日本国内の脆弱なIoT機器の現状と課題

- NICTERとNOTICEの事例を基に –

@第8回スマートIoT推進フォーラム総会(2023/3/24)

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
サイバーセキュリティ研究室 副室長
笠間 貴弘

NICT National Institute of Information and Communications Technology

CYBERSECURITY Laboratory

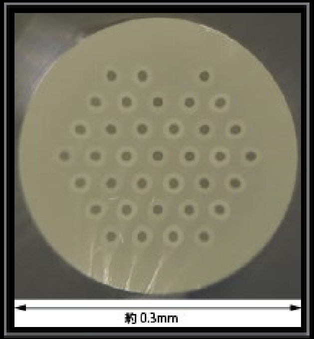
本日のアジェンダ

- **IoT機器を取り巻く脅威**
  - ✓ここ数年のサイバー攻撃事例
  - ✓NICTERで観測した国内IoT機器へのサイバー攻撃事例の紹介
  - ✓NOTICEで発見した国内の脆弱なIoT機器の対処事例の紹介
- **スマートかつセキュアなIoT環境の実現に向けて**

国立研究開発法人 情報通信研究機構とは？

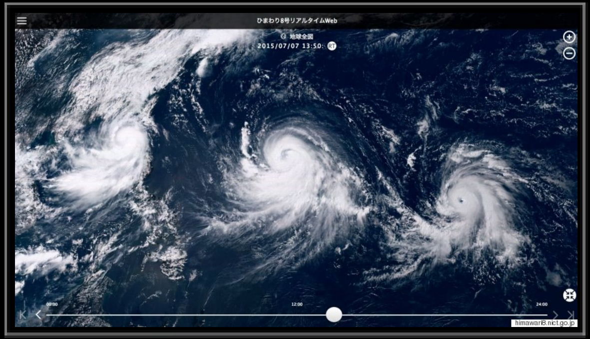
- 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入）



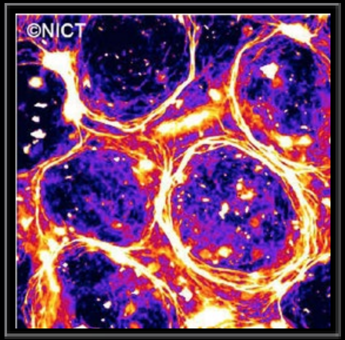
光通信システム
（ペタbps級 マルチコアファイバ）

宇宙通信システム
（超高速インターネット衛星きずな）

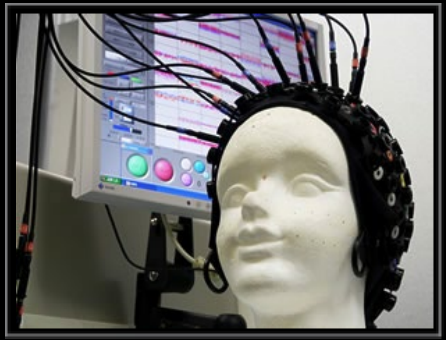


サイエンスクラウド
（ひまわり8号リアルタイムWeb）

電磁波センシング
（Pi-SAR2による3.11直後の仙台空港）



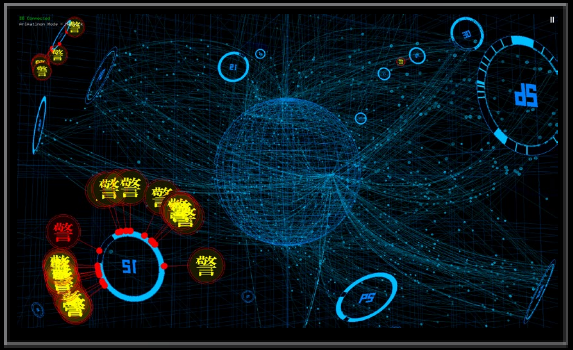
バイオ・ナノICT
（生体分子の自己組織化）



脳情報通信融合
（ブレイン・マシーン・インターフェイス）

多言語音声翻訳
（多言語音声翻訳アプリVoiceTra）

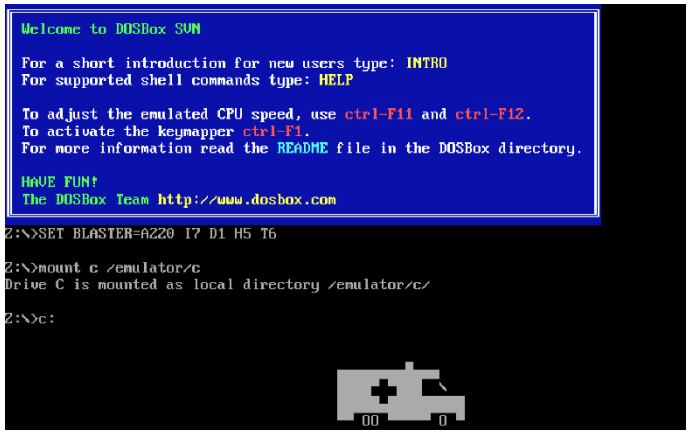
超臨場感コミュニケーション
（初音ミクさんの電子ホログラフィ）



サイバーセキュリティ
（対サイバー攻撃アラートシステムDAEDALUS）

サイバー攻撃の変遷

- 20世紀：愉快犯



ウイルス Ambulance（1990）

感染すると画面上を救急車が走る

https://archive.org/details/malware_AMBULANC.COM

- 21世紀：経済犯

示威活動
諜報活動

ランサムウェア（2019）

身代金要求型ウイルス
米国の年間被害額75億ドル以上？

https://www.technologyreview.jp/nl/ransomware-may-have-cost-the-us-more-than-7-5-billion-in-2019/

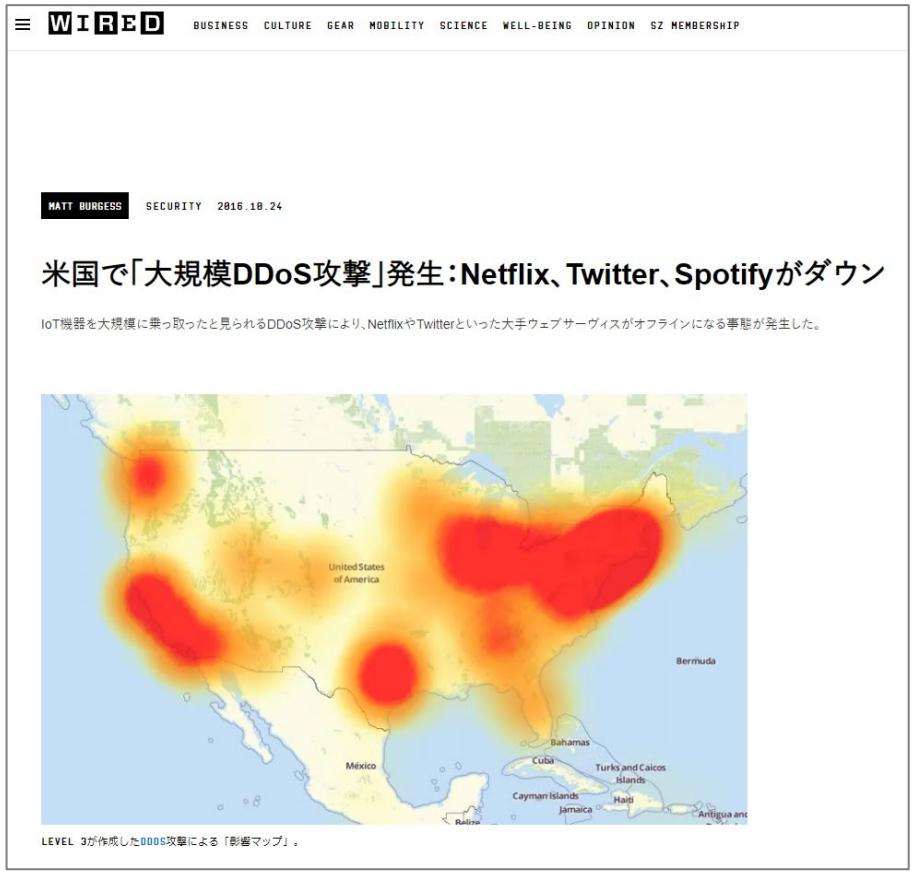
過去15年間の主なセキュリティ事案

発生年	事案名
2008	Downadup (a.k.a. Conficker)
2009	Gumblar (a.k.a. GENO)
2010	Stuxnet
2011	標的型攻撃
2012	バンキングマルウェア
	遠隔操作ウイルス
2013	リフレクター攻撃
	アカウントリスト攻撃
2014	Heartbleed, Shellsock
	ベネッセ 個人情報漏洩
2015	Sony Pictures Entertainment への攻撃
	日本年金機構 年金情報漏洩
2016	JTB 顧客情報漏洩
	超大規模DDoS攻撃　①

発生年	事案名
2017	Apache Struts2
	WannaCry
2018	パスワード大量流出
	仮想通貨マイニングツール設置
2019	NASAへのサイバー攻撃　②
	Emotet
2020	医療機関を狙った標的型ランサムウェア　③
	SolarWindsへのサプライチェーン攻撃
2021	米石油パイプライン企業のランサムウェア感染
	Log4j 脆弱性
2022	ロシアとウクライナのDDoS攻撃の応酬
	To be continued...

