NICTER観測で捉えた、日本国内の脅威2021

2021年11月24日

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
解析チーム

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

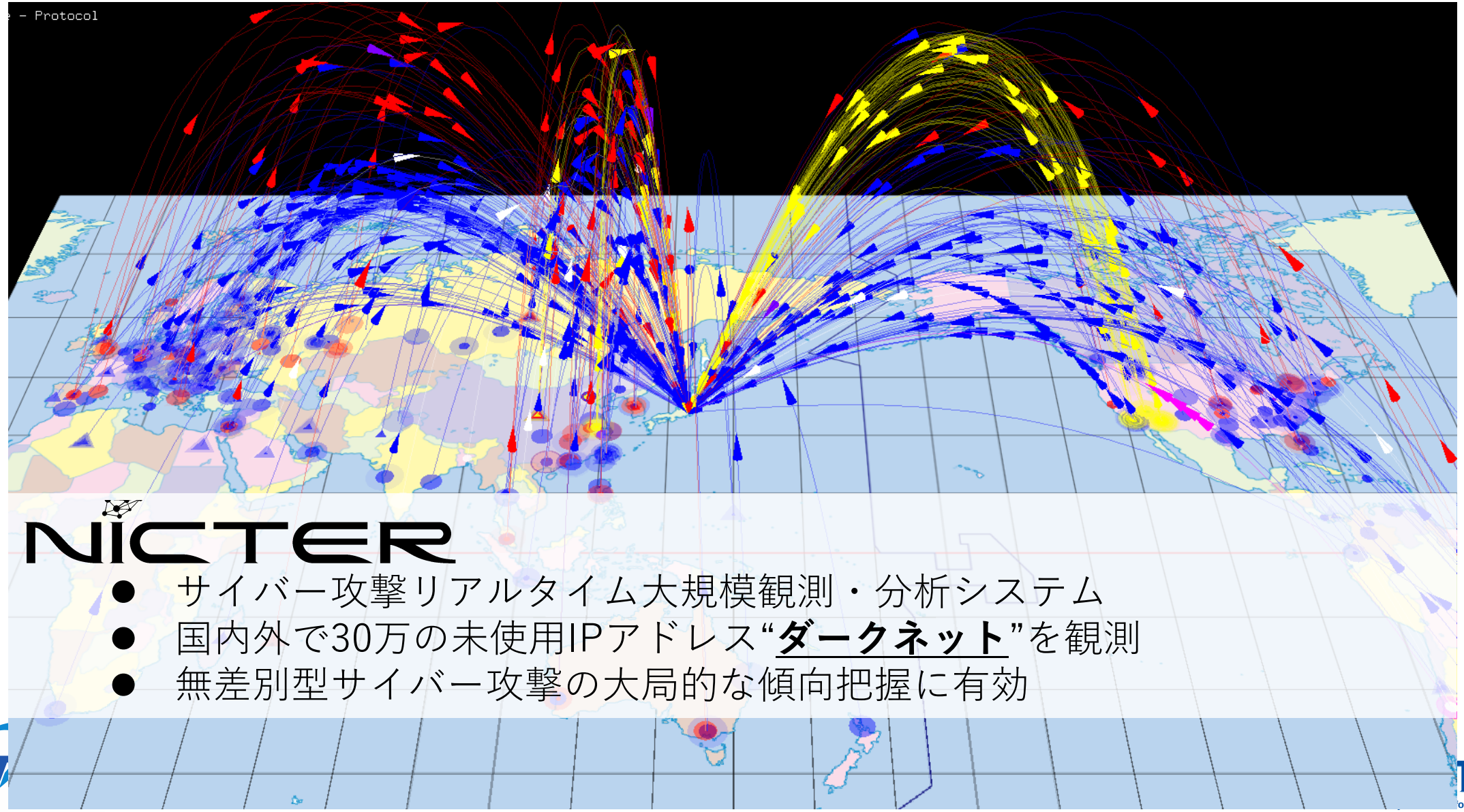
はじめに

- NICTではインターネット空間にばら撒かれるパケットを日々観測しています

- **パケットの特徴**や**送信元**を調査・分析することで，市場に出回る脆弱な機器の感染実態，マルウェアのトレンドなどを把握することができます

- 本日の講演では**2021年の日本の送信元の実態**を紹介します

NICTERダークネット観測

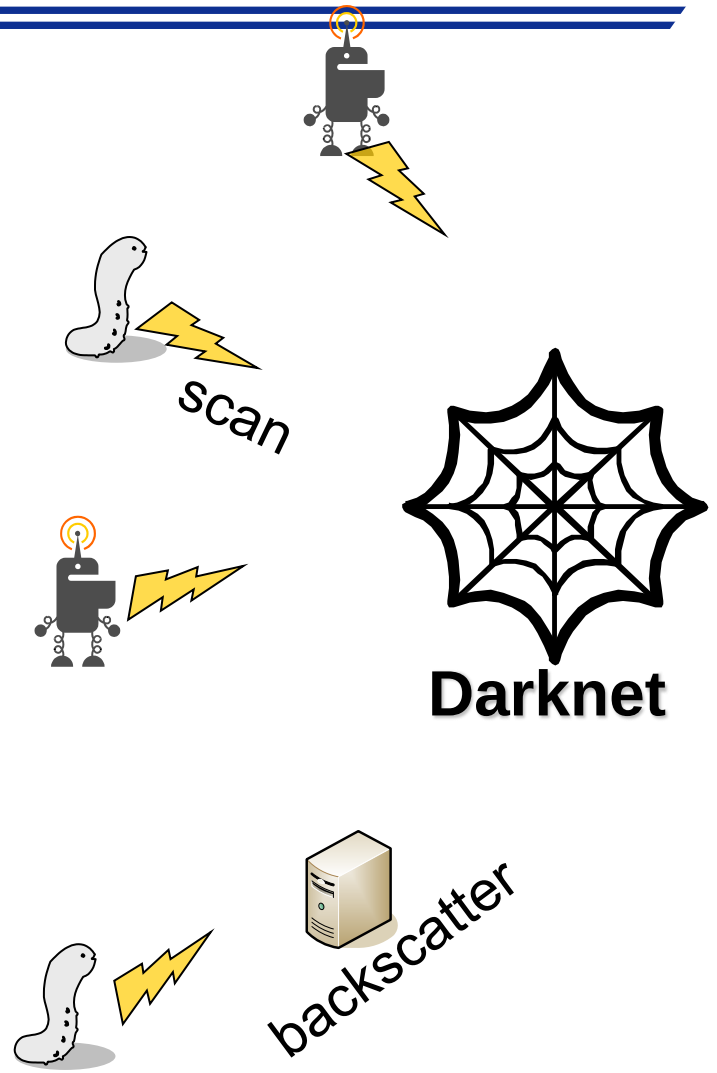


NICTER

- 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

ダークネット観測で見えるもの

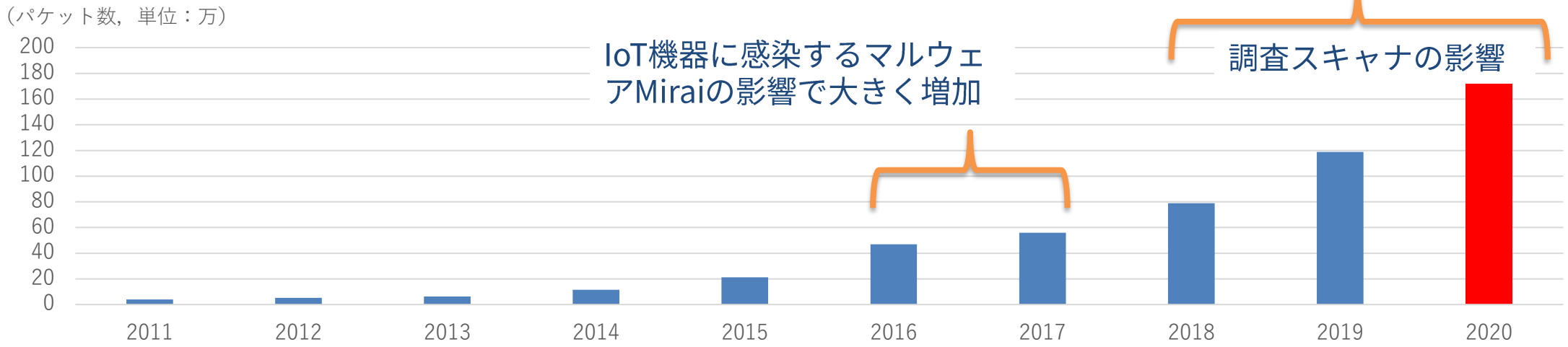
- インターネット上で何かを探す行為
  - ✓ ワーム型マルウェアによるスキャン
  - ✓ リフレクタ探索（DNS Open Resolver探索、NTP探索 etc.）
