大規模攻撃観測から読み解く サイバー攻撃の地理的傾向と最新動向

2025年10月1日@日本銀行金融研究所 情報セキュリティ・セミナー

笠間 貴弘

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 室長

NICT National Institute of Information and Communications Technology

CYBERSECURITY Laboratory

Who am I

笠間 貴弘（かさま たかひろ）

国立研究開発法人情報通信研究機構(NICT)
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　室長

研究分野：サイバーセキュリティ(サイバー攻撃観測、マルウェア解析, IoTセキュリティ, etc.)

経歴：

- ✓ 横浜国立大学 博士課程前期修了後、2011年にNICTサイバーセキュリティ研究室にパーマネント研究員として入所。
- ✓ 大学時代より一貫してサイバーセキュリティ分野の研究開発に従事し、 2024年4月より現職。博士(工学) 。
- ✓ NICTERやWarpDriveなどの研究開発を推進。2019年よりIoT機器調査プロジェクトNOTICEの立ち上げを牽引。

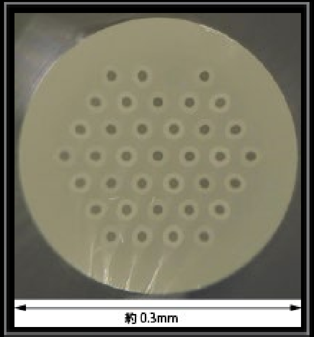
委員等：

- ✓ IPA セキュリティ要件適合評価及びラベリング制度における 通信機器適合基準検討WG 主査（2025年1月～）
- ✓ 東京電機大学 客員准教授 (2015年4月～2022年3月)
- ✓ 情報処理学会 マルウェア対策研究人材育成ワークショップ(MWS)委員 (2013年～。2017年実行委員長)
- ✓ 電子情報通信学会 ICSS研究会幹事 (2016年～2023年)
- ✓ 若手セキュリティイノベーター育成プログラムSecHack365トレーナー (2017年～2023年)
- ✓ etc.

国立研究開発法人 情報通信研究機構とは？

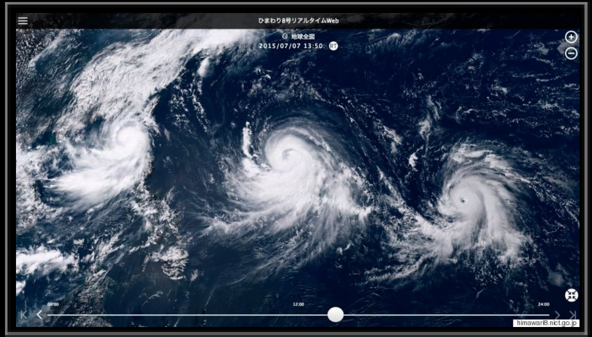
● 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入の様子）

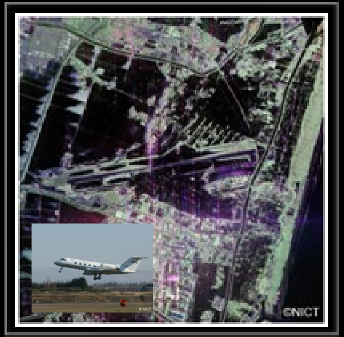


光通信システム
（ペタbps級 マルチコアファイバ）

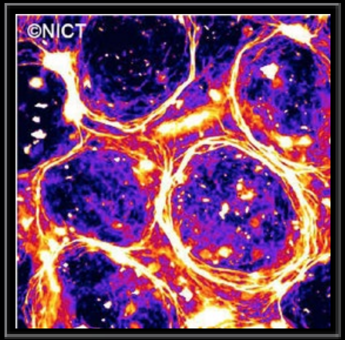
宇宙通信システム
（超高速インターネット衛星きずな）



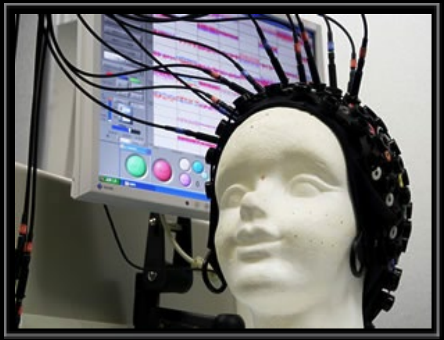
サイエンスクラウド
（ひまわり8号リアルタイムWeb）



電磁波センシング
（Pi-SAR2による3.11直後の仙台空港）



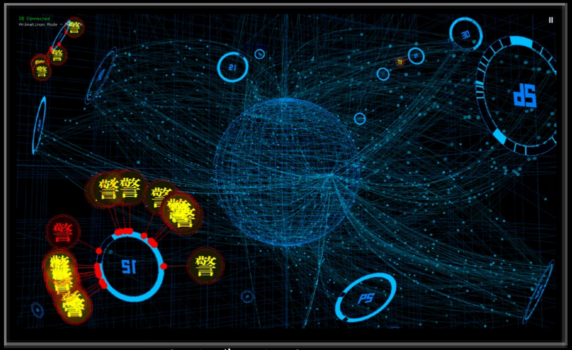
バイオ・ナノICT
（生体分子の自己組織化）



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）

NICT サイバーセキュリティ研究所

CYBERSECURITY Research Institute
サイバーセキュリティ研究所
(CSRI)

CYBERSECURITY Laboratory	SECURITY FUNDAMENTALS Laboratory	National Cyber Training Center	NATIONAL CYBER OBSERVATION CENTER	CYNEX CYBERSECURITY NEXUS	CREATE Center for Research on AI Security and Technology Evolution
サイバーセキュリティ研究室 (CSL)	セキュリティ基盤研究室 (SFL)	ナショナルサイバートレーニングセンター (NCT)	ナショナルサイバーオブザベーションセンター (NCO)	サイバーセキュリティネクサス (CYNEX)	AIセキュリティ研究センター (CREATE)
攻撃観測 分析・対策研究	暗号研究	セキュリティ人材育成	IoT機器セキュリティ対策	産学官連携拠点形成	AIセキュリティ研究

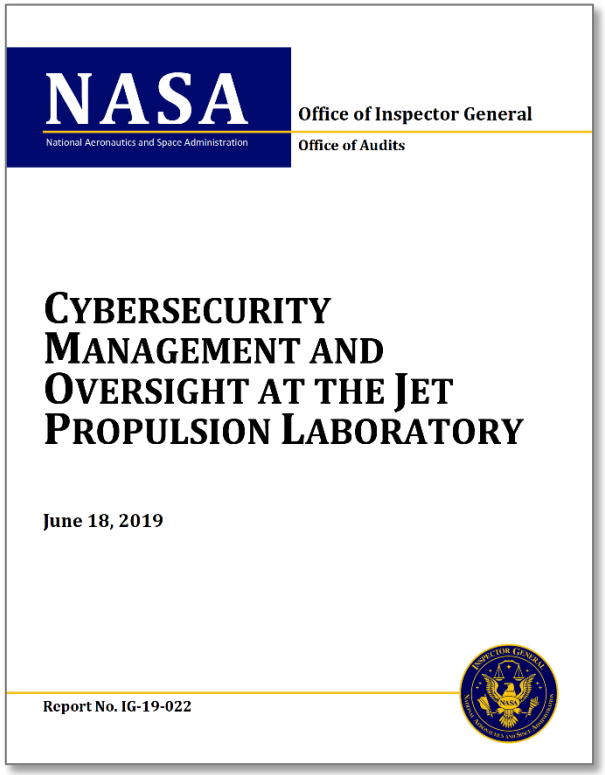
過去の主なセキュリティ事案

発生年	事案名
2008	Windows大規模感染 Conficker
2009	Web媒介型攻撃 Gumblar
2010	重要インフラ攻撃 Stuxnet
2011	三菱重工業への標的型攻撃
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 (DRDoS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
	IoTマルウェア Miraiによる超大規模DDoS攻撃
2017	Apache Struts2
	無差別型ランサムウェア WannaCry

発生年	事案名
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 ①
	メールでの感染連鎖 Emotet
2020	医療機関を狙った標的型ランサムウェア ②
	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
	トヨタ自動車の国内全工場停止 ③
2023	名古屋港システムのランサムウェア感染
	国土交通省 河川監視用カメラへの不正アクセス
2024	KADOKAWAグループへのサイバー攻撃
	DMM Bitcoinのビットコイン不正流出 ④
2025	国内証券口座のっとりによる不正取引 ⑤
	To be continued...