IoTマルウェアMiraiによる大規模DDoS攻撃

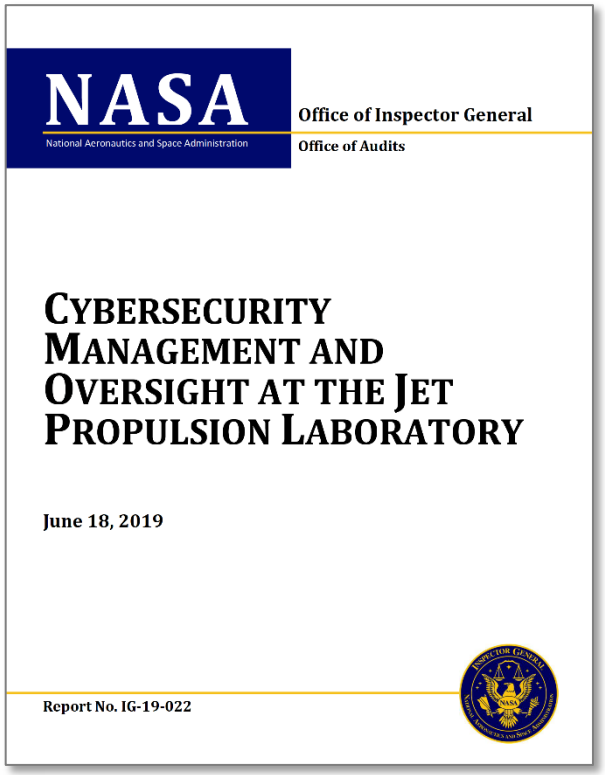
- **Mirai: 2016年に登場した主に家庭用ルータやWebカメラ等のIoT機器に感染を拡げるマルウェア**
  - ✓ Telnet(23/TCP, 2323/TCP)へのスキャン機能
  - ✓ ID/Passの辞書攻撃による感染機能
  - ✓ 様々なDDoS攻撃機能(**600Gbps**規模の攻撃発生)
  - ✓ 海外掲示板でソースコードが公開される



https://wired.jp/2016/10/24/internet-down-dyn-october-2016/

NASAへのサイバー攻撃

- NASAのジェット推進研究所（JPL）から機密データ漏洩
- 無許可接続されたRaspberry Piが原因（野良IoT）



NASA
National Aeronautics and Space Administration

Office of Inspector General
Office of Audits

CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY

June 18, 2019

Report No. IG-19-022

https://oig.nasa.gov/docs/IG-19-022.pdf

itmedia.co.jp

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」 - ITmedia NEWS

ITmedia NEWS > セキュリティ > NASA、サイバー攻撃で機密データ流出　侵入口は無許...

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」

2019年06月23日 07時45分 公開　[ITmedia]

印刷　1905　Share　B!　828

米航空宇宙局（NASA）のジェット推進研究所（JPL）の研究データが昨年、サイバー攻撃により盗まれていたことが、米連邦政府の監察総監室（OIG）が6月18日付で公開した報告書（リンク先はPDF）で明らかになった。

2018年4月にJPLのネットワークに侵入した攻撃者が約10カ月の間ネットワーク内の多数の脆弱性を利用して行動範囲を広げ、火星科学研究探査機のデータを含む約500MBの機密データを盗んだ。深宇宙通信情報網DSN（ディープスペースネットワーク）のデータにもアクセスした痕跡があるため、JPLのネットワークからDSNの宇宙飛行関連システムを切断したという。

DSNのパラボラアンテナ（画像：NASA）

攻撃者の侵入口はJPLのネットワークに無許可で接続していたRaspberry Pi端末だった。本来ならば最高情報責任者室（OCIO）がネットワークに接続するすべての端末を管理しているはずだが、正常に機能していなかった。管理者の1人はOIGに対し、新たに端末を接続する際はセキュリティデータベースに手動で登録することになっているが、更新機能がうまく動かないことがあり、そのまま登録を忘れることがあると語ったという。

https://www.itmedia.co.jp/news/articles/1906/23/news012.html

gigazine.net

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明 - GIGAZINE

GIGAZINE

2019年06月25日 19時00分　セキュリティ

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明

by Les Pounder

アメリカ航空宇宙局(NASA)は、2018年にジェット推進研究所(JPL)のネットワークがハッキングされたことを確認しました。報告によると、ハッキングをしかけたクラッカーは、JPLのネットワークに無許可で接続されたRaspberry Piを侵入口として、データを盗み出したとのことです。

"https://www.flickr.com/photos/biglesp/14234773312/"を新規タブで開く

https://gigazine.net/news/20190625-nasa-hacked-raspberry-pi/

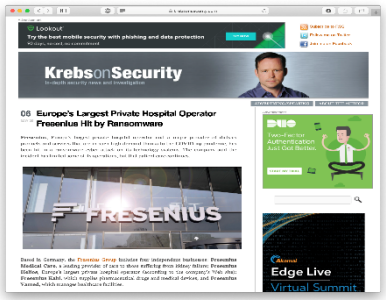
医療機関を狙った標的型ランサムウェア

- **ランサムウェア：感染端末のデータを暗号化し復号の見返りに金銭を要求するマルウェア**

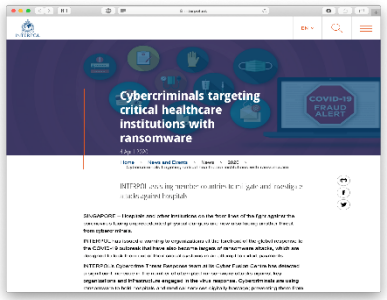
- **医療機関をターゲットにした標的型ランサムウェアの出現**
  - ✓ 2016年：米国Hollywood Presbyterian Medical Center ➡ 1万7000ドルの身代金を支払いデータ復旧
  - ✓ 2018年：奈良県宇陀市立病院 ➡ 電子カルテシステムの利用が不可能に

- **欧州最大の民間病院運営会社『Fresenius』がランサムウェアに感染（2020年5月）**
  - ✓ Freseniusは過去にもマルウェア感染し150万ドルを支払ったことがあるらしい#1
  - ✓ INTERPOL#2とDHS#3から医療機関を狙った標的型ランサムウェアに注意喚起

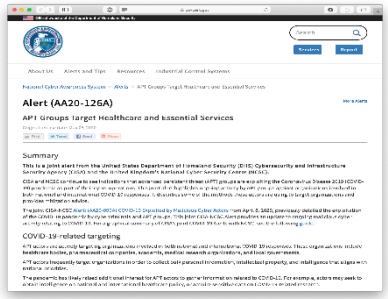
- **デュッセルドルフ大学病院でランサムウェアによる初の死亡例？ #4（2020年9月）**
  - ✓ 院内のITシステムへのマルウェア感染で患者の緊急搬送を受け入れられず移送先で死亡