  - ✓ セキュリティ関連組織等による定期スキャン
- DoS攻撃の跳ね返り
  - ✓ DDoSバックスキャッタ
    - ※ 送信元IPアドレス偽装されたSYN Floodへの応答
  - ✓ DNS水責め攻撃のバックスキャッタ
    - ※送信元IPアドレス偽装されたランダムサブドメイン攻撃
- 設定ミス



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
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	約2,121億	約30万	789,876
2019	約3,220億	約30万	1,187,935
2020	約5,001億	約30万	1,820,722
2021（～9月末）	**約3,464億**	**約30万**	**1,302,822**

1アドレスあたり
18秒に1回
パケット受信



1 IPアドレス当たりの年間総観測パケット数

調査スキャナ

- 2018年頃から主に海外組織からの調査目的とみられるスキャンが急増

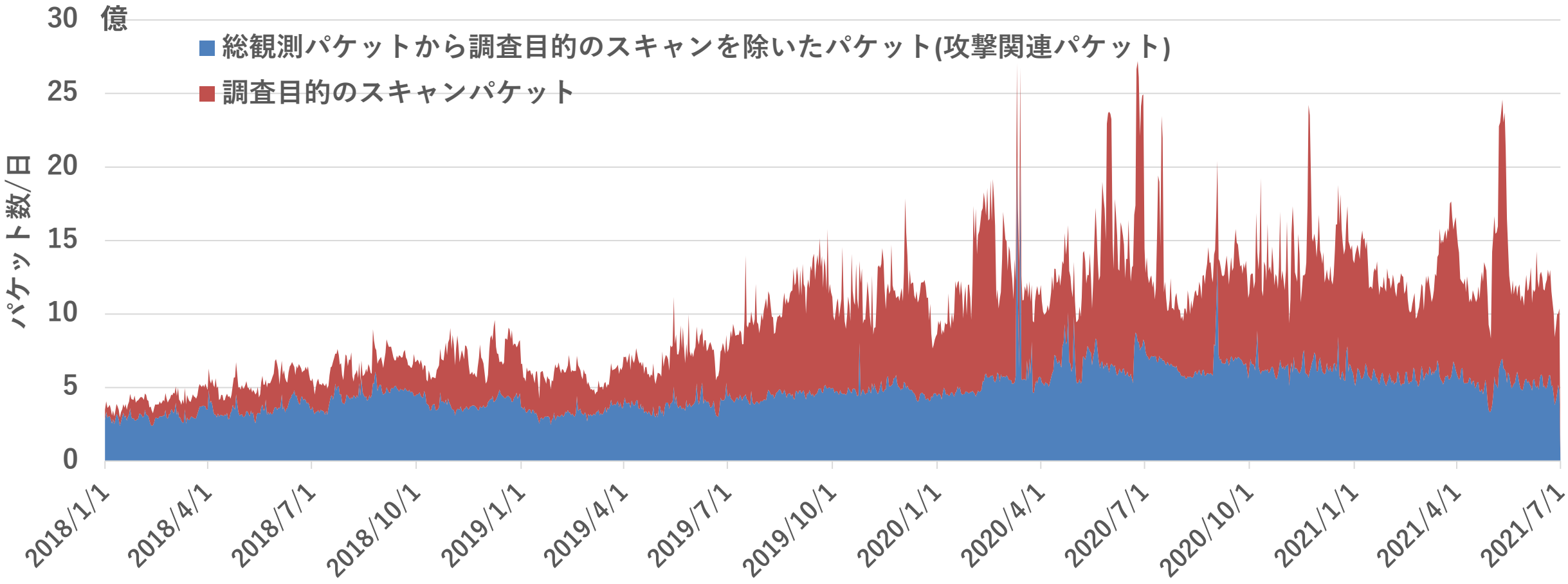
・・・

- 実行元が不明なIPアドレスが年間3,600以上観測されている（2020年）
  - 全ポートスキャン
  - 広域ネットワークスキャン
  - 1日に1億～4億パケット送信するIPアドレスも存在する