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

19万点超 著作権フリー音楽
日本最大級のBGM・効果音販売サービス「オーディオストック」 - Audiostock

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

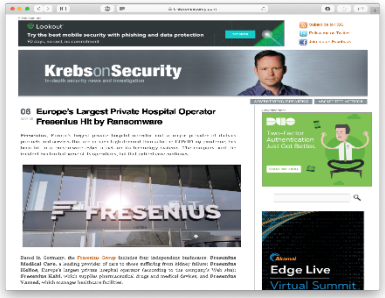
by Les Pounder

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

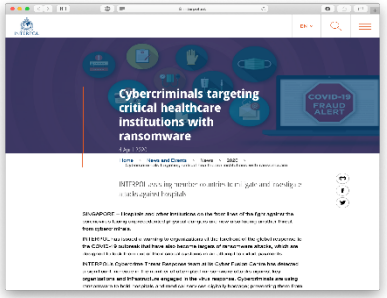
医療機関を狙った標的型ランサムウェア

- 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
- 徳島県つるぎ町立半田病院で**VPN装置でランサムウェア感染**（2021年10月）
  - ✓ 約2ヶ月間電子カルテシステムが停止



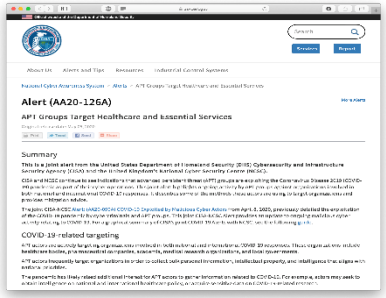
[#1] Krebs on Security

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/

トヨタ自動車の国内全工場停止

- トヨタ自動車部品仕入取引先の**小島プレス工業**のシステム障害
  - ✓ 2022年2月26日21時過ぎ：**社内サーバの1つが停止** ➡ 異常事象を検知
  - ✓ 2月27日朝まで：社内サーバ全停止とネットワークを遮断
  - ✓ 2月28日まで：対応が困難と判断して取引先に連絡
  - ✓ 3月1日：**トヨタ自動車の国内全工場停止**
  - ✓ 3月2日：稼働再開

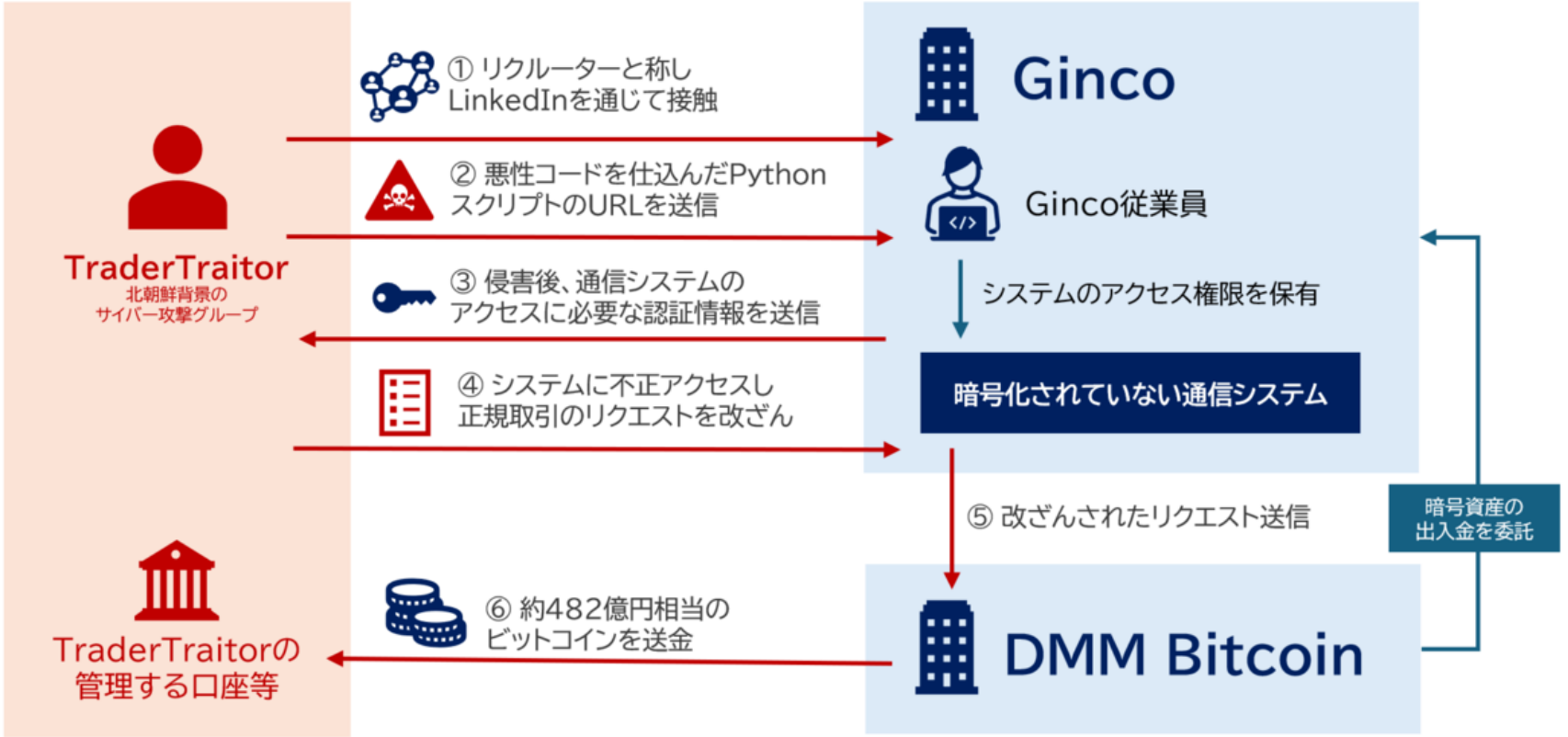
- 原因：**子会社のリモート接続機器（VPN？）**
  - ✓ 小島プレス工業の子会社が独自に利用していた機器
  - ✓ その機器の脆弱性により不正アクセス ➡ 本社へ侵入

➡ **サプライチェーンの一部障害が全体波及**

出典：トヨタタイムズニュース
https://toyotatimes.jp/newscast/008.html

DMM Bitcoinのビットコイン不正流出

- DMM Bitcoinから**482億円相当のビットコインが不正流出**（2024年5月31日公表）
  - ✓ 北朝鮮のサイバー攻撃グループ「TraderTraitor」が関与（警視庁、警察庁関東管区警察局サイバー特別捜査部が公表）
  - ✓ LinkedInを経由した標的型ソーシャルエンジニアリング
  - ✓ DMM Bitcoinは顧客の預かりビットコインを全量保証、同業他社へ移管後**2025年3月事業廃業**