#1 Krebs on Security
https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/



#2 INTERPOL
https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware



#3 DHS
https://www.us-cert.gov/ncas/alerts/AA20126A

#4 ZDNet
https://japan.zdnet.com/article/35159781/

NICTにおけるIoT機器のセキュリティ対策の取組

Active Countermeasure

パスワード設定等に
不備のある機器

特定アクセス
による調査

NOTICE
National Operation Towards IoT Clean Environment

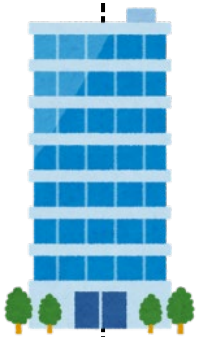
Passive Countermeasure

既にマルウェアに
感染している機器

ダークネット
による観測

NICTER

ISP



NICTにおけるIoT機器のセキュリティ対策の取組

Active Countermeasure

パスワード設定等に
不備のある機器

特定アクセス
による調査

NOTICE
National Operation Towards IoT Clean Environment

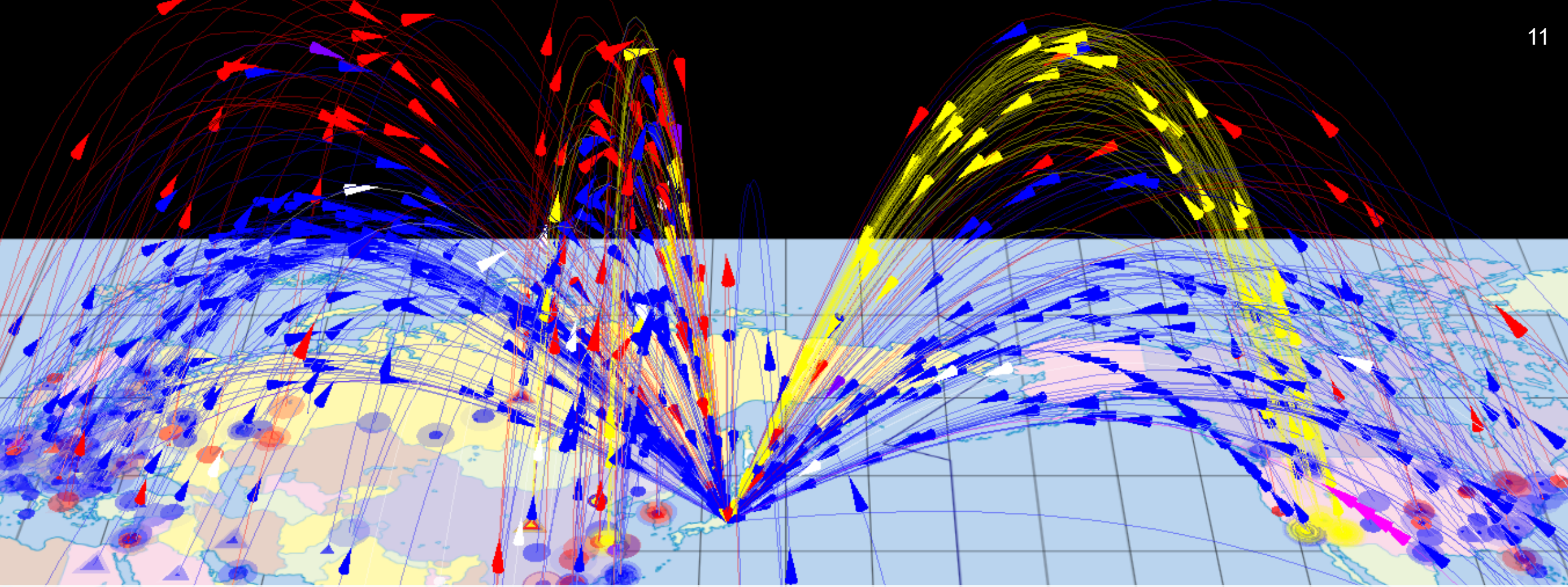
ISP

Passive Countermeasure

既にマルウェアに
感染している機器

ダークネット
による観測

NICTER

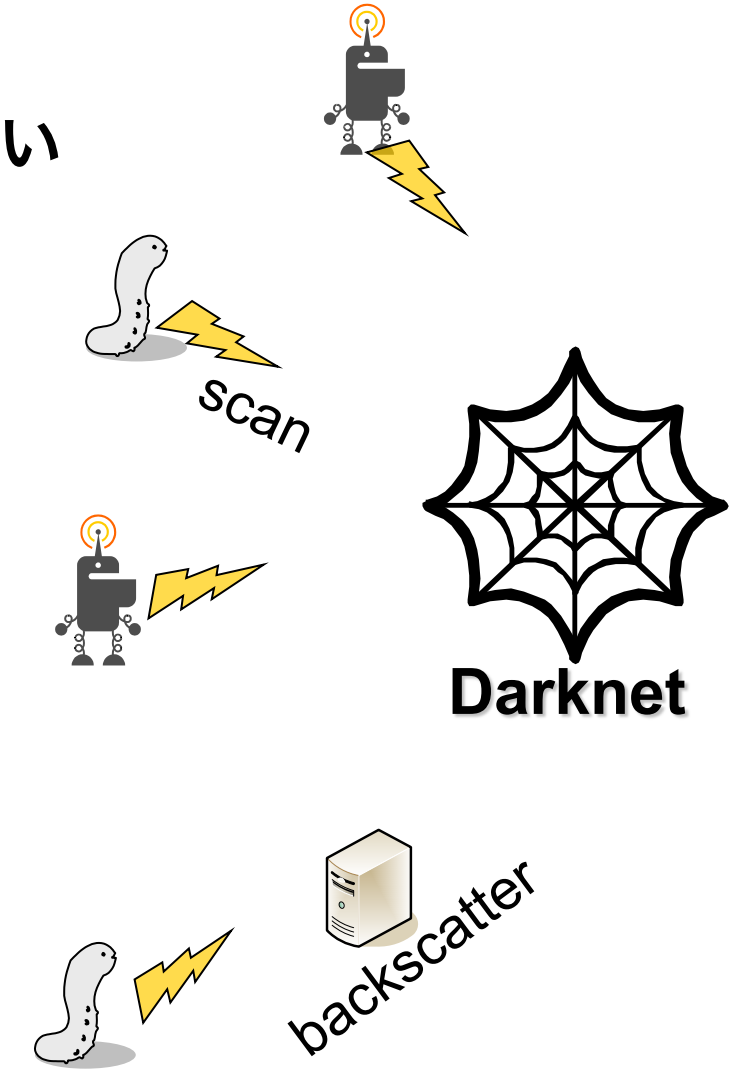


NICTER

- 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

ダークネットで見えるもの

- **ダークネット = 未使用IPアドレスブロック**
  - ✓何もない所にパケットが飛んでくること自体おかしい
- **ダークネットで見えるもの**
  - ✓インターネット上で何かを探す行為
    - ワーム型マルウェアによるスキャン
    - DRDoSのリフレクタ探索（DNS Open Resolver、NTP etc.）
    - セキュリティ関連組織等による調査
  - ✓DoS攻撃の跳ね返り
    - DDoSバックスキャッタ
      ※ 送信元IPアドレス偽装されたSYN Floodへの応答
    - DNS水責め攻撃のバックスキャッタ
      ※送信元IPアドレス偽装されたランダムサブドメイン攻撃
  - ✓設定ミス



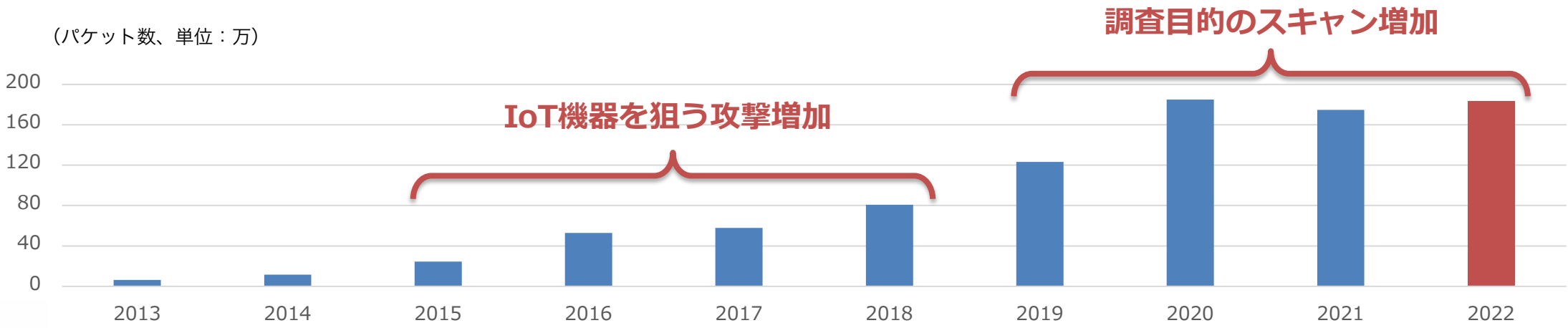
NICTERダークネット観測統計（過去10年）

年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2013	約128.8億	209,174	63,682
2014	約241.0億	212,878	115,335
2015	約631.6億	270,973	245,540
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	**約5,226億**	**288,042**	**1,833,012**

1アドレスあたり

17秒に1回

攻撃関連通信受信



1 IPアドレス当たりの年間総観測パケット数

調査目的のスキャンの増加

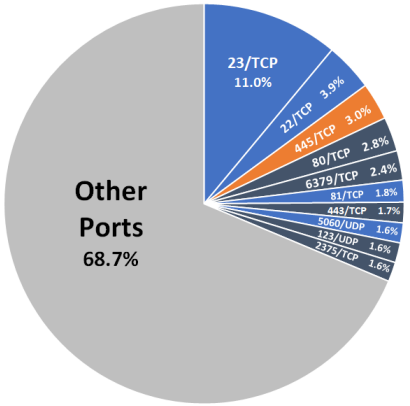
- **2018年頃から海外のセキュリティ企業や大学からの調査目的のスキャンが急増**
  - ✓ スキャン元アドレスの多くは素性不明（海外の防弾ホスティングなどを利用）

- **スキャン結果はインテリジェンスサービスとして公開(販売)される**

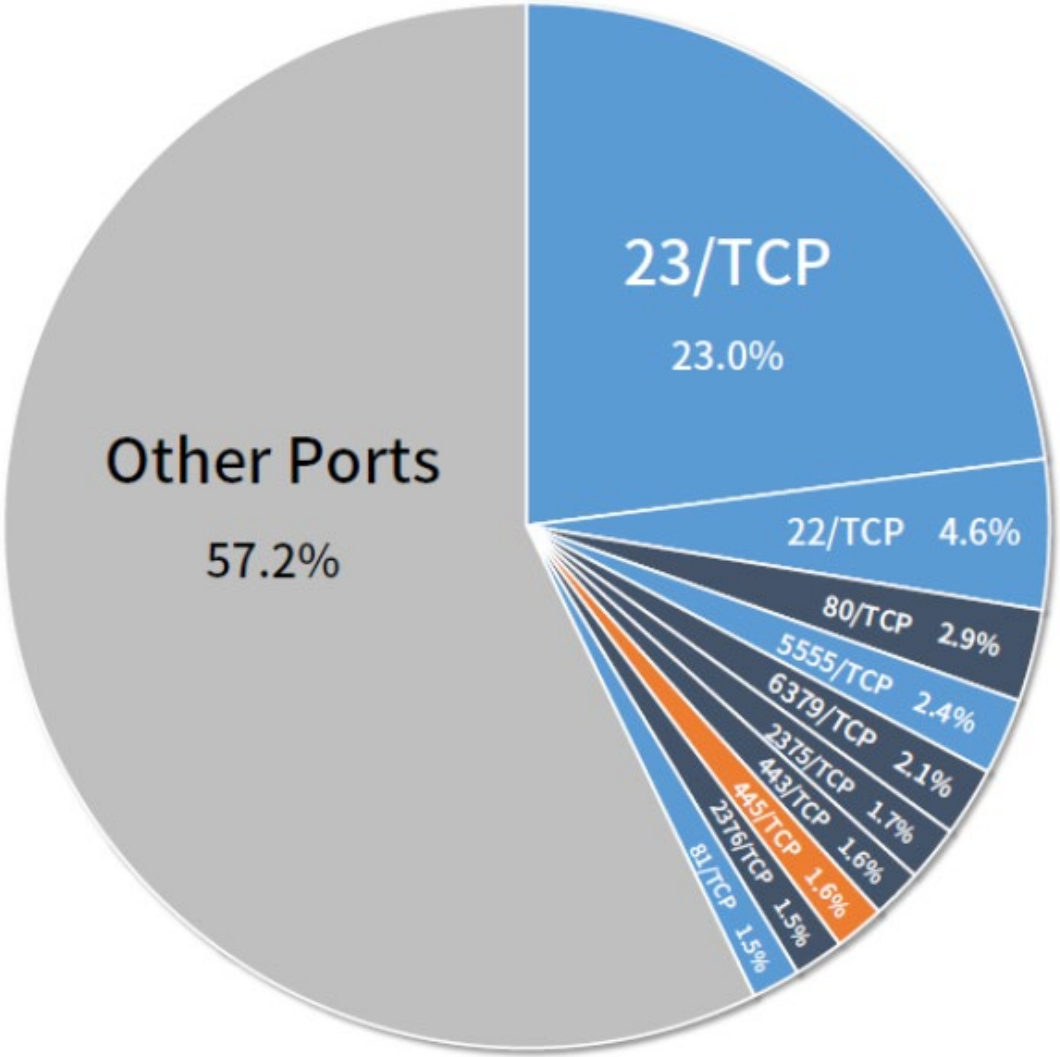
- **インターネット向けにOpenになっているポートは全て公開される時代**
  - ✓ デフォルトポートから変更していれば安全、ということは無い
  - ✓ きちんとしたアクセス制限や認証等のセキュリティ対策は必要不可欠