NICTER観測において、調査スキャナによるパケットはノイズ

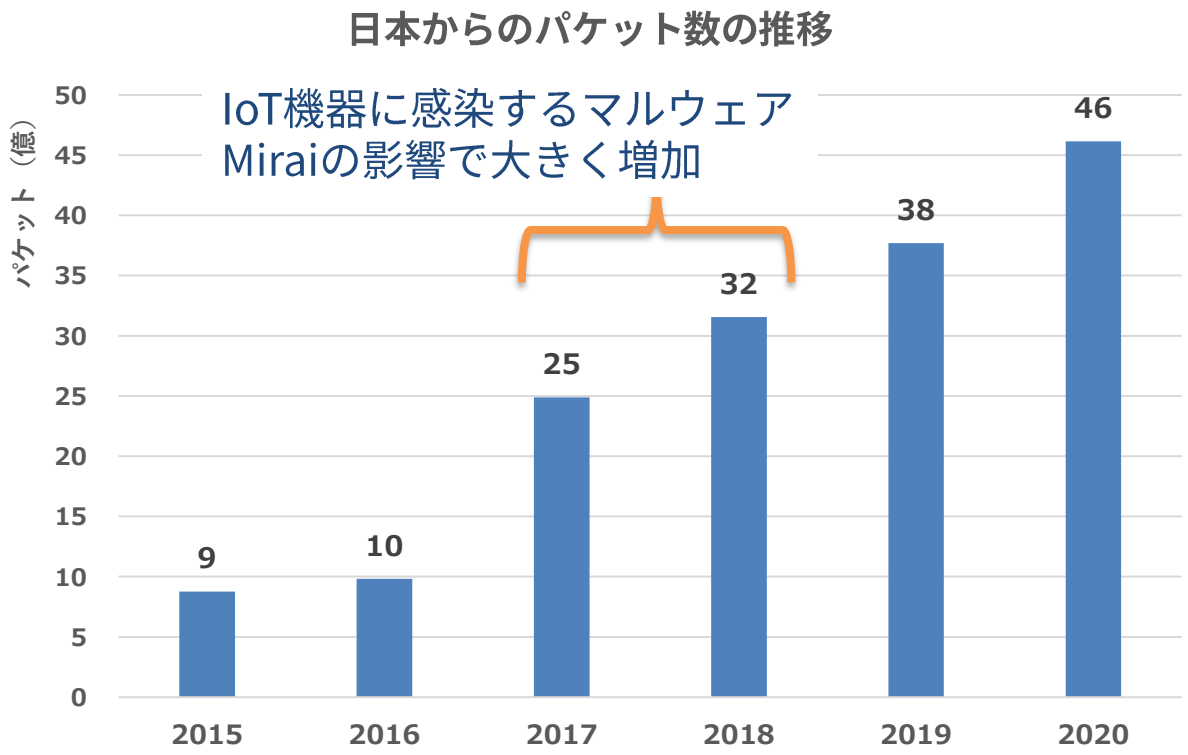
ネットワーク管理者、SOCの業務の支障にもなり得る

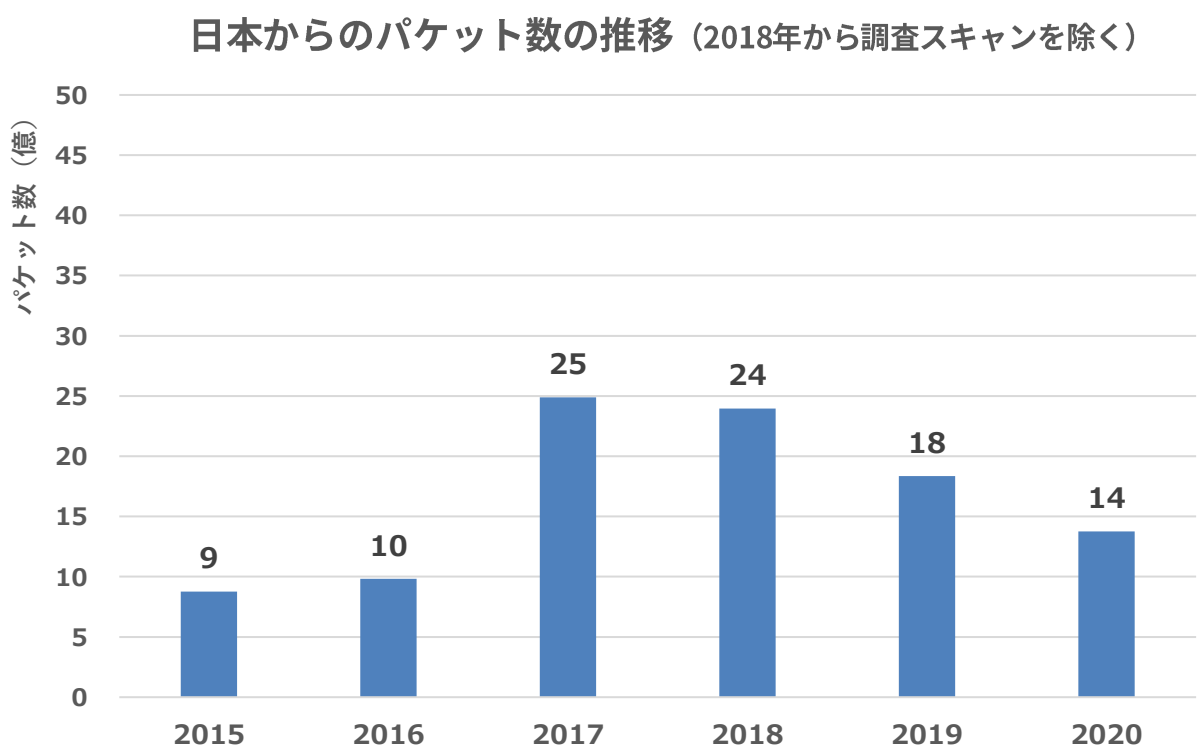
調査スキャンを除いた攻撃関連パケット数の実態



ここ3年の攻撃関連パケット数は緩い上昇傾向

日本の送信元からのパケット数





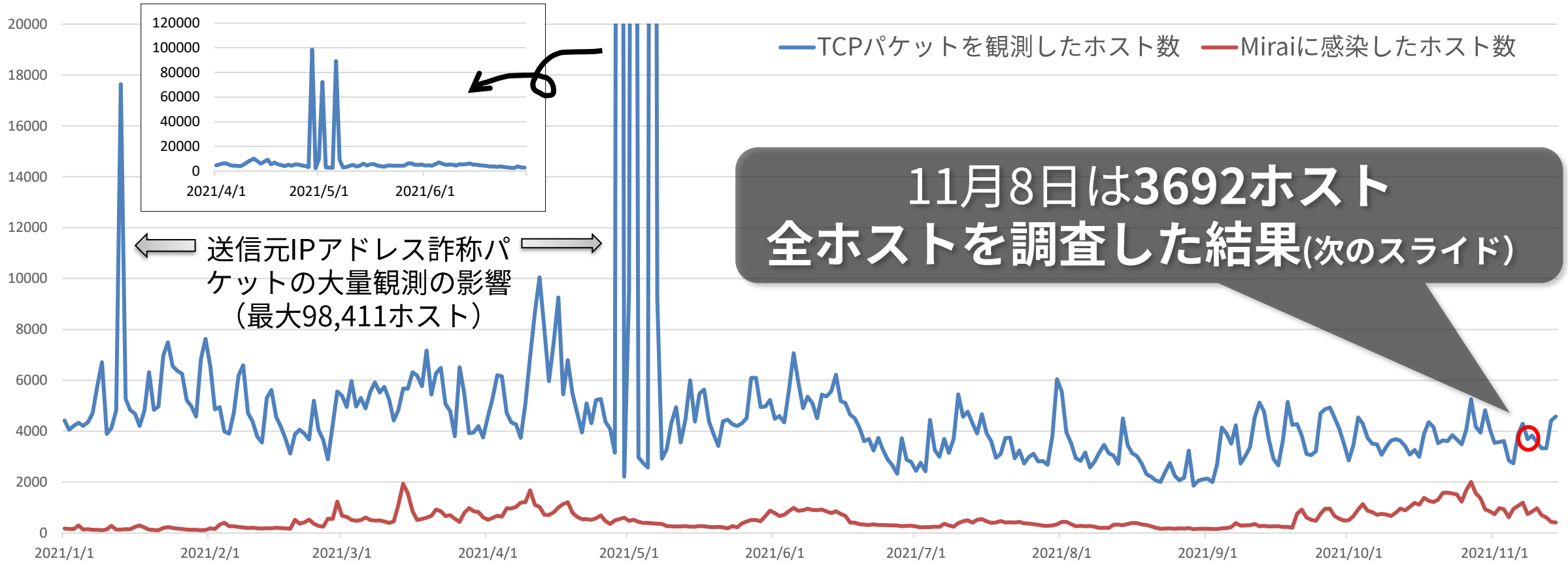
日本からのパケット数は世界全体と比較すると約 1～1.5% 程度

2019年、2020年は比較的落ち着いていた

National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

ダークネット宛にパケットを送信する日本国内のホスト



平均4300ホスト/日

（補足情報）
- 国判定はwhoisによる
- 詐称パケットの送信元IPアドレスも含む（TCPを1パケット以上観測した日本国内のホストをカウント
- UDPのみを送信するホストは除外（送信元詐称の可能性が高いため）