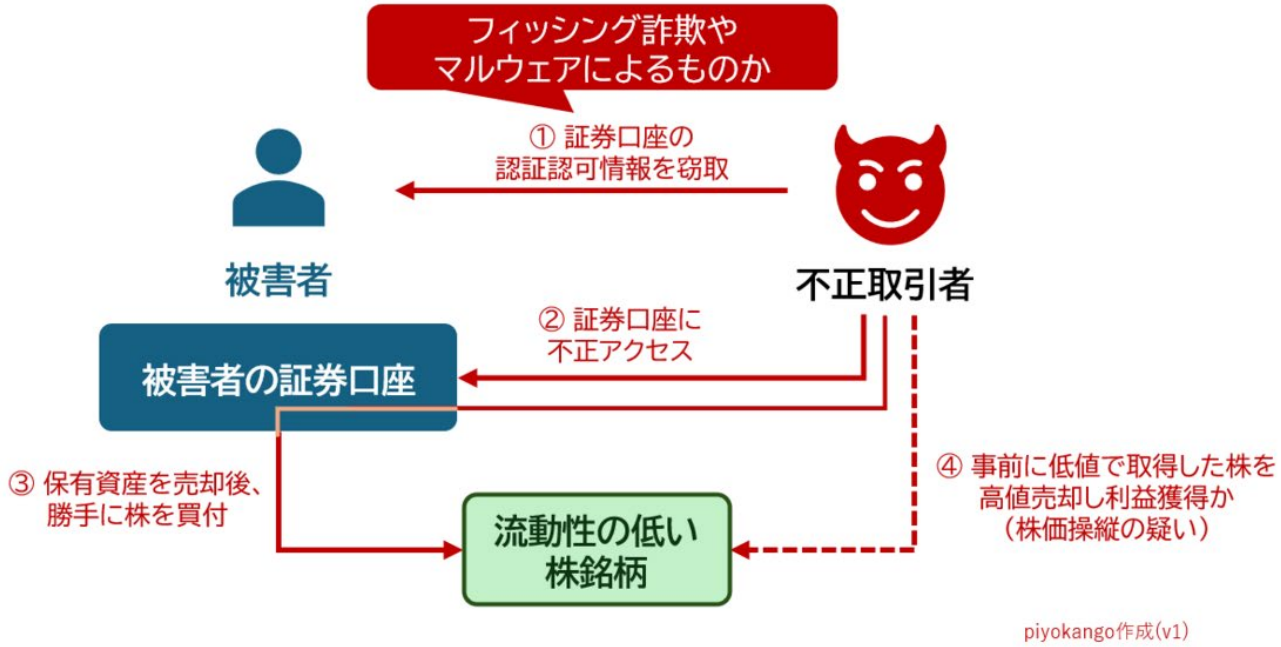


出典：piyolog https://piyolog.hatenadiary.jp/entry/2024/12/25/180139

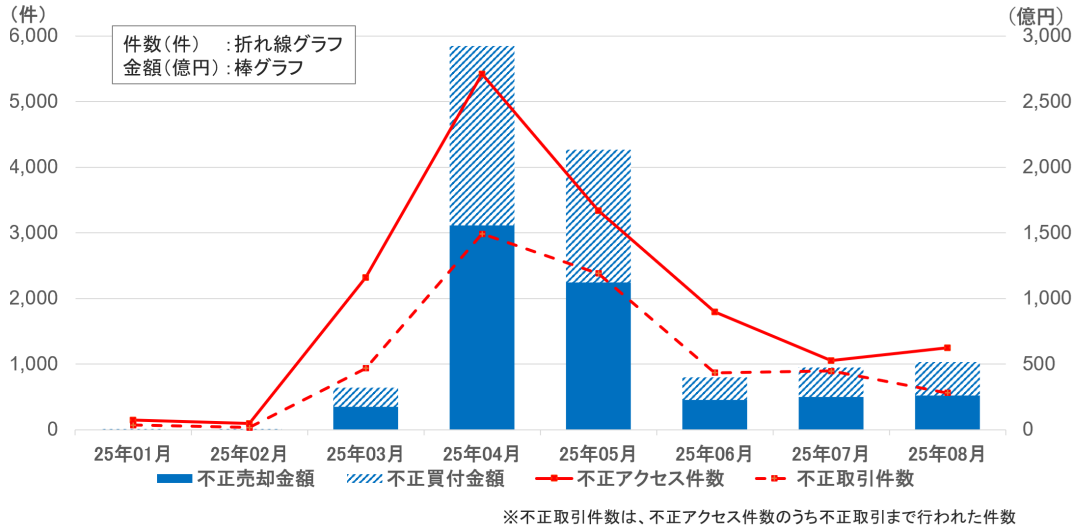
piyokango作成(v1)

国内証券口座のっとりによる不正取引

- 証券会社の**インターネット取引サービスへの不正アクセス・不正取引**が急増
  - ✓ **フィッシング詐欺やマルウェア感染により盗まれた認証・認可情報**を悪用
  - ✓ 楽天証券、SBI証券、野村證券などを含む**18社での被害が報告**されている
  - ✓ 2025年4月をピークに減少傾向にあるが、**依然として被害は継続中**



出典：piyolog https://piyolog.hatenadiary.jp/entry/2025/09/12/160227



※不正取引件数は、不正アクセス件数のうち不正取引まで行われた件数

不正取引が発生した証券会社数（社）							
25年1月	25年2月	25年3月	25年4月	25年5月	25年6月	25年7月	25年8月
2	2	5	10	16	7	6	7

出典：金融庁 https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

近年のセキュリティ事案のまとめ

- **攻撃手法は多様化**
  - ✓ 無差別型攻撃、標的型攻撃、ドライブバイダウンロード
  - ✓ ランサムウェア、サプライチェーン攻撃、etc.
- **攻撃対象も多様化**
  - ✓ 一般ユーザ、企業、重要インフラ、政府官公庁、etc.
- **どの攻撃も根絶に至っていない**
  - ✓ 依然Ongoingな脅威
- **インシデント発生時の初動対応の重要性**
  - ✓ 初動対応次第で組織のReputationにマイナスにもプラスにも

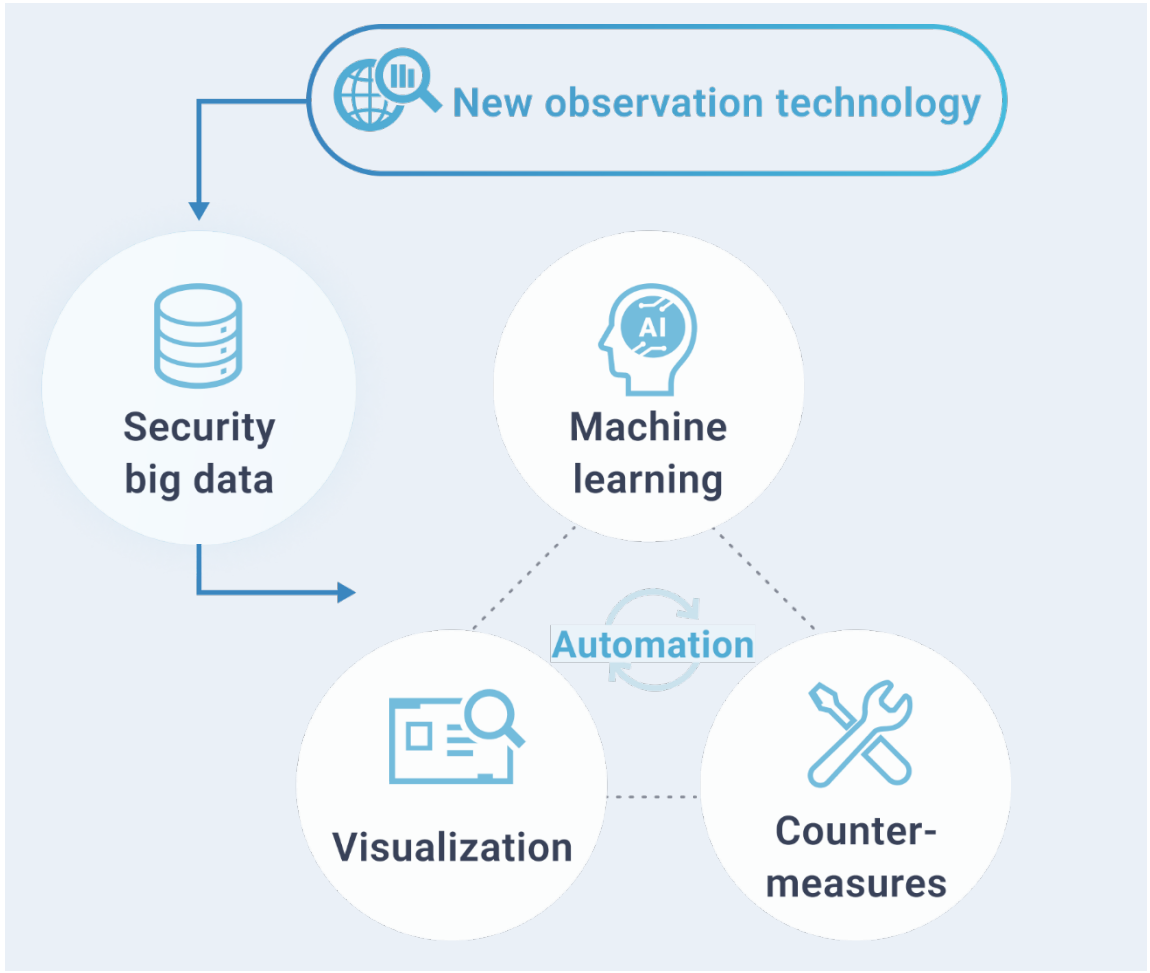
もっと詳しく知りたいあなたは…

piyolog 見ましょう！

https://piyolog.hatenadiary.jp

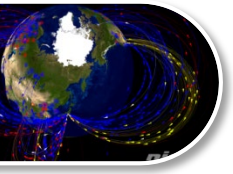
サイバーセキュリティ研究室における研究開発の柱

データ駆動型サイバーセキュリティ技術



エマージングセキュリティ技術

データ駆動型サイバーセキュリティ技術



インシデント分析センタ（ニクター）
NICTER

対サイバー攻撃アラートシステム（ダイダロス）
DAEDALUS

受 Passive

サイバー攻撃統合分析プラットフォーム（ニルヴァーナ・カイ）
NIRVANA

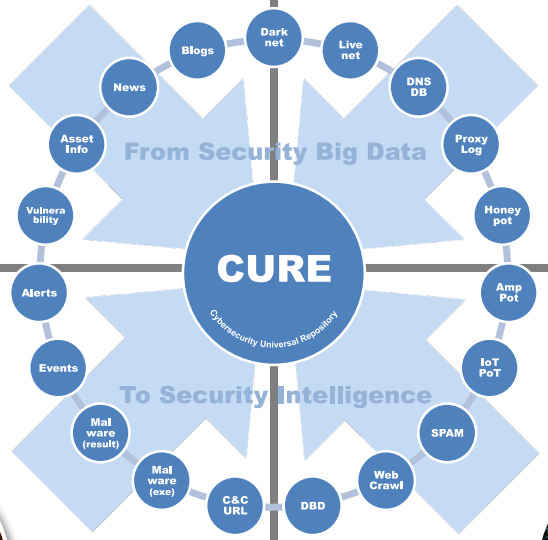
脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）
NIRVANA 改弐