感染機器の分布（2022年）

- NICTER 観測レポート 2022：宛先ポート番号別パケット数分布 -



2021年



2022年

ポート番号	主な攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Web管理画面）
5555/UDP	ADB (Android Debug Bridge)
6379/TCP	Redis
2375/TCP	Docker REST API
443/TCP	HTTPS (Webサーバ)
445/TCP	Microsoft-DS（SMB, Samba等）
2376/TCP	Docker REST API
81/TCP	HTTP（ホームルータ等）

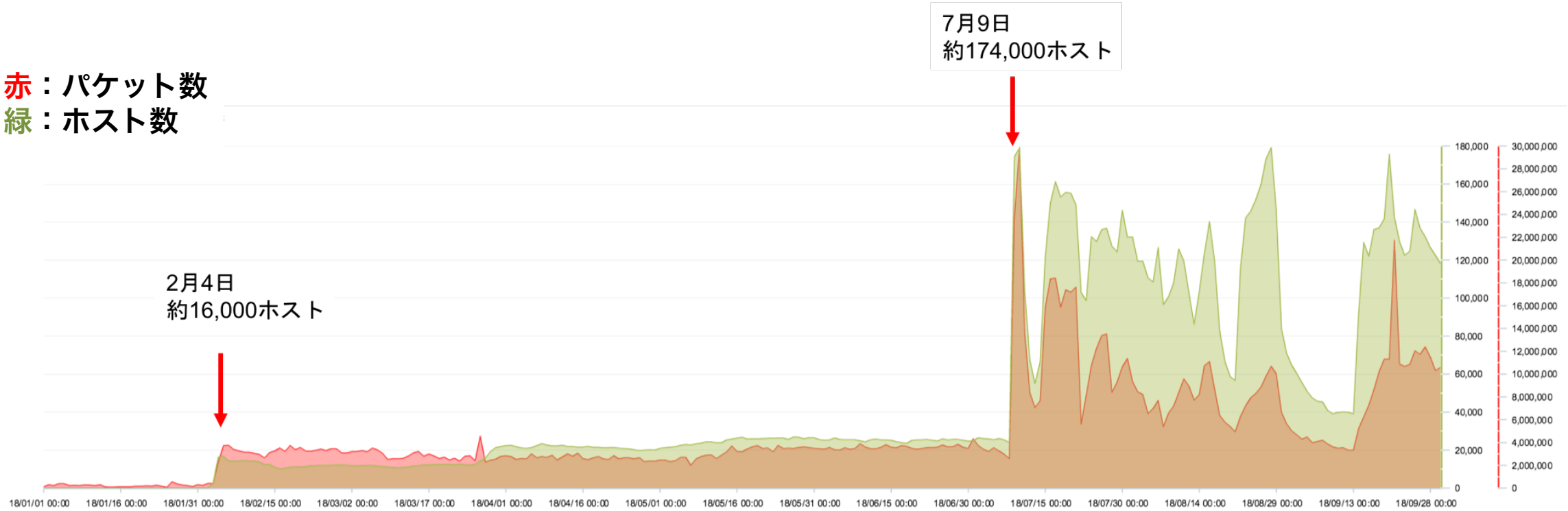
宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

出典：NICTER観測レポート2022
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

脆弱なAndroid機器の感染

●2018年7月以降、5555/TCPを狙う攻撃活動が増加

- ✓全世界の計17万ホスト以上からのスキャンを観測
- ✓**日本国内からも500ホスト/日**からのスキャンを観測



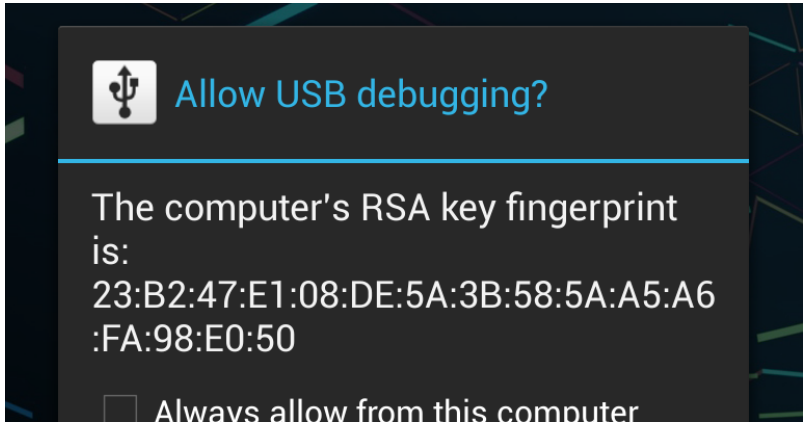
5555/TCPに関するNICTER観測統計(2018年当時)

National Institute of Information and Communications Technology

脆弱なAndroid機器の感染

- **5555/TCP：Android Debug Bridge(ADB)**
  - ✓Androidデバイスと通信するためのツール
  - ✓5555/TCP経由でデバイスにアクセスし様々なコマンドの利用が可能

- **認証無しでコマンド実行可能なADBが狙われていることを特定**
  - ✓adbコマンドによって不正なapkファイルを実行
  - ✓スマートフォンなど市販のAndroid端末ではSecure ADB設定になっており、ADB接続時に端末側での承認が必要になっているはず
  - ✓市販のAndroid端末以外が狙われている可能性



市販のAndroid端末では通常SecureモードがON

脆弱なAndroid機器の感染

●日本国内ADB有効ホスト Top10（2018年当時）

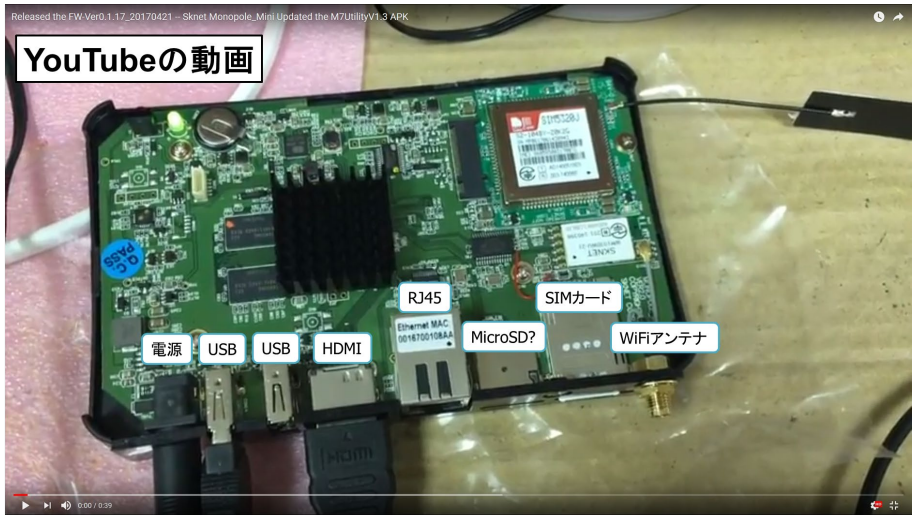
✓スマホのモデル名が取得できたものは原則エミュレータ（BlueStacks）

✓モバイル回線に繋がっているデジタルサイネージ機器らしきモデルを発見

モデル名	ホスト数	種別	備考
正常に取得できず	254	STB	CATV用STB
XT1052	120	スマホ/VM	エミュレータの可能性大
Sknet-Monopole_mini	114	デジタルサイネージ	モバイル回線利用
SAMSUNG-SM-N900A	82	スマホ/VM	エミュレータの可能性大
PIXEL 2 XL	24		
SM-G950F	23		
SM-G955F	22		
AFTT	21	mini STB	FireTV Stick (2nd Gen)
Pixel XL	17	スマホ/VM	エミュレータの可能性大
その他	74		