2021年11月8日の日本国内の全送信元ホストの内訳

ホスト数	送信元のホスト・機器	スキャンの宛先ポート	攻撃対象/サービス
494	Windowsなど(EoL製品含む)	{445}	Windows(SMB)
319	Miraiに感染したルーター	{23 2323}	IoT機器
212	BitTorrentのネゴシエーション？	{14830}	BitTorrentのネゴシエーション？
200	Miraiに感染したルーターとWebカメラ	{37215}	IoT機器
180	Miraiに感染したルータ	{23}	IoT機器
82	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス)
80	複数（サーバー、ラズパイ、OpenWRTなど）	{22}	SSH
68	[illegible]	{23 2323 37215}	IoT機器
43	半数が携帯キャリアA社	{80}	HTTP(宛先は単一のIPアドレス)
42	携帯キャリアA社	{389 7300 8080}	不明(宛先は単一のIPアドレス)
35	携帯キャリアA社	{7300}	不明(宛先は単一のIPアドレス)
33	マルウェアに感染したルータとDVRなど	{23 81}	IoT機器
31	Mirai感染端末（機器不明）	{5555}	Android OS搭載機器(ADB)
19	Windowsなど(EoL製品含む)	{3389}	Windows(RDP)
18	1/3がモバイル2社、パケット少数	{443}	HTTPS
14	不明（パケット少数）	{19927}	不明
14	マルウェア（Mozi系）感染端末	{37215 49152 52869 5555 7574 80 8080 81 8443}	IoT機器
13	マルウェアに感染したNASなど	{10000 2004 80}	不明
13	マルウェアに感染したルータとDVRなど	{23 26}	IoT機器
12	Windowsなど(EoL製品含む)	{1433}	Windows(MSSQL)
11	サムスン社製DVR	{81}	IoT機器
1759	不明	その他(ポートセットごとに10ホスト以下)	不明
計3692			

感染機器の実態

Exploitの宛先ポート・サービス

マルウェアの種類

Windowsの感染・攻撃の実態？

ホスト数	送信元のホスト・機器	スキャンの宛先ポート	攻撃対象/サービス
494	**Windowsなど**	**{445}**	**Windows(SMB)**
319	Miraiに感染したルーター	{23 2323}	IoT機器
212	BitTorrentのネゴシエーション？	{14830}	BitTorrentのネゴシエーション？
200	Miraiに感染したルーターとWebカメラ	{37215}	IoT機器
180	Miraiに感染したルータ	{22}	IoT機器
82	携帯キャリアA社	{80}	HTTP(宛先は単一のIPアドレス)
80	複数（サーバー、ラズパイ、OpenWRTなど）	{22}	SSH
68	Miraiに感染したルータ	{37215}	IoT機器
43	半数が携帯キャリアA社	{80}	HTTP(宛先は単一のIPアドレス)
42	携帯キャリアA社	{80}	HTTP(宛先は単一のIPアドレス)
35	携帯キャリアA社	{7300}	不明(宛先は単一のIPアドレス)
33	マルウェアに感染したルータとDVRなど	{23 81}	IoT機器
31	Mirai感染端末（機器不明）	{5555}	Android OS搭載機器(ADB)
19	**Windowsなど**	**{3389}**	**Windows(RDP)**
18	1/3がモバイル2社、パケット少数	{443}	HTTPS
14	不明（パケット少数）	{19927}	不明
14	マルウェア（Mozi系）感染端末	{37215 49152 52869 5555 7574 80 8080 81 8443}	IoT機器
13	マルウェアに感染したNASなど	{10000 2004 80}	不明
13	マルウェアに感染したルータとDVRなど	{23 26}	IoT機器
12	**Windowsなど**	**{1433}**	**Windows(MSSQL)**
11	サムスン社製DVR	{81}	IoT機器
1759	不明	その他(ポートセットごとに10ホスト以下)	不明
計3692			