Global (無差別型攻撃対策)

(標的型攻撃対策) Local

全

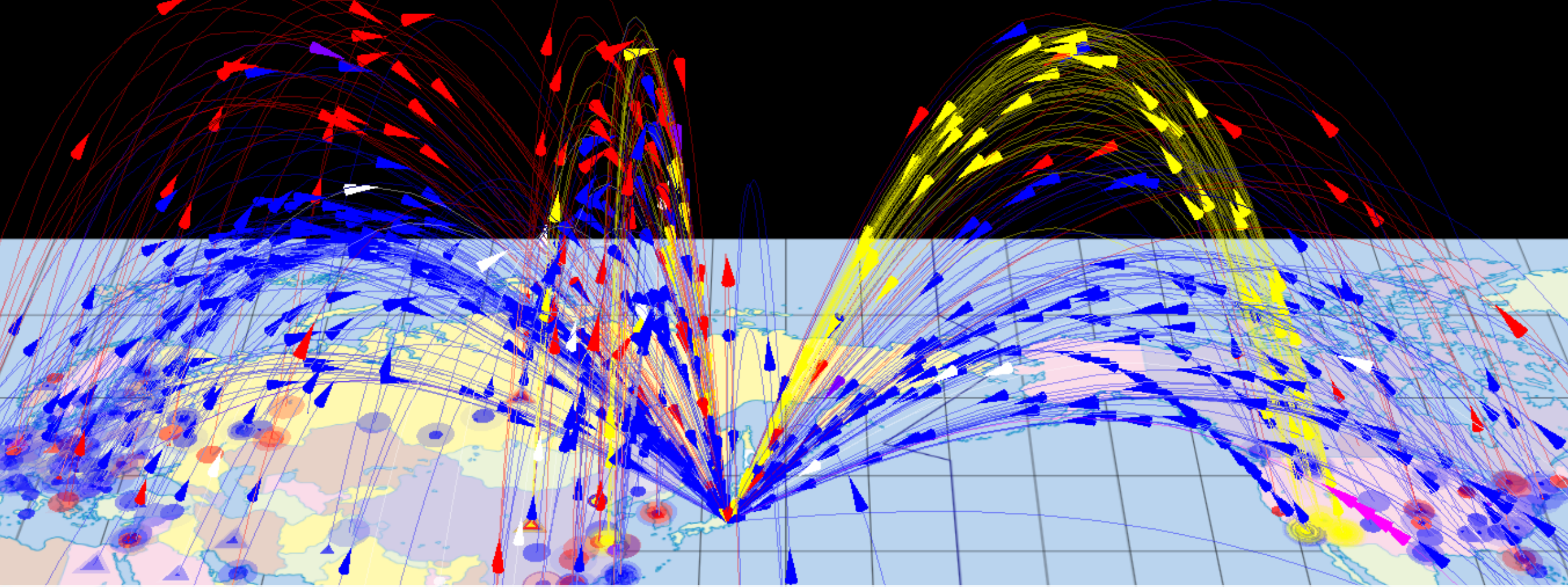
局



サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

能

Active

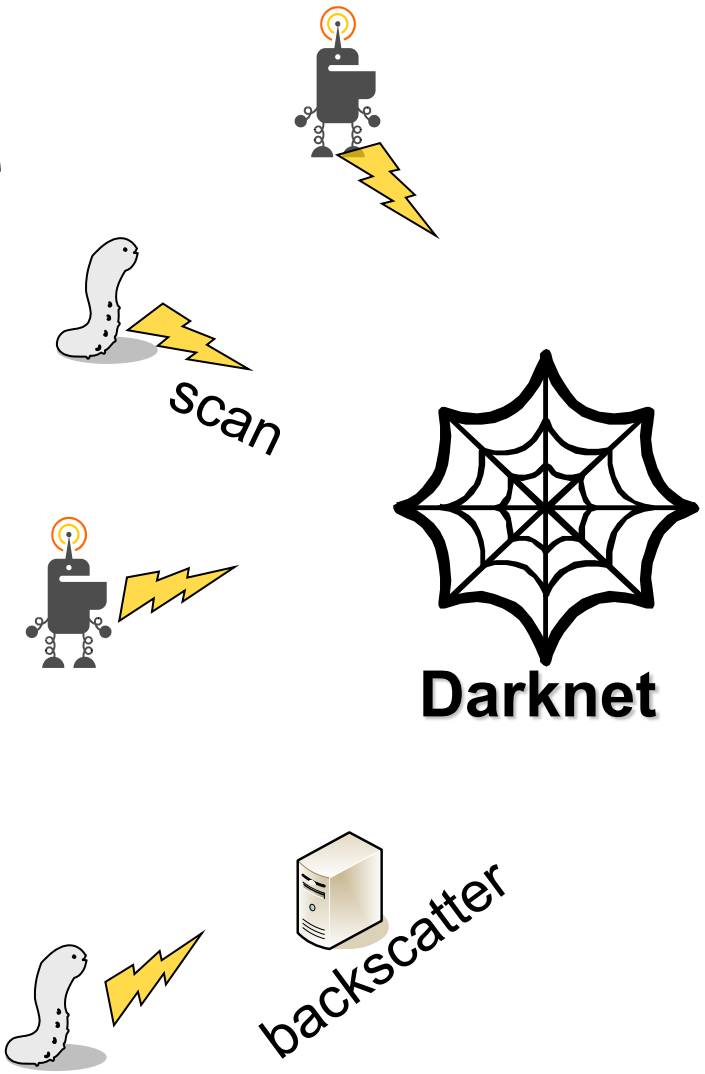


NICTER

- 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攻撃のリフレクタ探索（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



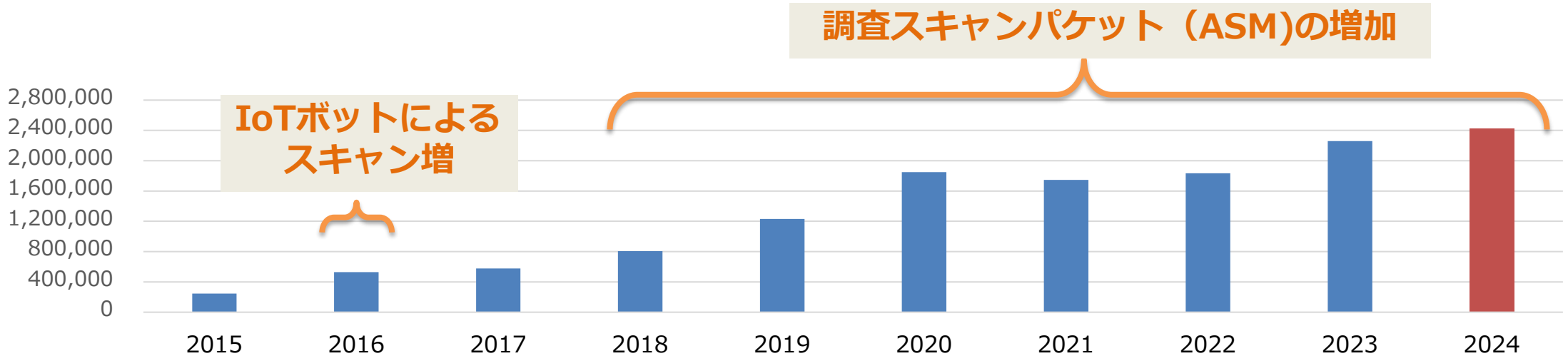
NICTERダークネット観測統計（過去10年）

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
2015	約632億	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
2023	約6,197億	289,686	2,260,132
2024	**約6,862億**	**284,445**	**2,427,977**

