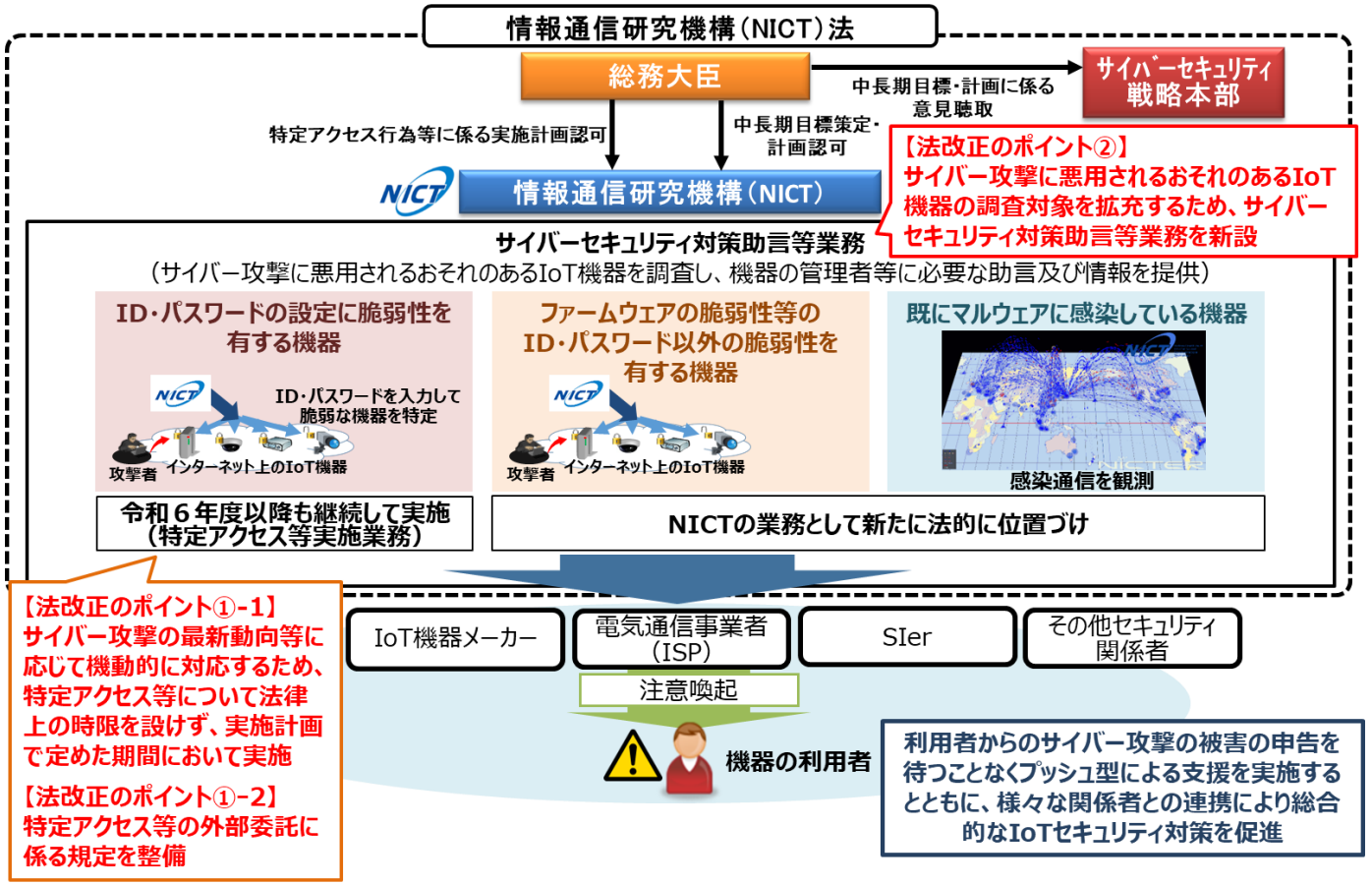
予備調査時(2022 (R4) 年3月)のISP別のhttp/https特定アクセス成功数

特定されたISP配布のルータシリーズ

情報通信研究機構法の改正（令和６年４月１日施行）

NATIONAL CYBER OBSERVATION CENTER

✓時限設定の解除による **NOTICE 事業の継続的実施**へ
✓パスワード設定の不備**以外**の脆弱性（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