- Windowsの感染，Windowsを狙う攻撃は過去も上位を占める
- Windows7などEOL製品の感染も確認

多様なIoT機器が感染しているという実態

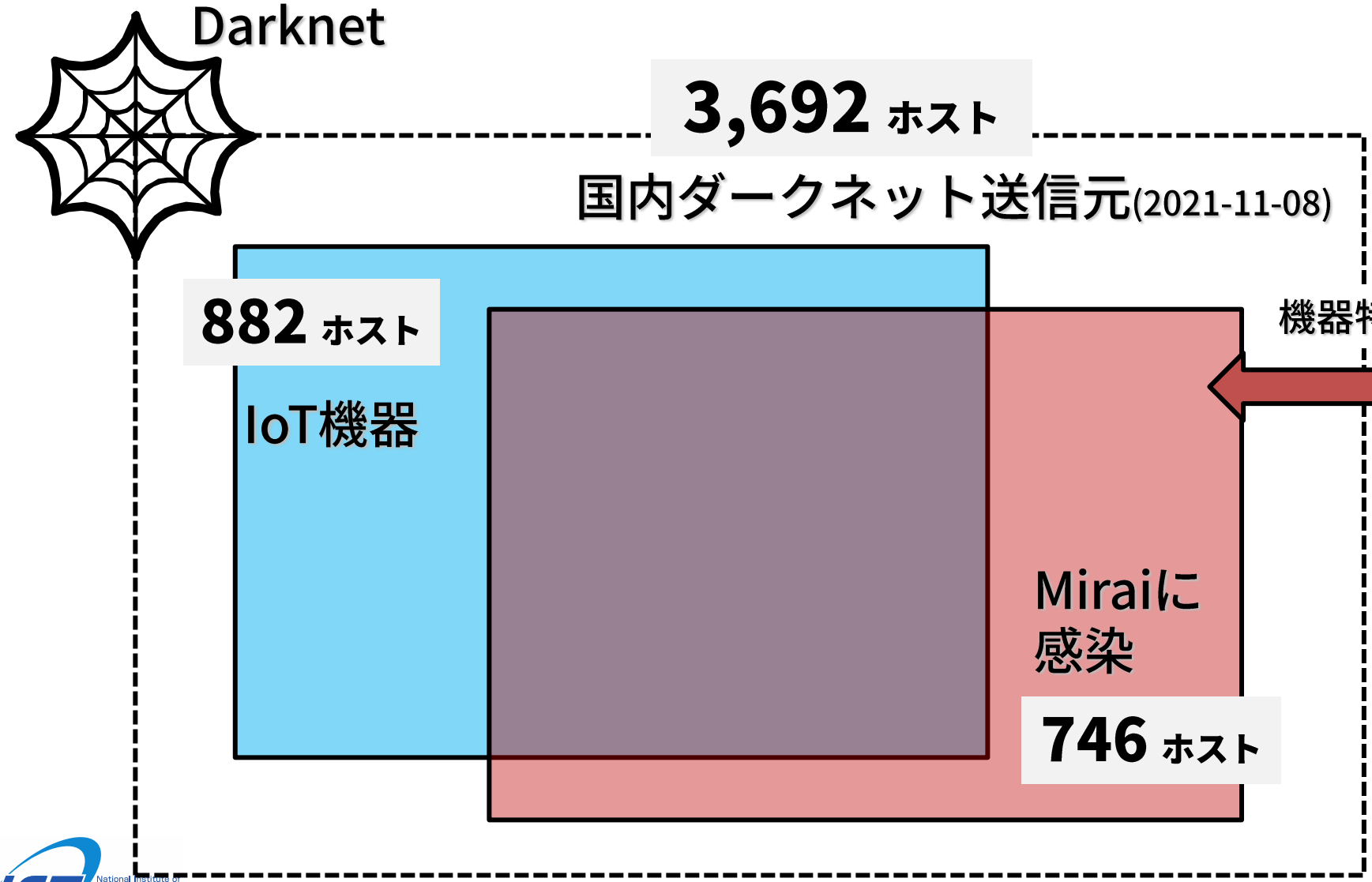
ホスト数	送信元のホスト・機器	スキャンの宛先ポート	攻撃対象/サービス
494	Windowsなど(EoL製品含む)	{445}	Windows(SMB)
319	**Miraiに感染したルーター**	**{23 2323}**	**IoT機器**
212	BitTorrentのネゴシエーション？	{14830}	BitTorrentのネゴシエーション？
200	**Miraiに感染したルーターとWebカメラ**	**{37215}**	**IoT機器**
180	**Miraiに感染したルータ**	**{23}**	**IoT機器**
82	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス)
80	複数（サーバー、ラズパイ、OpenWRTなど）	{22}	SSH
68	**Miraiに感染したルータ**	**{23 2323 37215}**	**IoT機器**
43	半数が携帯キャリアA社	{80}	HTTP(宛先は単一のIPアドレス)
42	携帯キャリアA社	{80 8080}	不明(宛先は単一のIPアドレス)
35	携帯キャリアA社	{7300}	不明(宛先は単一のIPアドレス)
33	**マルウェアに感染したルータとDVRなど**	**{23 81}**	**IoT機器**
31	**Mirai感染端末（機器不明）**	**{5555}**	**Android OS搭載機器(ADB)**
19	Windowsなど(EoL製品含む)	{3389}	Windows(RDP)
18	1/3がモバイル2社、パケット少数	{443}	HTTPS
14	不明（パケット少数）	{19927}	不明
14	**マルウェア（Mozi系）感染端末**	**{37215 49152 52869 5555 7574 80 8080 81 8443}**	**IoT機器**
13	**マルウェアに感染したNASなど**	**{10000 2004 80}**	**不明**
13	**マルウェアに感染したルータとDVRなど**	**{23 26}**	**IoT機器**
12	Windowsなど(EoL製品含む)	{1433}	Windows(MSSQL)
11	**サムスン社製DVR**	**{81}**	**IoT機器**
1759	不明	その他(ポートセットごとに10ホスト以下)	不明
計3692			

882ホスト/全体の23%がIoT機器

機器や原因の特定に結びつかない事象もそれなりにある

ホスト数	送信元のホスト・機器	スキャンの宛先ポート	攻撃対象/サービス
494	Windowsなど(EoL製品含む）	{445}	Windows(SMB)
319	Miraiに感染したルーター	{23 2323}	IoT機器
212	**BitTorrentのネゴシエーション？**	**{14830}**	**BitTorrentのネゴシエーション？**
200	Miraiに感染したルーターとWebカメラ	{37215}	IoT機器
180	Miraiに感染したルータ	{23}	IoT機器
82	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス）
80	**複数（サーバー、ラズパイ、OpenWRTなど）**	**{22}**	**SSH**
68	Miraiに感染したルータ	{23 2323 37215}	IoT機器
43	**半数が携帯キャリアA社**	**{80}**	**HTTP(宛先は単一のIPアドレス）**
42	**携帯キャリアA社**	**{389 7300 8080}**	**不明(宛先は単一のIPアドレス）**
35	**携帯キャリアA社**	**{7300}**	**不明(宛先は単一のIPアドレス）**
33	マルウェアに感染したルータとDVRなど	{23 81}	IoT機器
31	Mirai感染端末（機器不明）	{5555}	Android OS搭載機器(ADB)
19	Windowsなど(EoL製品含む）	{3389}	Windows(RDP)
18	1/3がモバイル2社、パケット少数	{443}	HTTPS
14	**不明（パケット少数）**	**{19927}**	**不明**
14	マルウェア（Mozi系）感染端末	{37215 49152 52869 5555 7574 80 8080 81 8443}	IoT機器
13	マルウェアに感染したNASなど	{10000 2004 80}	不明
13	マルウェアに感染したルータとDVRなど	{23 26}	IoT機器
12	Windowsなど(EoL製品含む）	{1433}	Windows(MSSQL)
11	サムスン社製DVR	{81}	IoT機器
1759	**不明**	**その他(ポートセットごとに10ホスト以下）**	**不明**
計3692			

日本国内の感染機器の傾向

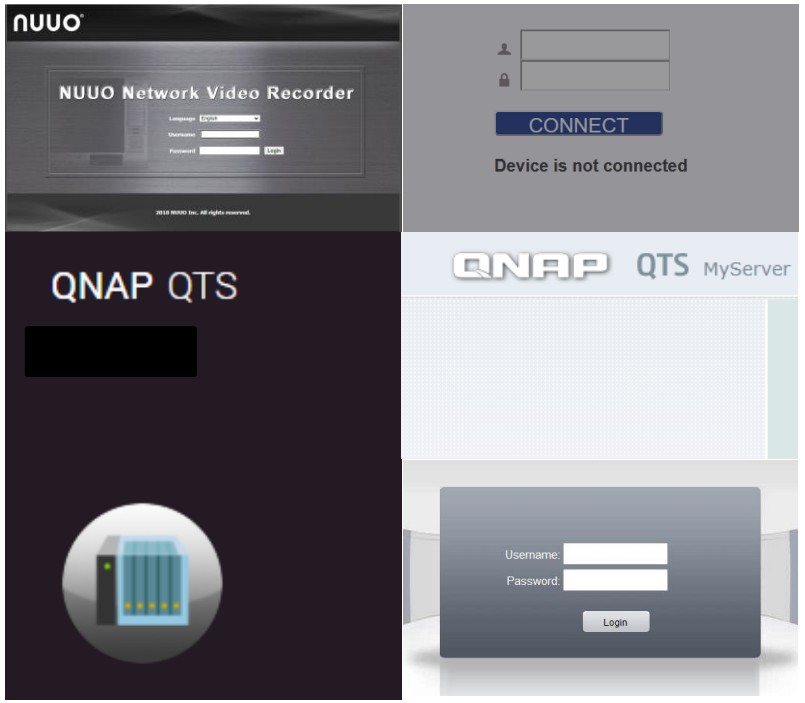


- shodan,censys, KARMA
- HTTP(80/tcp), other open ports
- source port, address

609ホストを機器特定

Miraiに感染していた609台ホストの内訳

	機器名	ホスト数
ルータ	Logitec製	267
	メーカー・機種不明	41
	Buffalo製	16
	モバイルルータ（複数）	3
	エレコム製	1
	IPアドレス変動（Logitec含む）	118
Webカメラ	VSTARCAM	112
	CMS_WebViewer	21
	防犯カメラ製品（複数）	15
	Nuuo	9
NAS	QNAP製NAS	6
不明	不明（接続不可など）	137