1アドレスあたり

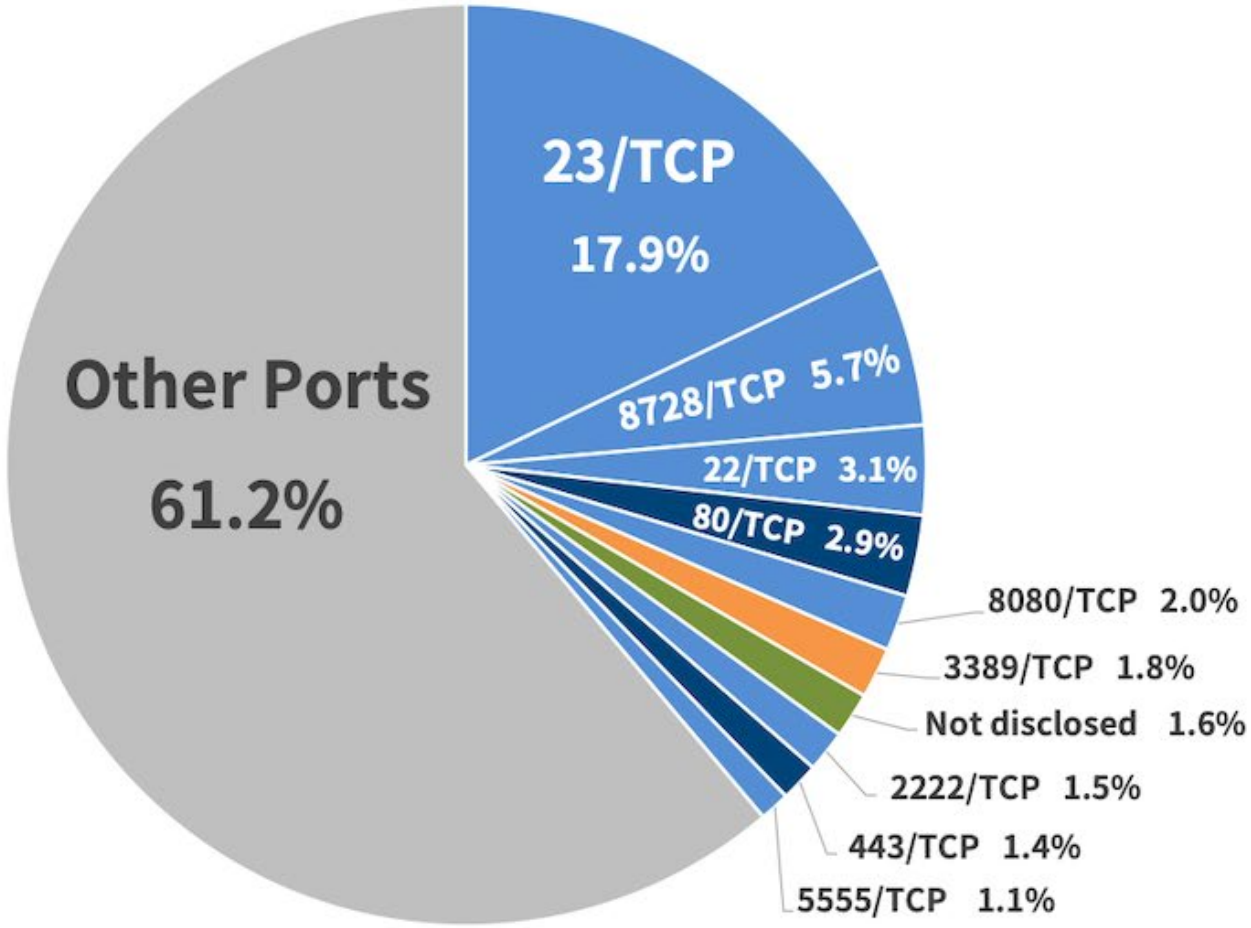
13秒に1回

攻撃関連通信受信



感染機器の分布（2024年）

- NICTER 観測レポート 2024：宛先ポート番号別パケット数分布 -



Port	Target Service
23/TCP	**Telnet** (Router，Web Camera)
8728/TCP	**MikroTik RouterOS API**
22/TCP	**SSH** (Server，Router)
80/TCP	**HTTP** (Web Server)
8080/TCP	**HTTP** (Web Console)
3389/TCP	**Remote Desktop**
Not disclosed	-
2222/TCP	**SSH** (IoT device)
443/TCP	**HTTPS** (Web Server)
5555/TCP	**ADB** (Android)

Percentage of Packets by Destination Port
(Excluding Internet Scanners)

出典：NICTER観測レポート2024
https://csl.nict.go.jp/report/NICTER_report_2024.pdf

無差別型攻撃観測における地理的偏りの要因

- **マルウェア感染機器の偏り**
  - ✓グローバルIPアドレスの保有数・IoT機器の普及率
  - ✓特定の国や地域で普及しているIoT機器の脆弱性が悪用される事例
- **スキャン送信元サーバの偏り**
  - ✓ASM（Attack Surface Management）サービスの提供組織
  - ✓防弾ホスティング業者の所在地
- **攻撃対象サーバの偏り**
  - ✓DDoS攻撃の被害サーバ/サービス（バックスキャッタ）

ある日のマルウェア感染機器数の分布

国別ユニークホスト数 Top10

国名（国コード）	ホスト数	割合
中国（CN）	208,370	39%
インド（IN）	34,316	6%
ブラジル（BR）	31,204	6%
アメリカ（US）	29,744	6%
韓国（KR）	22,310	4%
ロシア連邦（RU）	18,398	3%
イラン（IR）	14,256	3%
ベネズエラ（VE）	13,008	2%
台湾（TW）	12,326	2%
日本（JP）	9,511	2%

2024年1月1日

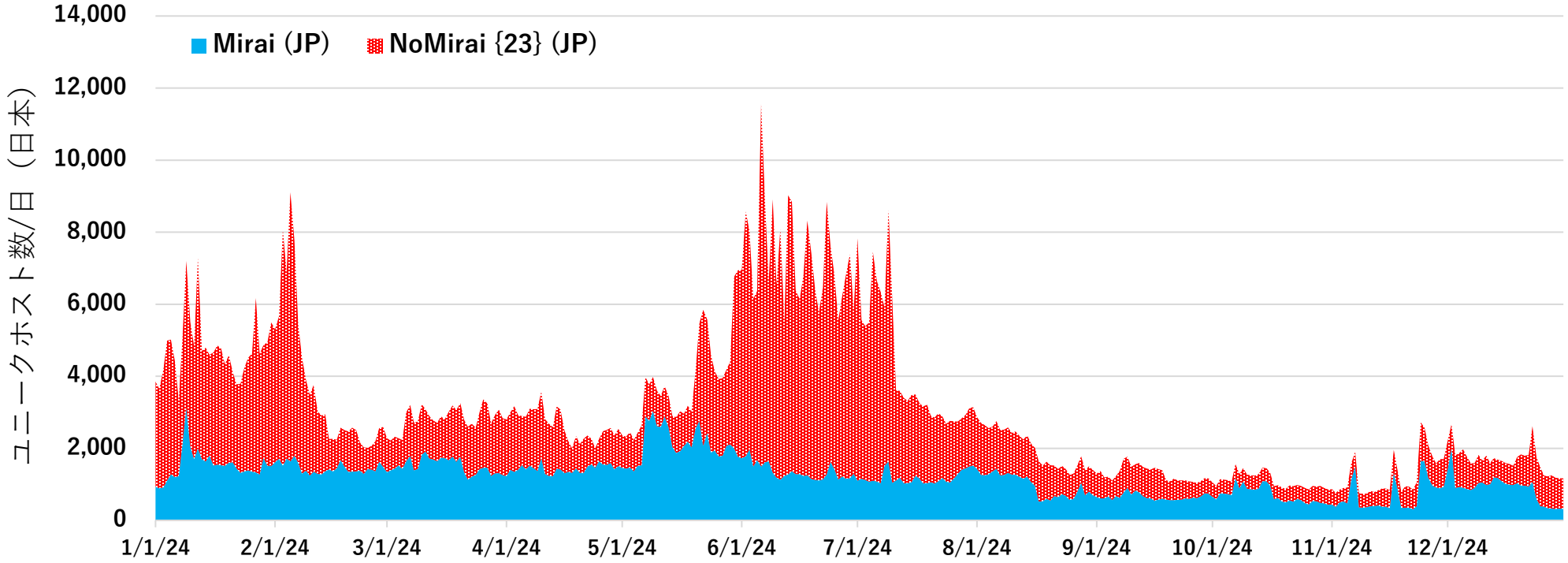
国別ユニークホスト数 Top10

国名（国コード）	ホスト数	割合
中国（CN）	198,148	51%
アメリカ（US）	27,726	7%
インド（IN）	19,821	5%
ロシア連邦（RU）	13,290	3%
エジプト（EG）	11,088	3%
ブラジル（BR）	7,383	2%
インドネシア（ID）	6,923	2%
イラン（IR）	6,712	2%
ベトナム（VN）	5,730	1%
台湾（TW）	5,512	1%