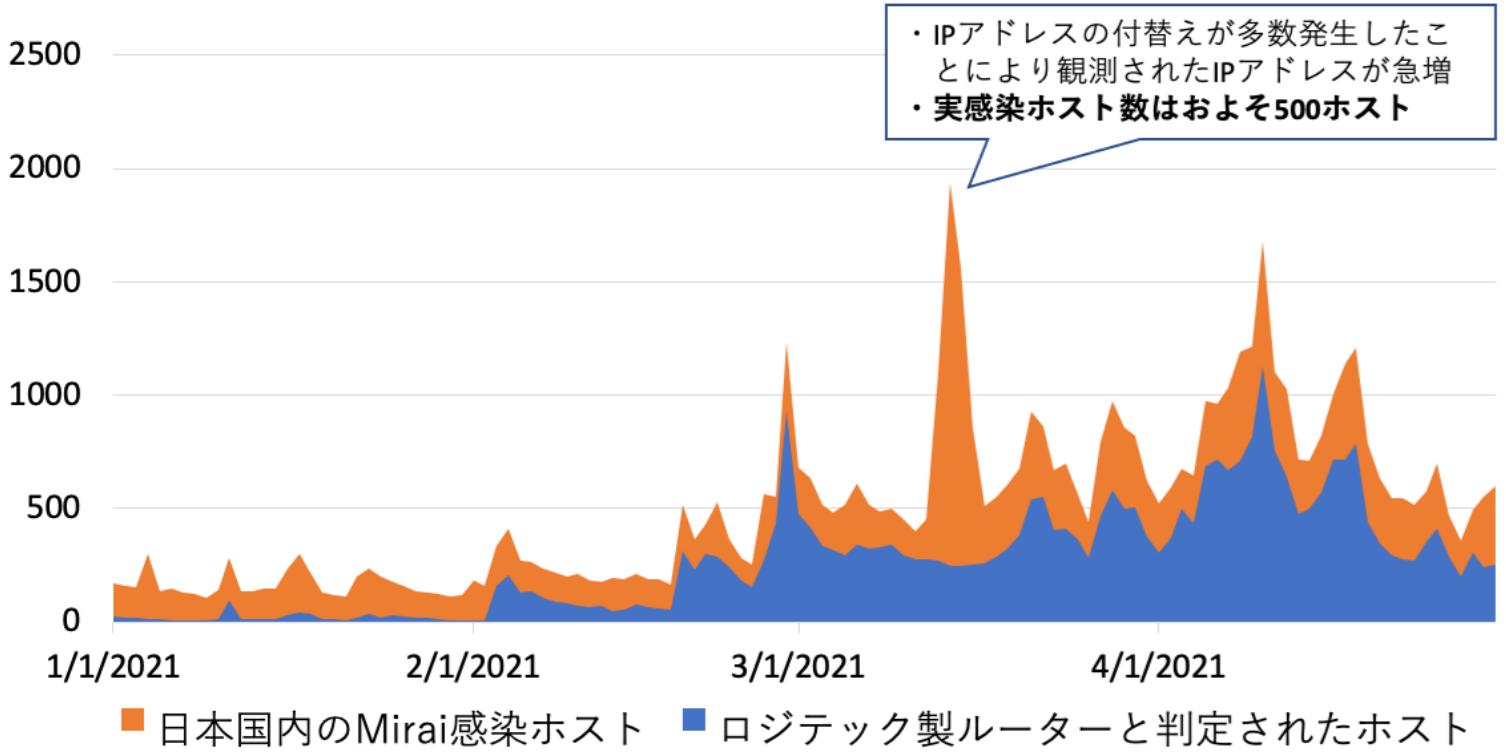
脆弱なAndroid機器の感染

- **利用会社を特定しJPCERT/CC経由で連絡、現場訪問**
  - ✓工事現場で現物確認（施行担当の建設会社の持ち込みで設置）
- **販売元の会社へ連絡**
  - ✓別会社から機材を購入し独自のサイネージ用アプリをインストールして販売
- **機材の販売会社へ訪問**
  - ✓デフォルトADB有効で出荷していることを確認。無効にするように対処



サポート期限切れのホームルータ感染

- **2021年以降、国内のMirai感染ホストは概ね500～1000ホスト/日前後で推移**
- **調査により、約半数がロジテック社の特定のホームルータであることが判明**
- **当該ホームルータは発売から10年以上が経過しており、既にサポート期限切れ**

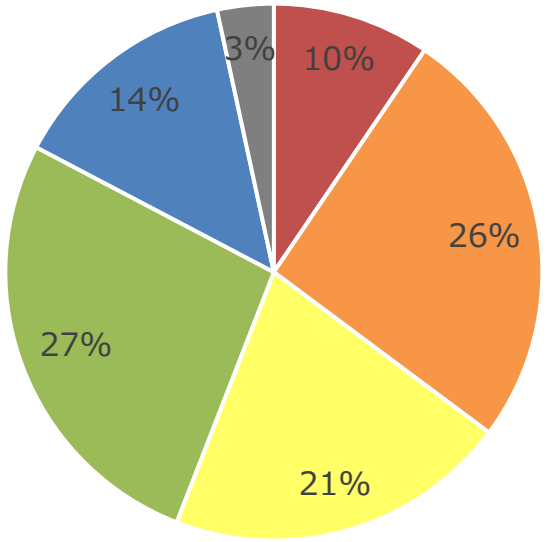


（出典）NICTER Blog「日本国内のMiraiに感染する機器の観測状況」
https://blog.nicter.jp/2021/05/jp_mirai_and_infected_logitec_routers/

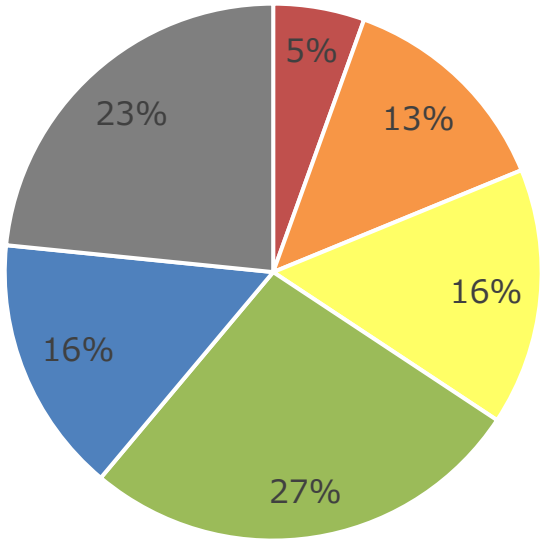
ユーザのIoT機器利用状況の調査

- **アンケート調査：**
  - ✓ 調査期間：2022年12月頭～中旬
  - ✓ 国内在住の個人、18歳以上、ルータ/ネットワークカメラ/NASのいずれか1台でも自ら管理している

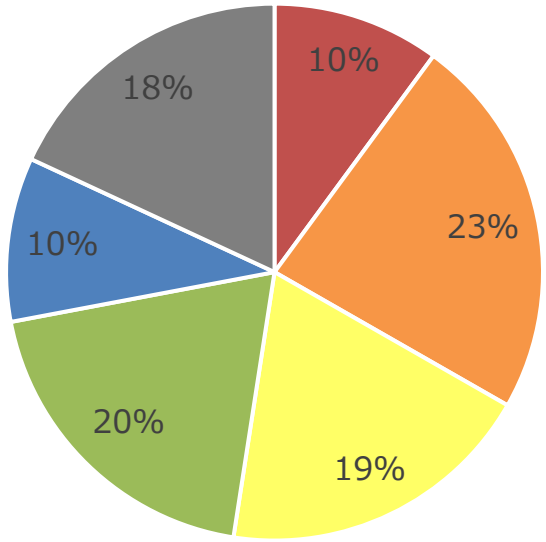
- **Q：そのIoT機器を何年くらい利用していますか？**



ルータ(n=28,716)



ネットワークカメラ(n=5,178)

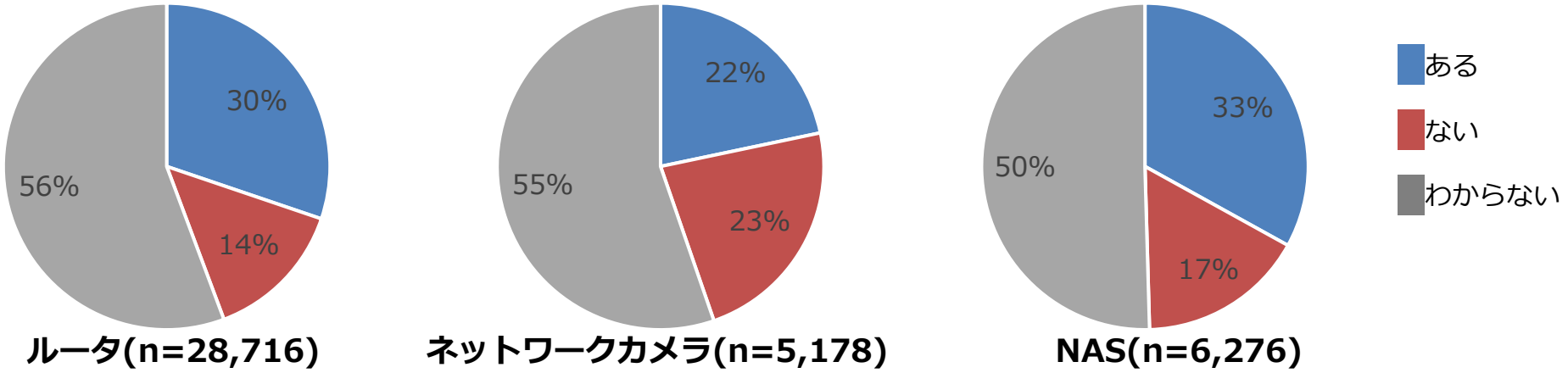


NAS(n=6,276)

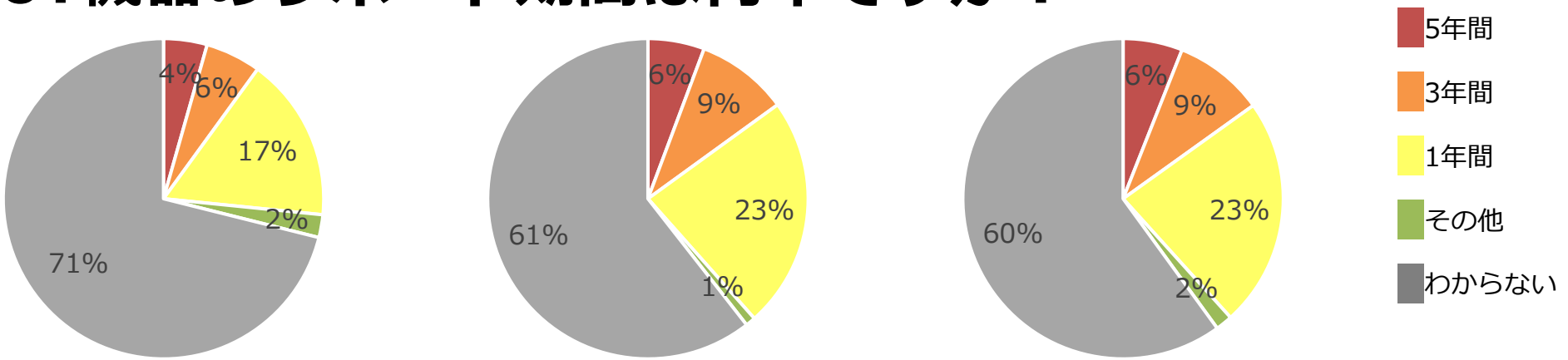
10年以上　5年以上～10年未満　3年以上～5年未満　1年以上～3年未満　1年未満　わからない