防犯カメラ製品/NAS製品の中には、
・shodanにカメラ映像が掲載されてしまっている
・企業名と場所が設定されており、有名企業の物流センターで使われていることがわかる
・プライベートの写真がWeb（80/TCP）のログイン画面に設定されているものもあり

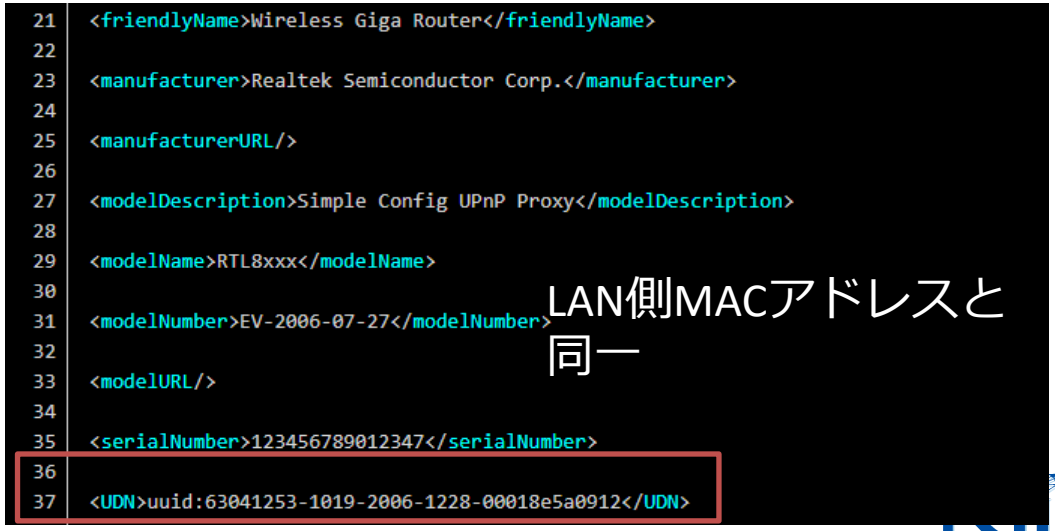
感染数最多のルータ：ロジテック社製ルータ

- 2009年8月販売のLAN-W300シリーズ
- 2012年、外部から管理画面に外部からアクセス可能な脆弱性※1が公開された
  - 外部からPPPoEの接続情報が取得できるため問題に
- 2017年12月、UPnPを利用した脆弱性※2が公開
- 2017年以降、NICTERダークネットにおいてLogitecを送信元と思われるMiraiのスキャンを観測．現在も観測を継続
  - 2017年の観測当初には特別レポート※3を公開

- ※1 https://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-000051.html
- ※2 https://www.logitec.co.jp/info/2017/1219.
- ※3 https://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf

ロジテック製ルータの特定方法

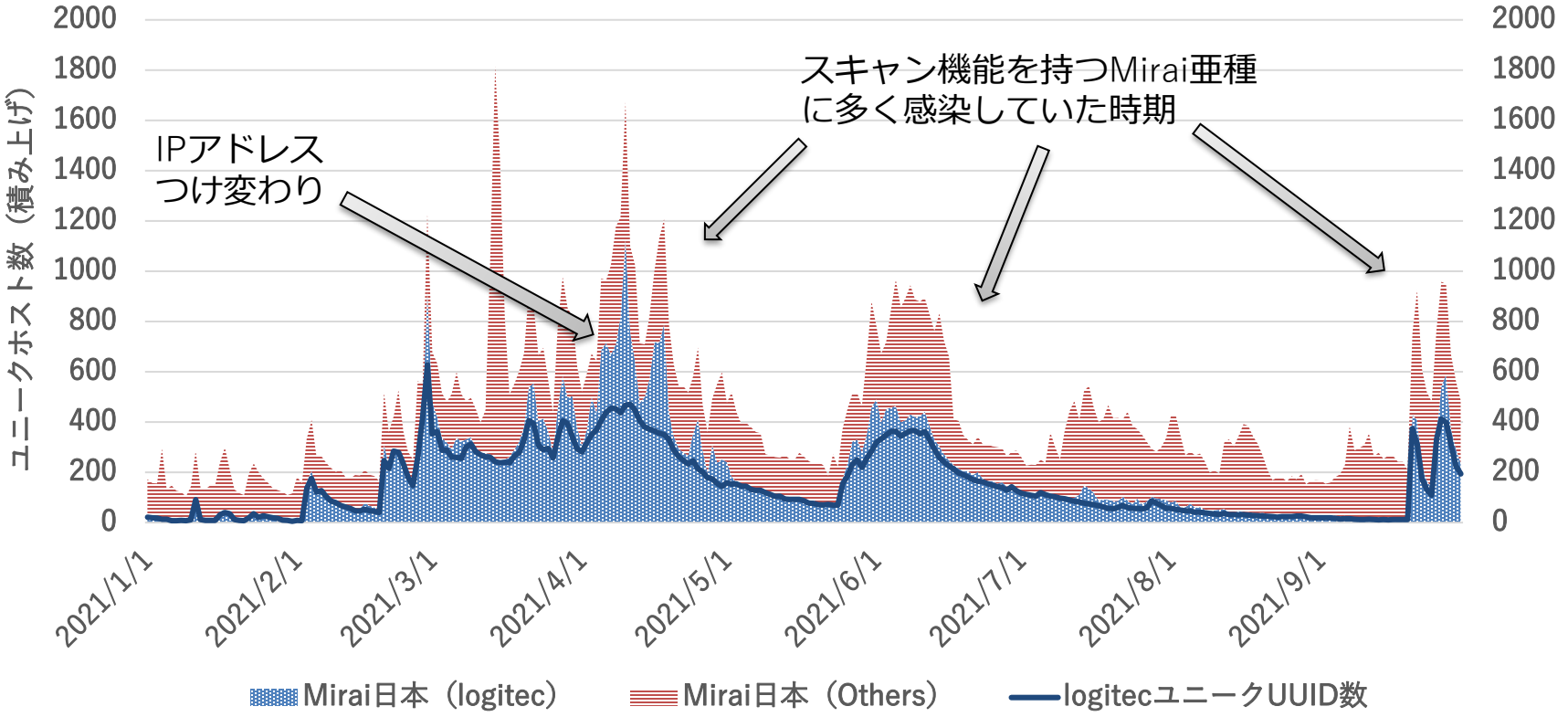
- バナー情報（device description）に含まれるUUIDの下12桁は MACアドレス
  - UUIDバージョン1の場合
  - MACアドレスの上位3オクテット（ベンダID）を調べることで機器ベンダを特定できる
    - ロジテック製ルータの場合，ベンダID が00018e