2025年9月28日

日本国内のIoTマルウェア感染規模

- **NICTERで1日あたり最低3,000～10,000台が観測されている**
  - ✓ここ数年はスキャンをばら撒かないマルウェアも攻撃に利用されているため，実際の感染機器はさらに多いと考えられる

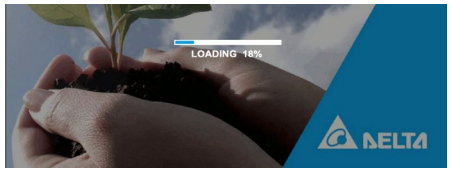


国内の特徴的なIoTマルウェアの感染機器の変遷

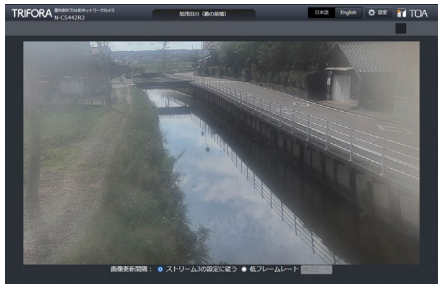
- **2016年：Miraiボット**
  - ✓ IoT機器に感染し大規模なDDoS攻撃を実行

- **NICTで観測した特徴的な感染機器**
  - ✓ 2017～18年：ホームルータ製品
  - ✓ 2019年　　：Android OS搭載製品
  - ✓ 2020年　　：中国製 DVR 製品
  - ✓ 2021年末～：韓国製 DVR 製品
  - ✓ 2023年～　：モバイル回線で繋がる製品
  - ✓ **2025年**　　：**家庭用Wi-Fiルータ**

ソーラーパネル



河川の監視カメラ



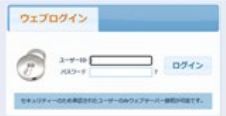
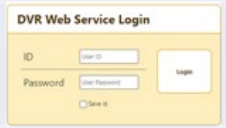
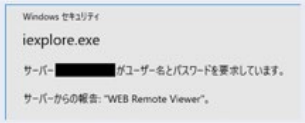
PLC（制御システム）

ボットに感染した産業用LTEルータに
接続されていた機器の管理画面（2024年）

- **感染後に観測された動作**
  - ✓ 感染拡大のためのネットワークスキャン、指令によるDDoS攻撃等

韓国OEM製DVR/NVR製品の脆弱性

- **国内で販売されている5社8機種の感染機器をNICTで解析**
  - ✓ **7機種にメンテナンス用バックドア**（未公開の脆弱性）を確認
  - ✓ そのうち**4社の製品のバックドアが実際に攻撃者によって悪用**されていた
  - ✓ 脆弱性[1,2,3]をベンダに報告し、ファームウェアの修正に協力

製造元	筐体（一例）	管理ログイン画面
FocusH&S		
Rifatron		
Pinetron		
CTRing		
ITX		

脆弱性を発見した韓国製DVR/NVR

[1] JVNDB-2022-002337 ユニモテクノロジー製デジタルビデオレコーダにおける重要な機能に対する認証の欠如の脆弱性
https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002337.html

[2] JVNDB-2022-002768 ユニモテクノロジー製デジタルビデオレコーダにおける複数の脆弱性
https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002768.html

[3] JVNDB-2023-002055 ケービデバイス製デジタルビデオレコーダにおける複数の脆弱性
https://jvndb.jvn.jp/ja/contents/2023/JVNDB-2023-002055.html

国交省河川カメラのマルウェア感染事例

- **国交省河川ネットワークカメラへの不正アクセス**
  - ✓ 2023年1月、国土交通省所管の河川情報提供システムの簡易型河川ネットワークカメラにおいて大量の通信が発生。不正アクセスと思われる痕跡が確認された。
  - ✓ 被害に遭った機種のパスワードは**工場出荷時のまま変更されていなかった**。結果として、338台の運用を停止し、全機器交換するとなった。

※ 日経クロステックより
https://xtech.nikkei.com/atcl/nxt/column/18/00142/01554/

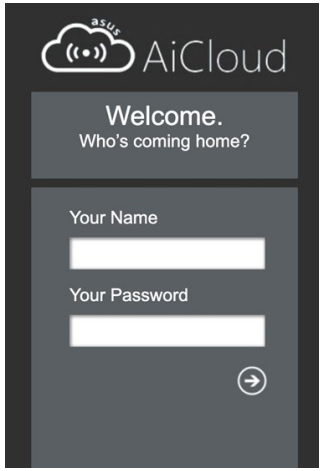
現場に導入された簡易型の河川監視カメラ
（写真：気象工学研究所）

ASUS製Wi-Fiルータ(AiCloud機能)の脆弱性悪用

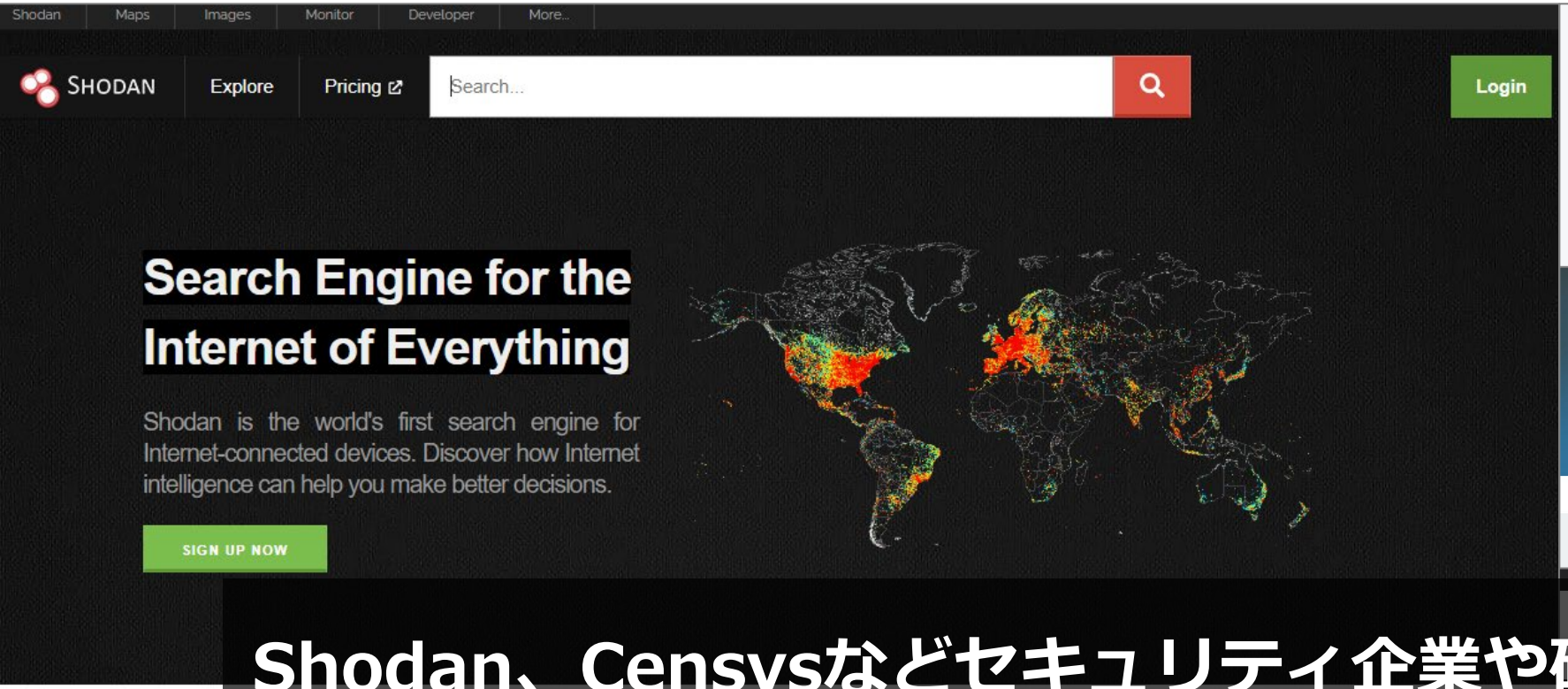
- **AiCloud: ASUSルータに搭載されているクラウドストレージ機能**
  - ✓ LAN or USBに接続されたストレージをパーソナルクラウドとして利用できるサービス
- **証明書インストール機能に認証無しでコマンド実行の脆弱性が存在(CVE-2025-2492)**
  - ✓ NICTER(+実機ハニーポット)により**世界規模で3000台規模の被害**を観測
  - ✓ ASUSより修正ファームウェアとアドバイザリが公開済みのため、速やかな更新を推奨