ユーザのIoT機器利用状況の調査

- Q：そのIoT機器にアップデート機能はありますか？

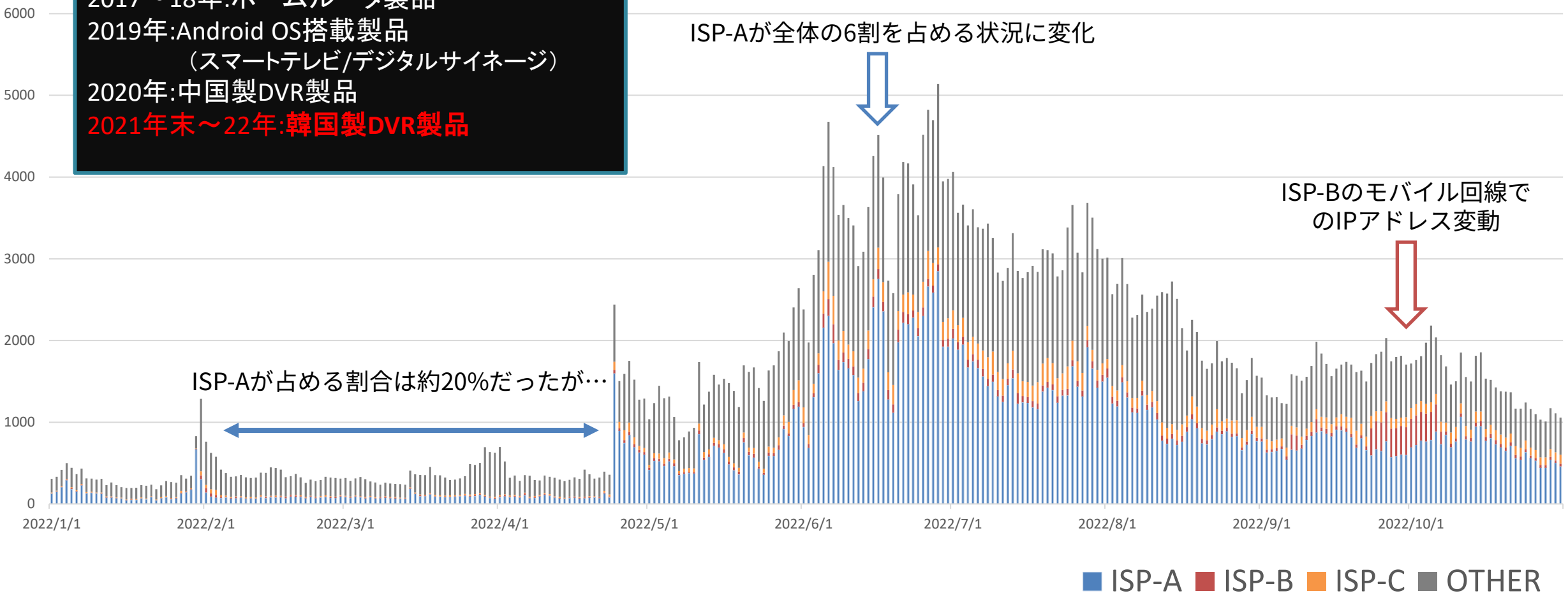


- Q：そのIoT機器のサポート期間は何年ですか？



2022年の日本国内のMirai感染ホスト数の推移

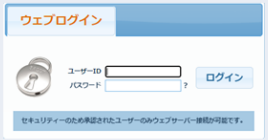
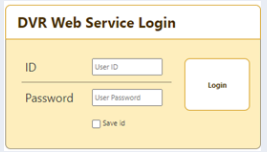
2017～18年:ホームルータ製品
2019年:Android OS搭載製品
（スマートテレビ/デジタルサイネージ）
2020年:中国製DVR製品
2021年末～22年:**韓国製DVR製品**



海外ベンダ製のDVR(OEM品)の感染

●2022年以降、国内でDVRのマルウェア感染が増加中

- ✓ 海外ベンダ製のOEM機器が国内で販売され感染している
- ✓ 脆弱性、ハードコードされたID/Pass、バックドアなど感染経路は機器で異なる

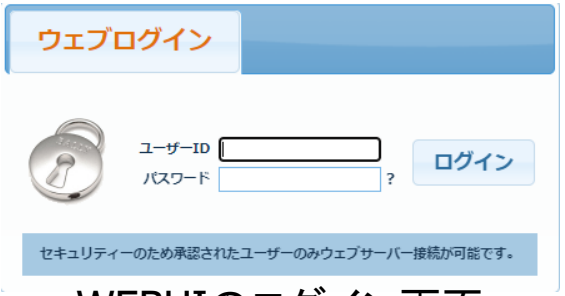
製造元	筐体	管理画面	有効なポート （※FWにより異なるため参考情報）
FocusH&S			80/TCP 8002/TCP 9010/TCP 10801/TCP
Rifatron			21/TCP 23/TCP 80/TCP 1998/TCP 50100/TCP
Pinetron			7000/TCP
CTRing			23/TCP 80/TCP 5920/TCP

NICTで感染（脆弱性）を確認したDVRの一部

海外ベンダ製のDVR(OEM品)の感染

- **Focus H&S製DVR製品の場合**
  - ✓日本国内で販売
  - ✓**認証不要で任意コード実行可能**
    - CVE-2022-35733
    - Webシェルが存在
    - 機器のパスワード変更では攻撃を防げない
- **攻撃者のスキャン対象：**
  - ✓日本やアメリカ、韓国など

筐体画像



WEBUIのログイン画面

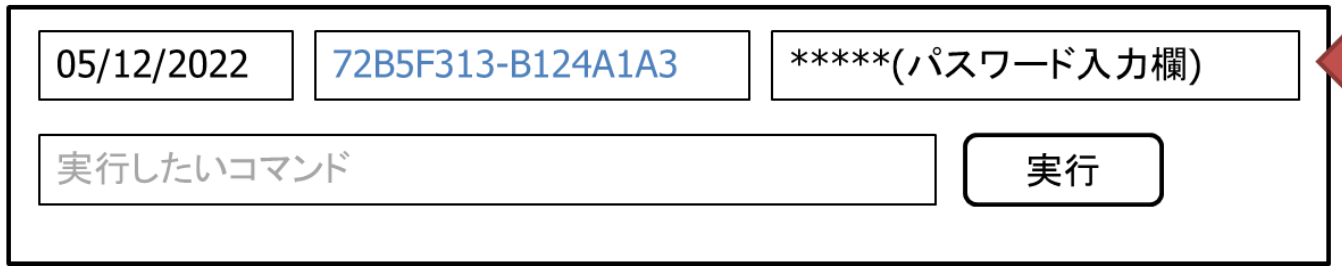
```
22   153.132.36.162 title: main page ||| org: Open Computer Network ||| ports: [8080]
23   153.142.97.170 title: main page ||| org: Open Computer Network ||| ports: [9080]
24   153.144.76.118 title: main page ||| org: NTT Plala Inc. ||| ports: [80, 83]
25   153.156.173.87 title: main page ||| org: Open Computer Network ||| ports: [9080]
26   153.156.85.234 title: main page ||| org: Open Computer Network ||| ports: [81]
```

攻撃者作成のスクリプト内に
日本の攻撃可能なホスト情報が書かれていた

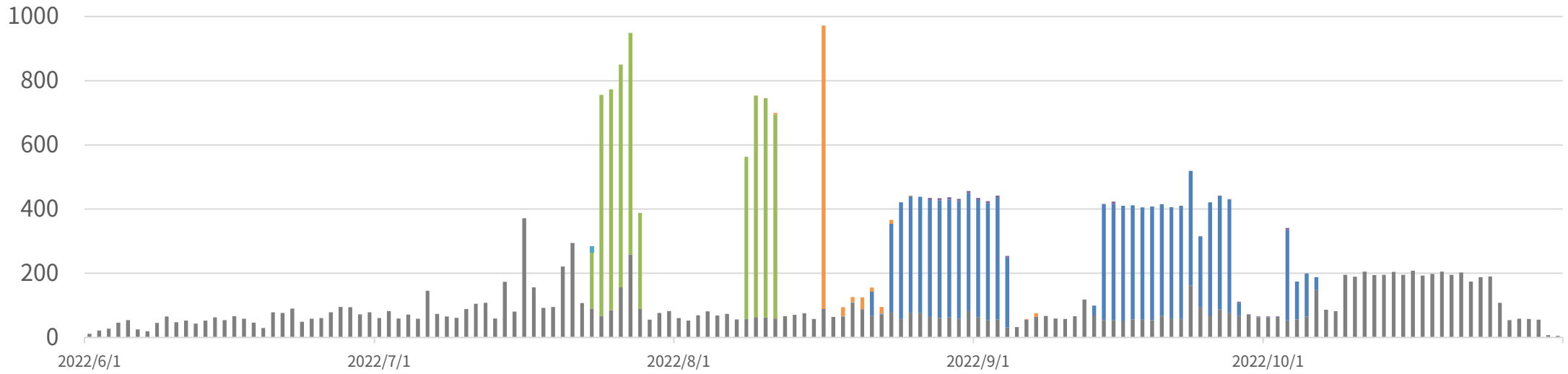
海外ベンダ製のDVR(OEM品)の感染

- **任意コマンド入力ができるバックドアページが悪用されていた**
  - ✓ コマンド実行にはワンタイムパスワードの入力が必要だが、攻撃者は突破していた

バックドアのページ（認証なしでアクセス可能） ※再現イメージ



ワンタイムパスワードのアルゴリズムは製造元もしくはファームウェア解析をしないと分からないはず



NICTで観測したFocus H&S製DVRを狙った攻撃

NICTER観測から見える動向

- **アタックサーフェスの探索が定常化**
  - ✓インターネット側にOpenなポート・サービスは必ず発見される
- **Telnet/SSH以外の感染経路が毎年のように登場**
  - ✓野良Android、特定機器の脆弱性、OEM機器、etc.
- **適切な設定・管理が行われていない機器は格好の獲物**
  - ✓ユーザが機器のセキュリティ状況を正しく認識することは容易ではない