ロジテックルータの推移と特徴

- NICTERでロジテックルータへの感染が確認されたのは2017年11月　～現在も継続～
  - 国内で動作している感染機器の情報を収集（2020年8月～）
  - 調査対象： Miraiの特徴をもつパケットの送信元 IP アドレス（日本のみ）
  - 調査方法： Mirai感染ホストの52881/TCPにHTTPプロトコルでアクセスし，UPnP Descriptionファイルを収集

※UUID（Universally Unique Identifier）の値から
グローバル IP アドレスが変わったとしても同じ機器と推定可能



ロジテックの Mirai 感染台数

- 1日当たり約20~500
- 2021/1/1-9/30の9か月間に
  観測したユニーク台数は 1,905

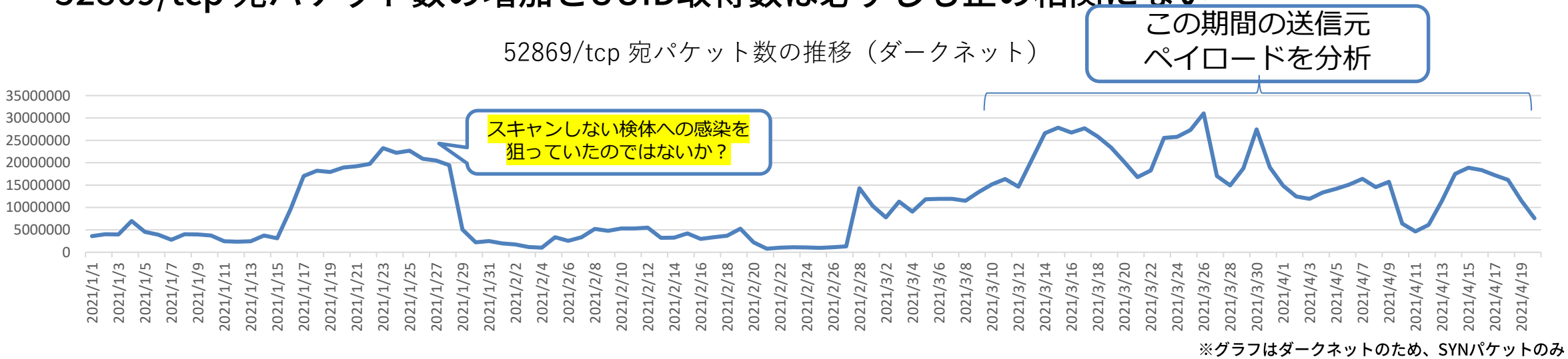
何らかの原因で**グローバルIPアドレスの変動が発生**することがある

複数の攻撃グループが
脆弱な機器を奪いあっている
（スキャンする/しない検体が混在）

NICTER
Network Incident analysis Center for Tactical Emergency Response

ロジテック製ルータを狙う52869/tcp 宛通信_参考

- 52869/tcp 宛パケット数の増加とUUID取得数は必ずしも正の相関にない

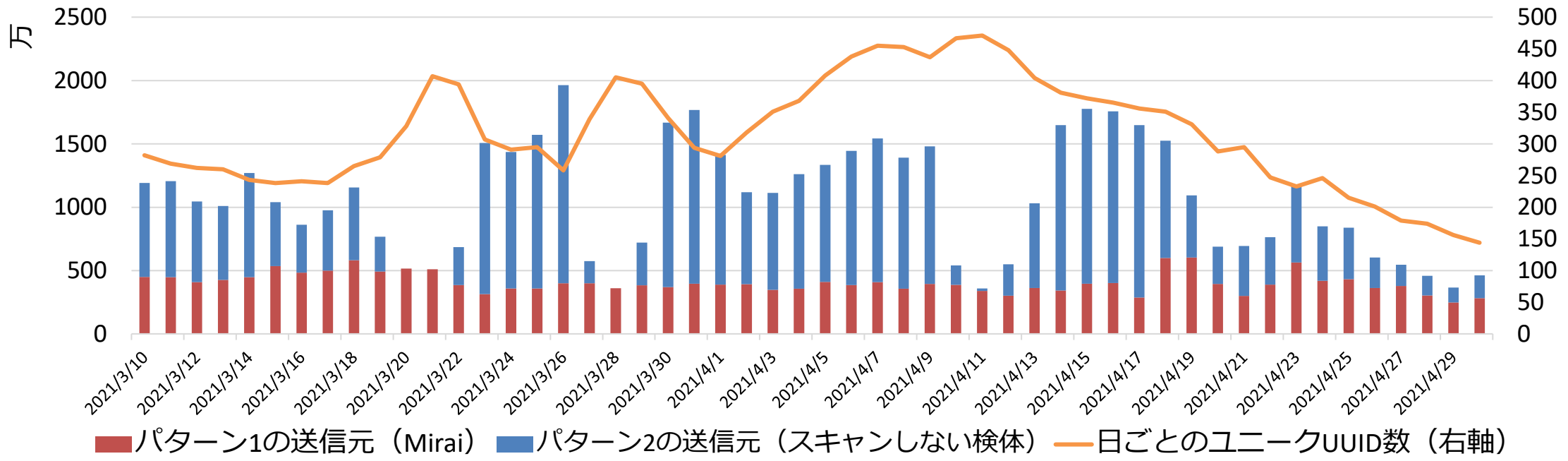


※グラフはダークネットのため、SYNパケットのみ

- 3/10～4/30に観測されたパケットの90%以上が，たかだか 19 の IPアドレスから届いていた
- 全ポート応答型ハニーポットでこれら19のIP アドレスから届いたペイロードを確認したところ，以下の3パターンに分類できることが判明した
  1. 脆弱性を悪用し，スキャン機能を有するマルウェア（Mirai）への感染を狙う
  2. 脆弱性を悪用し，スキャン機能を持たないマルウェアへの感染を狙う
  3. SYNスキャンのみ(Shodan,Censysなど)
- **パターン1に感染した場合のみ，ダークネットで観測される**

52869/tcp 宛通信とユニークUUID数の増加に関する考察

- パターン1の送信元（Mirai）＋パターン2の送信元（スキャンしない検体）+1ホストからの大量のSYNパケットの3種類（計11ホスト）がNICTERダークネットの52869/tcp 宛通信の93%を占める
  ※大量のSYNパケットを送っていた1ホストおよびその他の約7%のパケットは以下のグラフから除外



※1.パターン2に感染するとネットワークスキャンを行わないため，ダークネットで観測できなくなる

※2.4月上旬はパターン2のダウンロードサーバがダウンしていたため，
パターン2のパケット数は多かったが感染しなかったと考えられる

ユニークUUIDの数からパターン1とパターン2で機器の奪い合いが発生していると考えられる

感染数最多のWebカメラ：VSTARCAM

- 2017年、盗撮や遠隔操作されるということでテレビにも取り上げられた
- 「NICTER観測レポート2017」でもマルウェアに感染することを紹介
- 一部の販売代理店からは、修正済みのファームウェアも提供されているが現在でもAmazon等でバージョン/サポートが不明なものを購入可能