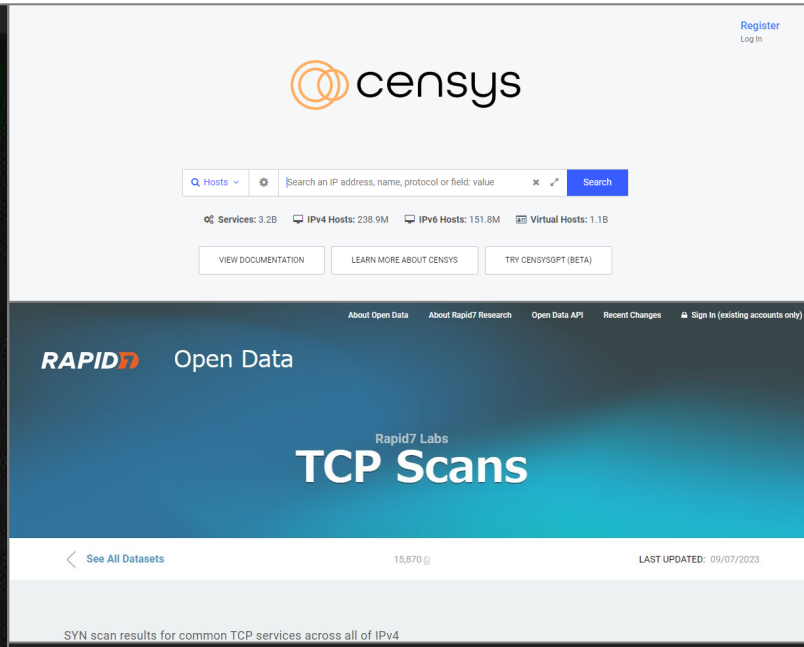
実機ハニーポットによって観測した悪用パターン

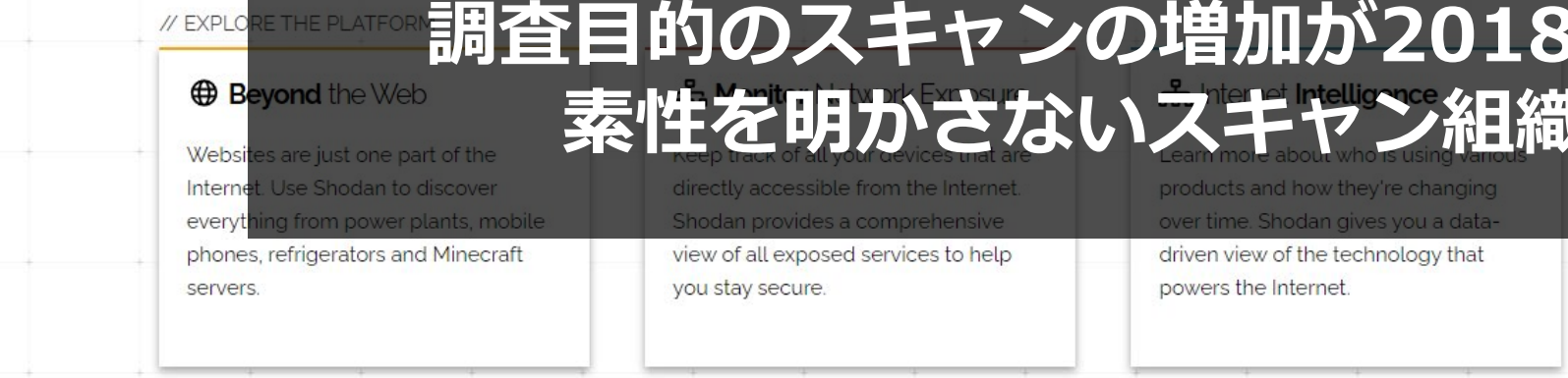
	脆弱なAiCloud バージョン	実際に観測した攻撃活動	悪用された独自メソッド
パターン1	2.0.2.28以下	✓ バックドア（Telnetなど）の有効化 ✓ ファイアーウォールの操作 ✓ Hostファイルの操作 ✓ /etc/passwd の操作 ✓ マルウェアへの感染	•APPLYAPP
パターン2	2.0.2.36以下	✓ マルウェアへの感染	•SETROOTCERTIFICATE •APPLYAPP
パターン3	2.0.2.12以下	✓ マルウェアへの感染	•SETROOTCERTIFICATE



調査目的の海外組織からのスキャン増加 (2018年~)