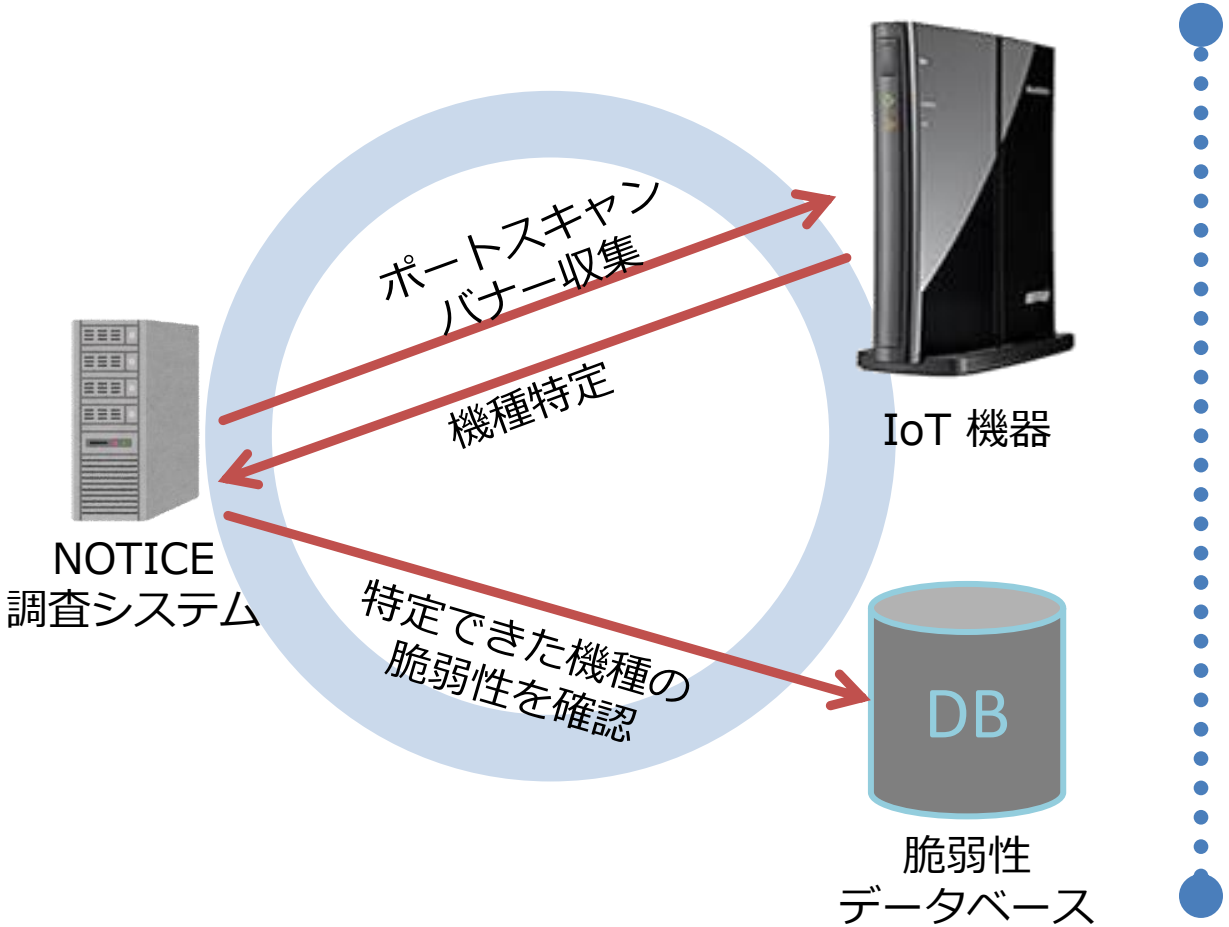
パスワード設定の不備以外の脆弱性調査

- **NOTICE調査の過程で、約40ベンダ300機種以上のファームウェア解析を実施**
  → 150件以上のファームウェアの脆弱性を報告 (CVE取得数47件)

- **今後このようなファームウェアの脆弱性を有する機器を新たな注意喚起対象とする**

ファームウェア脆弱性の調査？

- 機器に対して脆弱性検査を行うわけではない
- 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



おわりに

NATIONAL CYBER OBSERVATION CENTER

- **NOTICE 事業のこれまで**
  - ✓ 脆弱なパスワードが設定された機器は **32% 減少** (telnet / SSH)
  - ✓ 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

- **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

- **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