Shodanのバナー情報

2019年4月には、マルウェアに感染したと思われるレビュー
2020年5月でも「勝手に動いた」というレビューも…

参考:実機を使ったハニーポット

※カメラのレンズは
塞いであります

ホワイトリスト方式のファイアーウォール環境にて
攻撃者からの通信を招き入れています。

まとめ

日本国内では(EoLを迎えた)脆弱なIoT機器が多数マルウェアに感染．攻撃インフラを形成
- 平均600台/日
- 約2000台のいまだに脆弱なロジテックルータ
- 世界全体では5万～10万台がいまだMirai に感染．Dyn/DDoS規模の攻撃インフラは健在

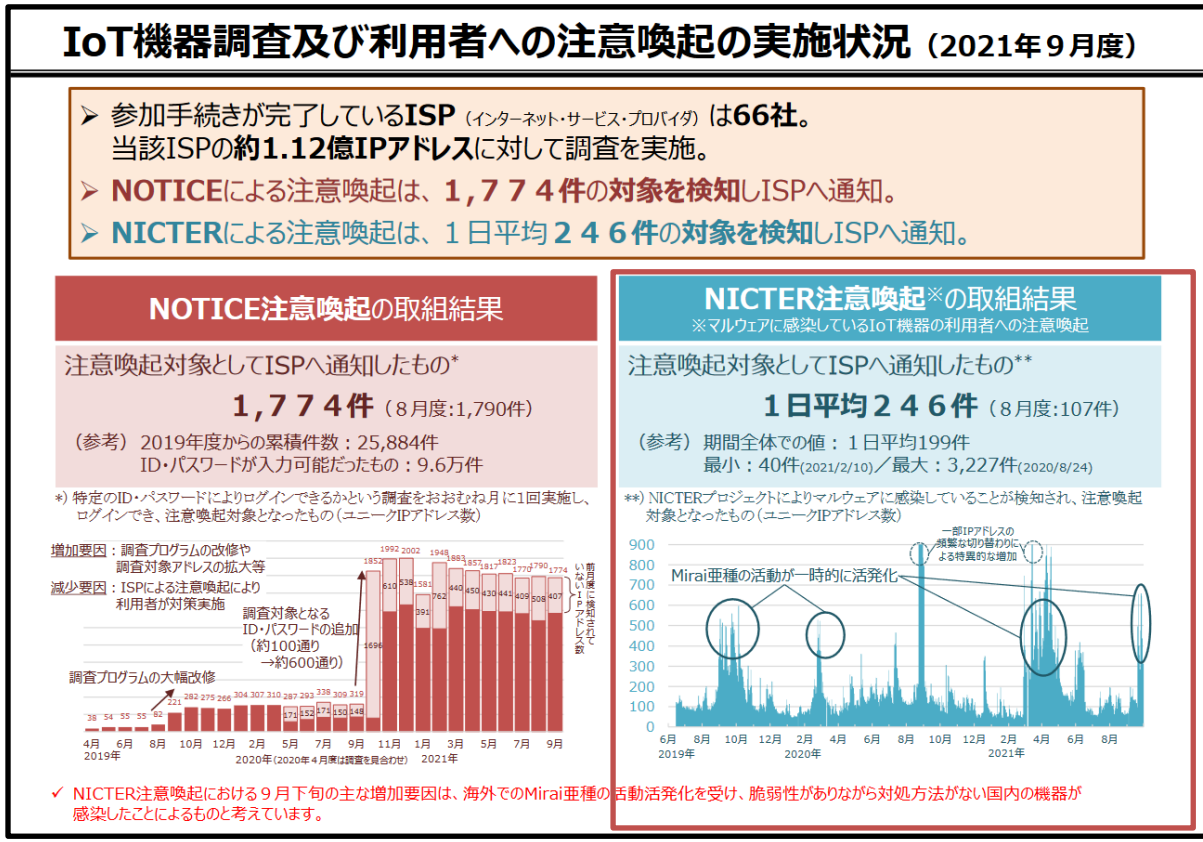
複数のIoTマルウェアが脆弱な機器を奪い合っている
- 脅威は常に変化
- より高度なNICTERでは観測できない攻撃も（ex. VPNFilter)

当たり前の対策以外の有効な手立てがないのが現状
- パスワードの変更
- ファームウェアの更新
- 本当に機器をインターネット晒す/インターネットからアクセス可能にする必要があるのか？再考を！
  - モバイル回線で繋がるデジタルサイネージがマルウェアに感染していた事例
  - デフォルトのパスワード
  - 防犯カメラやNAS製品からは、映像や写真も漏洩している可能性がある

脆弱性の機器を減らす取り組み

- NICTERデータを使用した注意喚起
  - NOTICE（右側赤枠）
    - Miraiに感染している機器全般
  - 解析チーム
    - Miraiに感染した機器の個別調査
    - Mirai以外のマルウェアに感染している機器（サーバ含む）

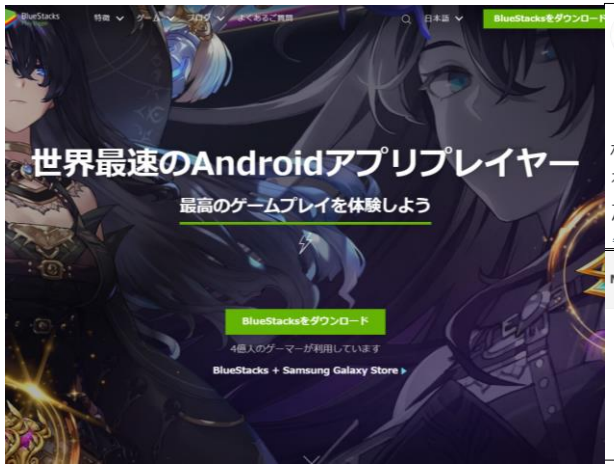
二つの手段で注意喚起を実施中



引用元:https://notice.go.jp/status

解析チームの活動（一例）

Androidエミュレータの脆弱性に関しての対応



攻撃対象となってしまった事例

Androidエミュレータに脆弱性があり、外部から認証なしで不正なプログラムの実行などをすることができた。開発元に修正およびバージョンアップ対応をしていただき、開発元のTwitterおよび解析チームのBlogにて注意喚起を実施

デジタルサイネージへのマルウェアの感染事例への対応

攻撃元として利用されてしまった事例

NICTERへ国内のモバイル回線からのパケットを観測機器の設置場所が分かる情報があったため、設置者から購入元を教えていただき、製造元/販売元へ修正対応および購入者への注意喚起をお願いした。

ルータ製品やテレビ視聴用のセットトップボックスなどでも
製造元/販売元へ情報共有をして脆弱性修正や注意喚起を依頼

情報発信（参考）

- Twitter
  https://twitter.com/nicter_jp
  ダークネットで観測した情報や
  Blog化が難しい事象などについて呟いてます。

- NICTER Blog
  https://blog.nicter.jp/
  Twitterには書ききれない統計情報や個別の機器
  NICTのSoCで観測した情報を掲載してます。

ご清聴ありがとうございました。