NICTにおけるIoT機器のセキュリティ対策の取組

Active Countermeasure

パスワード設定等に
不備のある機器

**特定アクセス
による調査**

NOTICE
National Operation Towards IoT Clean Environment

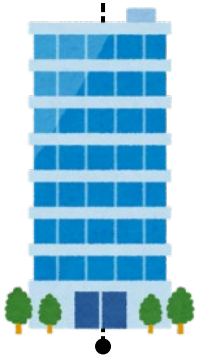
Passive Countermeasure

既にマルウェアに
感染している機器

**ダークネット
による観測**

NICTER

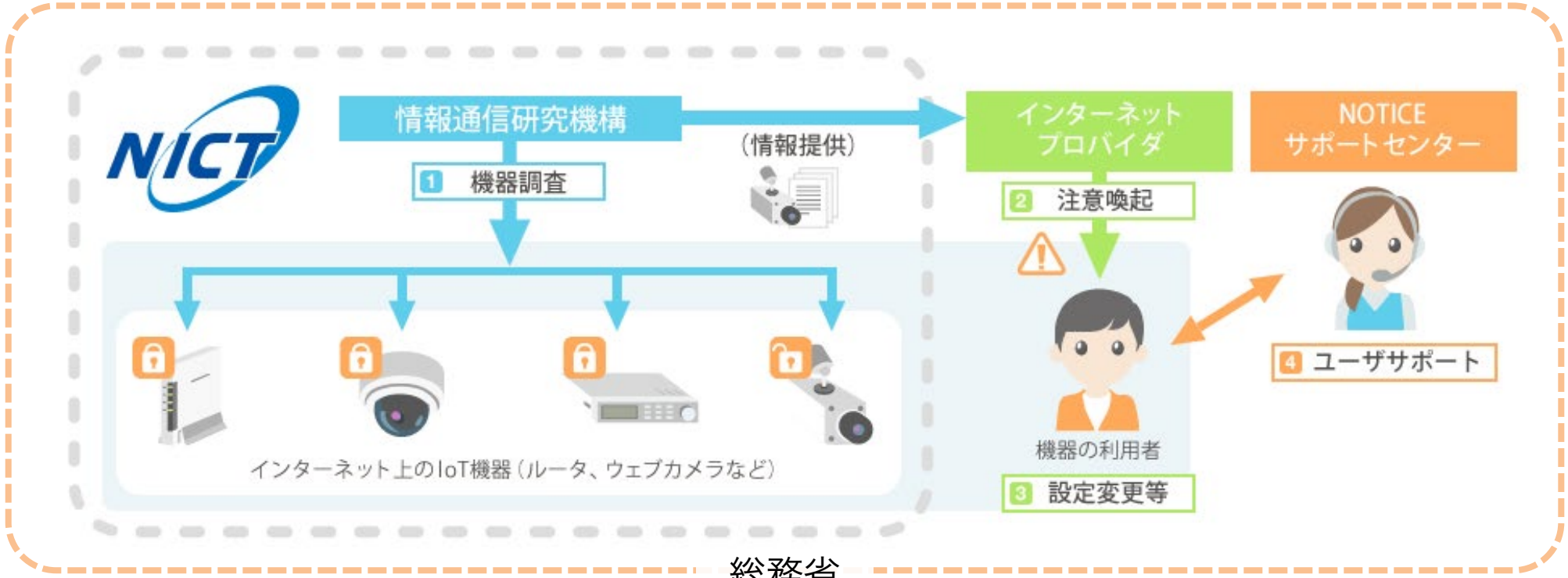
ISP



NICT National Institute of Information and Communications Technology

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



総務省

https://notice.go.jp/

NICT法改正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。

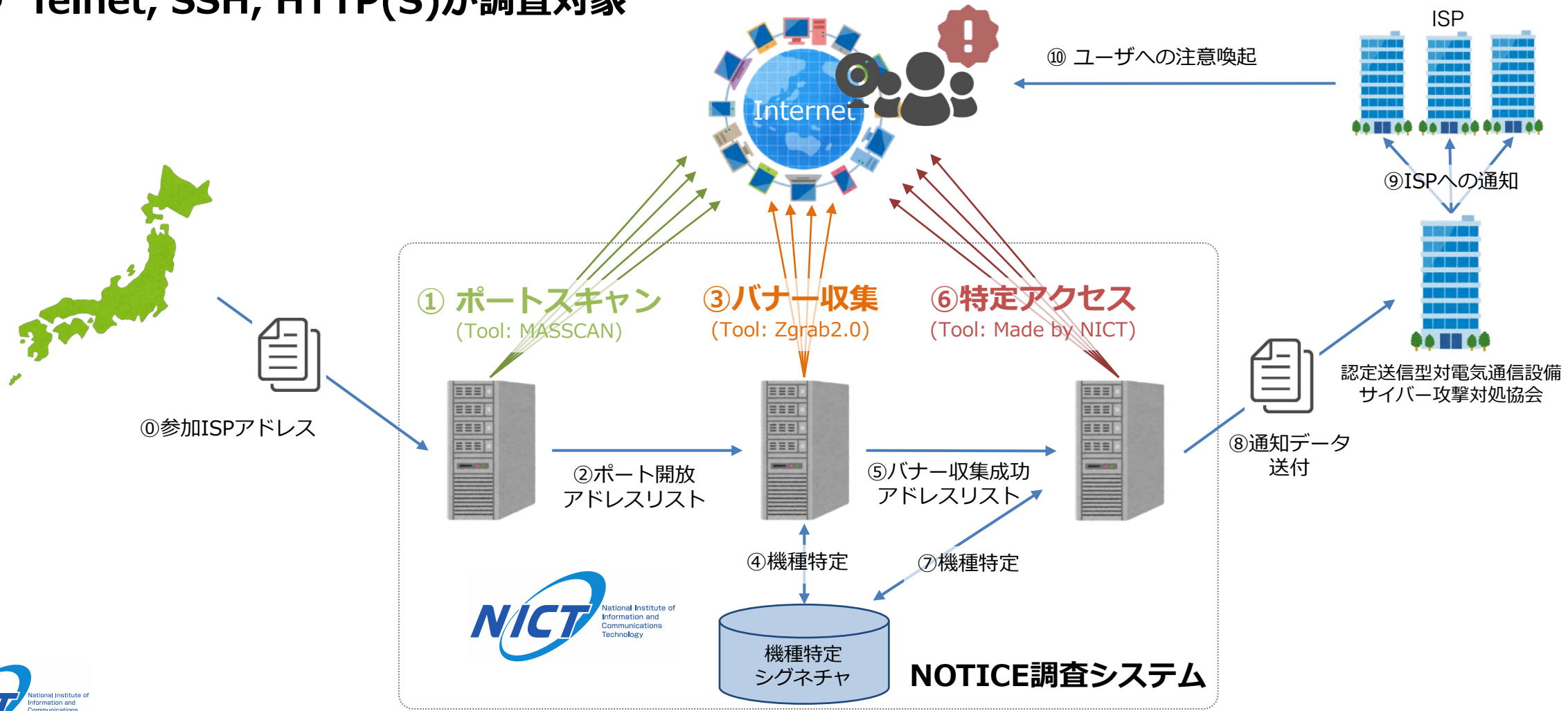
二　特定アクセス行為に係る電気通信の送信先の電気通信設備が次のイ又はロに掲げる者の電気通信設備であるときは、当該イ又はロに定める者に対し、通信履歴等の電磁的記録を証拠として当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする**送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行う**こと。

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

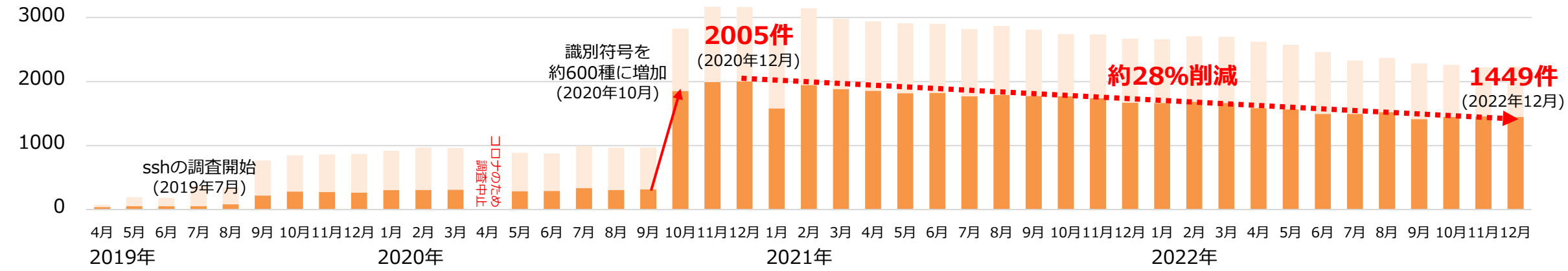
日本国内にあるID/パスワード設定不備の機器を調査

- 2023年3月時点で75社のISPが参画(約1.12億IPv4アドレスが対象)
- Telnet, SSH, HTTP(S)が調査対象



NOTICE調査結果の推移

- **Telnet/SSHに関して注意喚起対象数は約28%減少 (ピーク比)**
  - ✓ 新規ISPの追加や新たな機器が発見されるケースがあるため増加分も含む統計値であることに注意



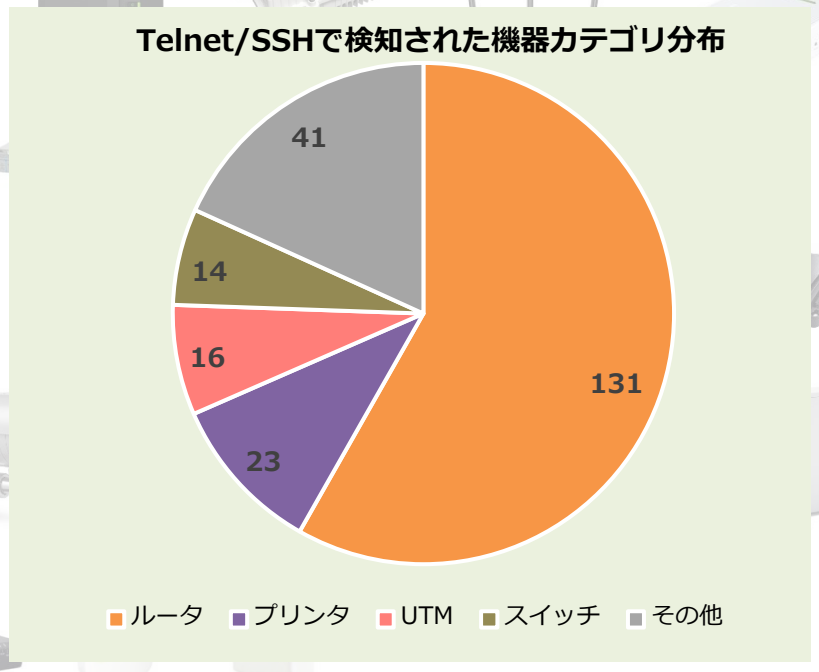
Telnet/SSHの注意喚起対象数の推移(月毎)

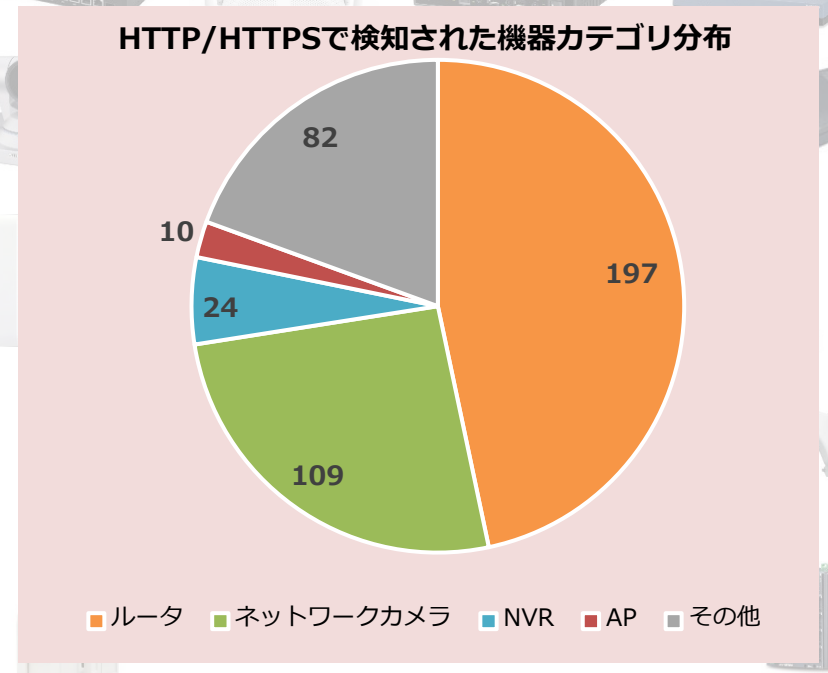
HTTP/HTTPS(Basic認証/Digest認証)の注意喚起対象数の推移(月毎)

NOTICEで発見した機器の機種特定に成功(約600機種)

パスワード設定不備のまま利用されている要因は様々なケースがある

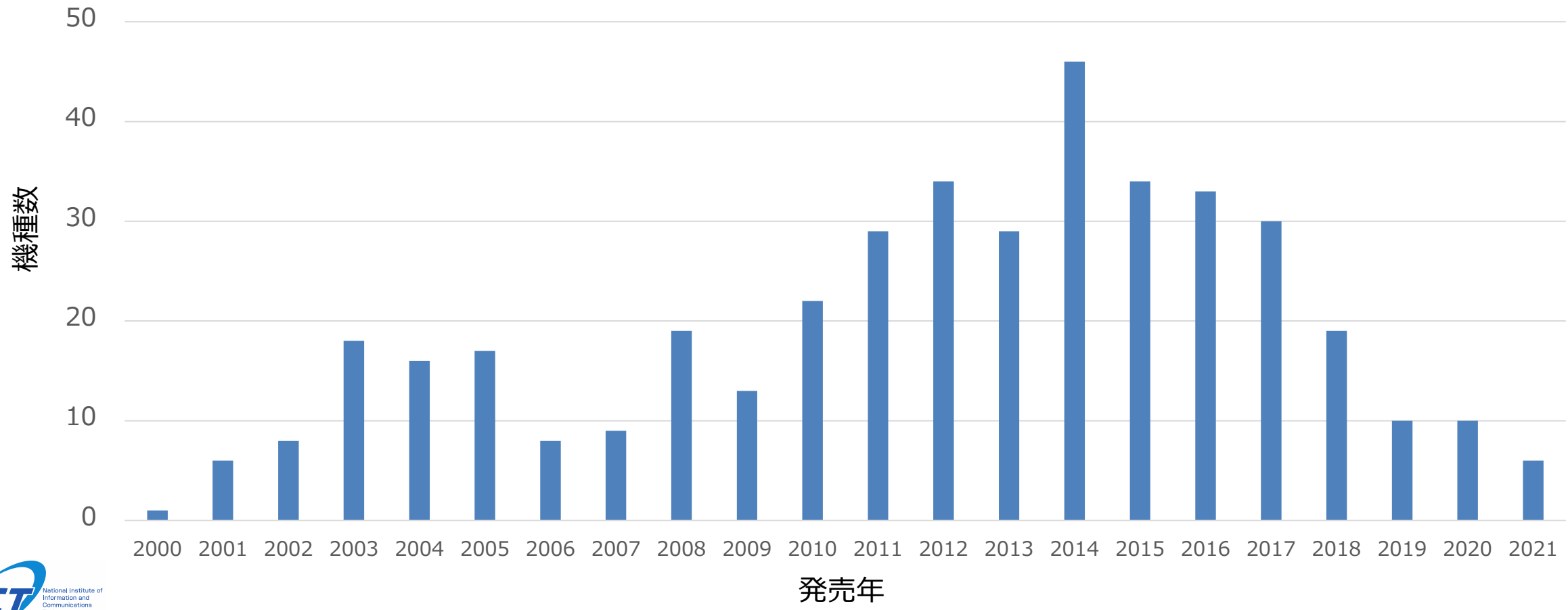
- 購入時の初期設定でポートが開いていて、パスワードを変えずに使っている
- パスワードを変更しているけど、簡単なパスワードを使っている
- 業者が設置した機器の保守管理アカウントが、簡単なパスワードを使っている
- 脆弱性がある機器が攻撃された結果、Telnetを起動されている
- etc.





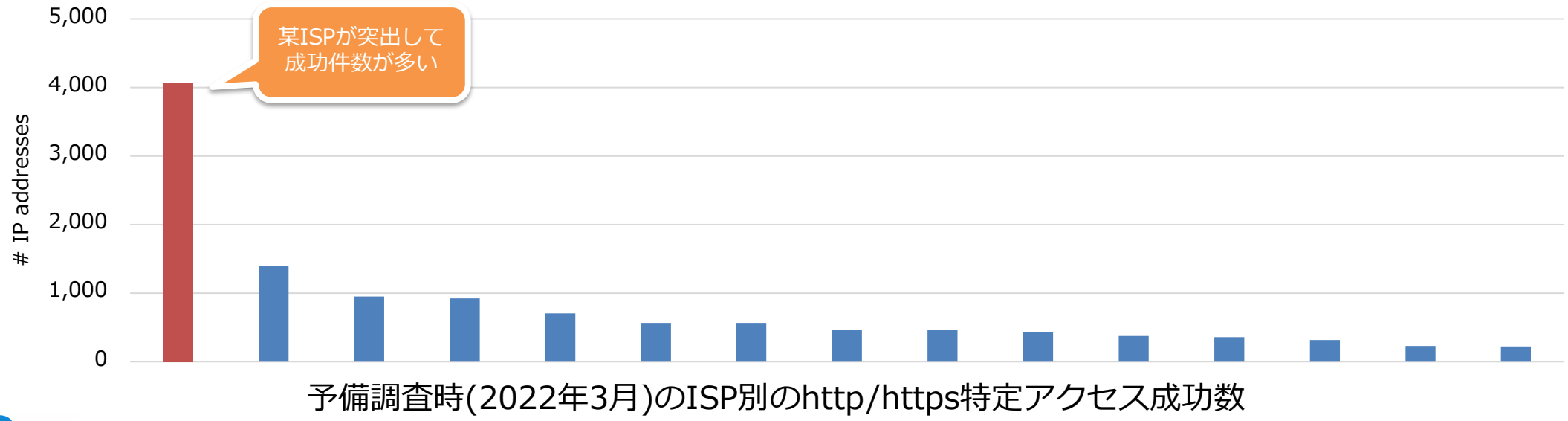
特定アクセスに成功した機器の発売年

- **約600機種のうち発売年が検索出来た約400機種の発売年分布**
  - ✓ 全体的に古い機器（多くが既にサポート切れ）が多数発見されている



ユーザ注意喚起無しでISPが直接対処した事例

- **2022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**



NOTICE調査から見える現状

- **ID/パスワード設定不備の機器は国内に相当数残存**
  - ✓Mirai登場から引き続き、IoT機器に対する主要な侵入経路
- **設定不備の要因は必ずしもユーザやベンダのみではなく様々**
  - ✓ユーザよりもインフラやサービス側の対応不備の方が影響範囲は大きくなる
- **普及後の事後的なセキュリティ対応は高コスト**
  - ✓ユーザ行動を促し適切な対処に繋げるのは容易ではない

スマートかつセキュアなIoT環境の実現に向けて

- **アタックサーフェスの最小化**
  - ✓適切なアクセス制御がリスク軽減には最重要
- **製造からEoLまでを見据えたセキュリティLCM**
  - ✓サプライチェーンリスク、SBOM、脆弱性対応、利用者への情報提供、etc.
- **セキュリティはベースラインであり、付加価値に**
  - ✓各種規制・ガイドライン制定の活発化、認証制度