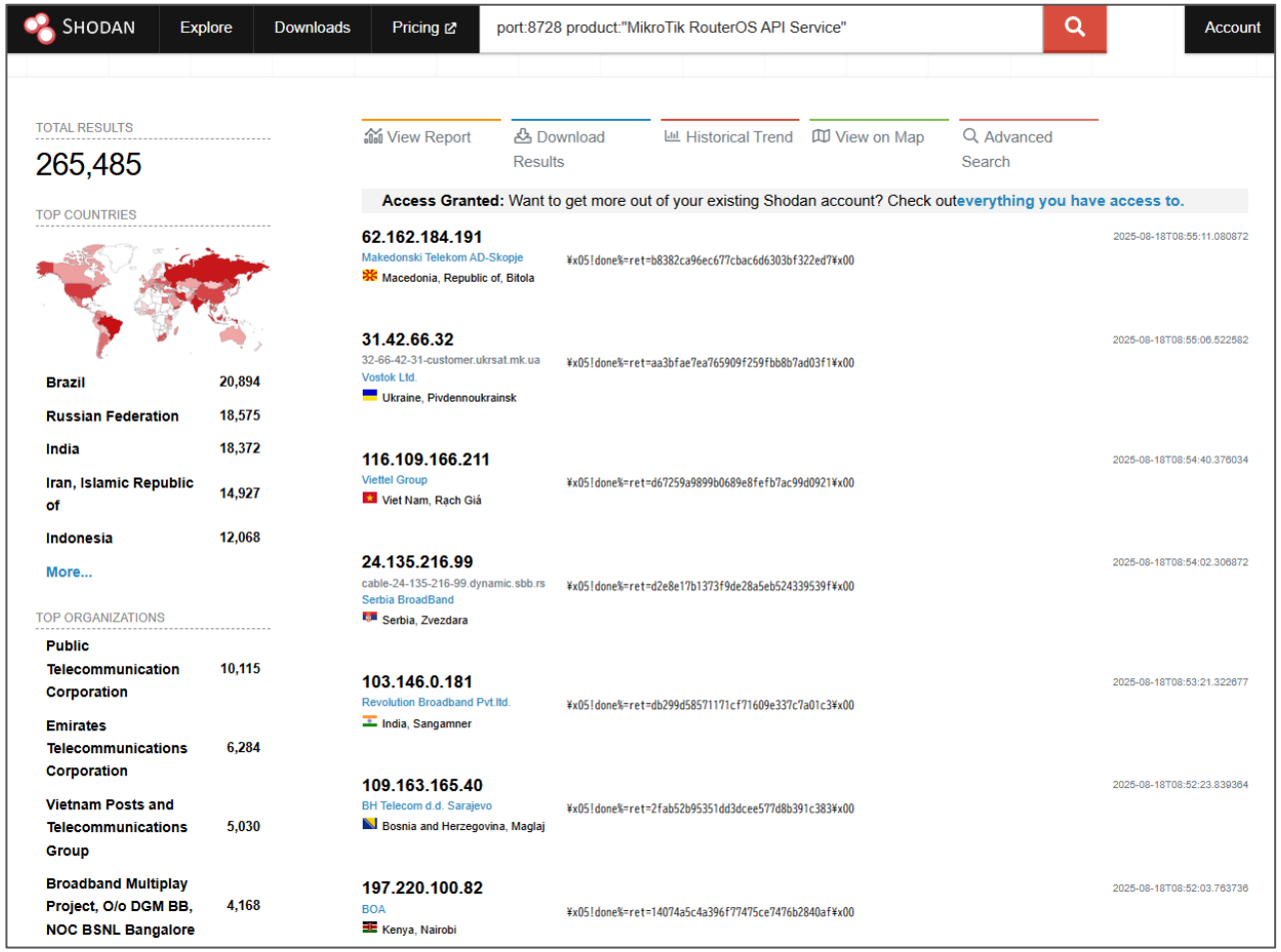




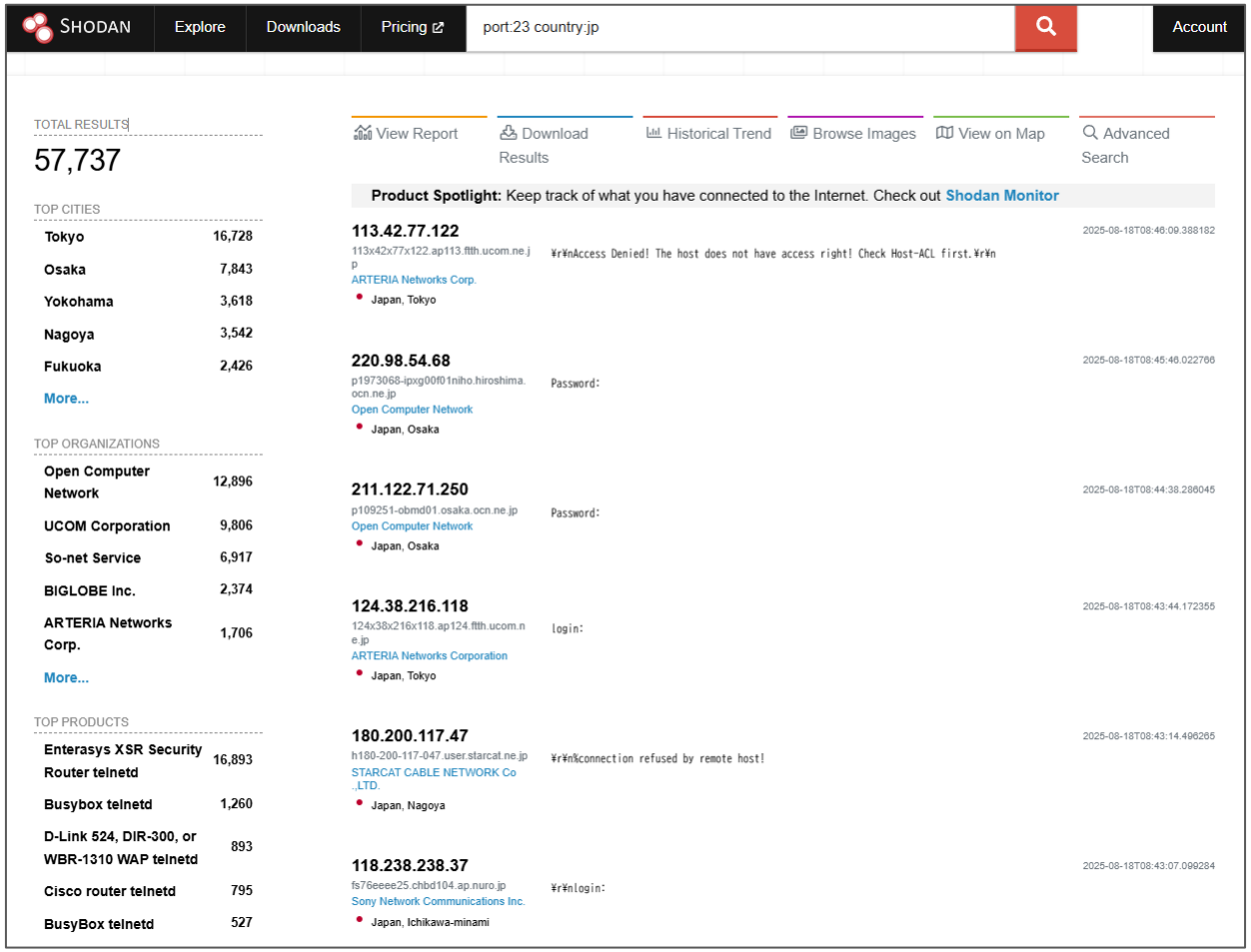


Shodan、Censysなどセキュリティ企業や研究組織による調査目的のスキャンの増加が2018年から特に顕著
素性を明かさないスキャン組織も多数存在

Shodan等を利用したASM(Attack Surface Management)



8728/TCPでMikroTik RouterOS APIが稼働しているホスト



日本国内で23/TCP(Telnet) が稼働しているホスト

素性特定に成功したASM実施組織

- 2024年に特定したASM実施組織：79

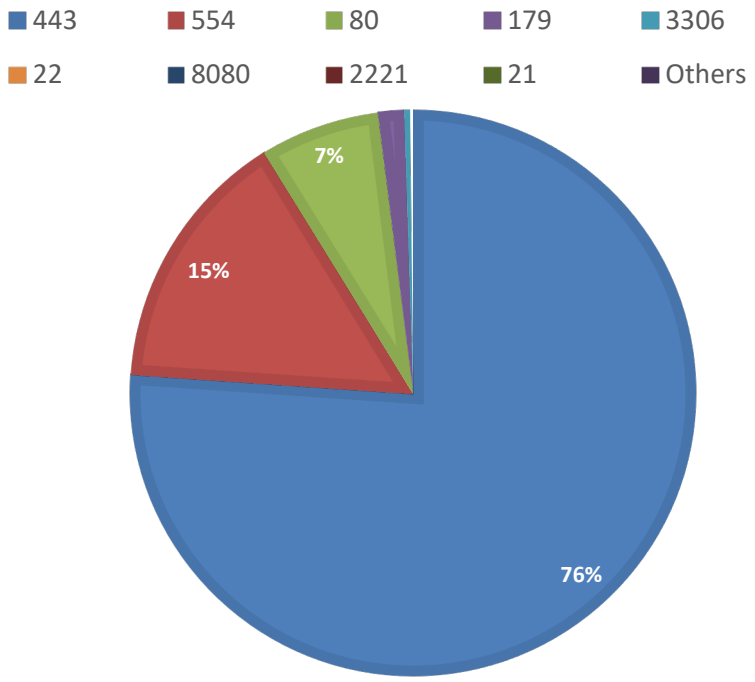
1	Censys	アメリカ
2	Palo Alto Networks (Cortex-Xpanse)	アメリカ
3	Stretchoid	不明
4	The Recyber Project	不明
5	Shadowserver	アメリカ
6	CriminalIP	アメリカ
7	driftnet (internet-measurement.com)	アメリカ
8	Academy for Internet Research	不明
9	Inspici	アメリカ
10	Shodan	
11	internettl	
12	Onyphe	
13	bitsight	
14	一般社団法人ICT-ISAC	
15	GROUP-IB	
16	Binaryedge	アメリカ
17	NETSCOUT (Arbor)	アメリカ
18	bufferover.run	不明
19	Rapid7 (Project Sonar)	アメリカ
20	ScanOpticon	不明
21	Qrator (Qrator.Radar)	チェコ
22	ipip	中国
23	Limes Security (Alpha Strike Labs)	ドイツ
24	Open Port Stats	不明
25	Adscore	UAE
26	UpGuard (CyberResilience)	アメリカ
27	FR Cert	フランス
28	横浜国立大学	日本
29	Intrinsec	フランス
30	スタンフォード大学	アメリカ
31	Leakix	ベルギー
32	トゥヴェンテ大学 (Internet Transparency research project)	オランダ
33	Cybergreen	アメリカ
34	ミュンヘン工科大学 (TUM)	ドイツ
41	マックスプランク研究所	ドイツ
42	internet.survey	不明
43	Crowd Strike (Reposify)	アメリカ
44	ミシガン大学	アメリカ
45	ミラノ工科大学	イタリア
46	Edgewatch	スペイン
47	The Internet Archive	アメリカ
48	ANT lab	アメリカ
49	エスリンゲン大学 (Project Patchwatch)	ドイツ
50	ルール大学ボーフム	ドイツ
51	ESET	スロバキア
52	コロラド大学	アメリカ
53	CAIDA	アメリカ
54	research-scanner.com	不明
55	Research knoq	不明
56	NOKIA (Deepfield)	フィンランド
57	SBA Research	オーストリア
58	ジョージア工科大学	アメリカ
59	Facebook (FacebookBot)	アメリカ
60	THESEUS	オランダ
61	semrush	アメリカ
62	dataforseo	エストニア
		アメリカ
		アメリカ
		シンガポール
		不明
		中国
		ドイツ
69	SI6 Networks	アルゼンチン
70	ドレスデン工科大学	ドイツ
71	FOI Internet Scanning Project	スウェーデン
72	ByteDance (Bytespider)	中国
73	アーヘン工科大学	ドイツ
74	Winnti Scanner	不明
75	WebMeUp (BlexBot)	キプロス
76	Cyble (ODIN)	インド
77	フリーステート大学 (UFS)	南アフリカ
78	ブラウンシュヴァイク工科大学 (IAS Lab)	ドイツ
79	NICT（NOTICE）	日本

特定できた調査スキャナリストを4半期毎にGithubで公開中

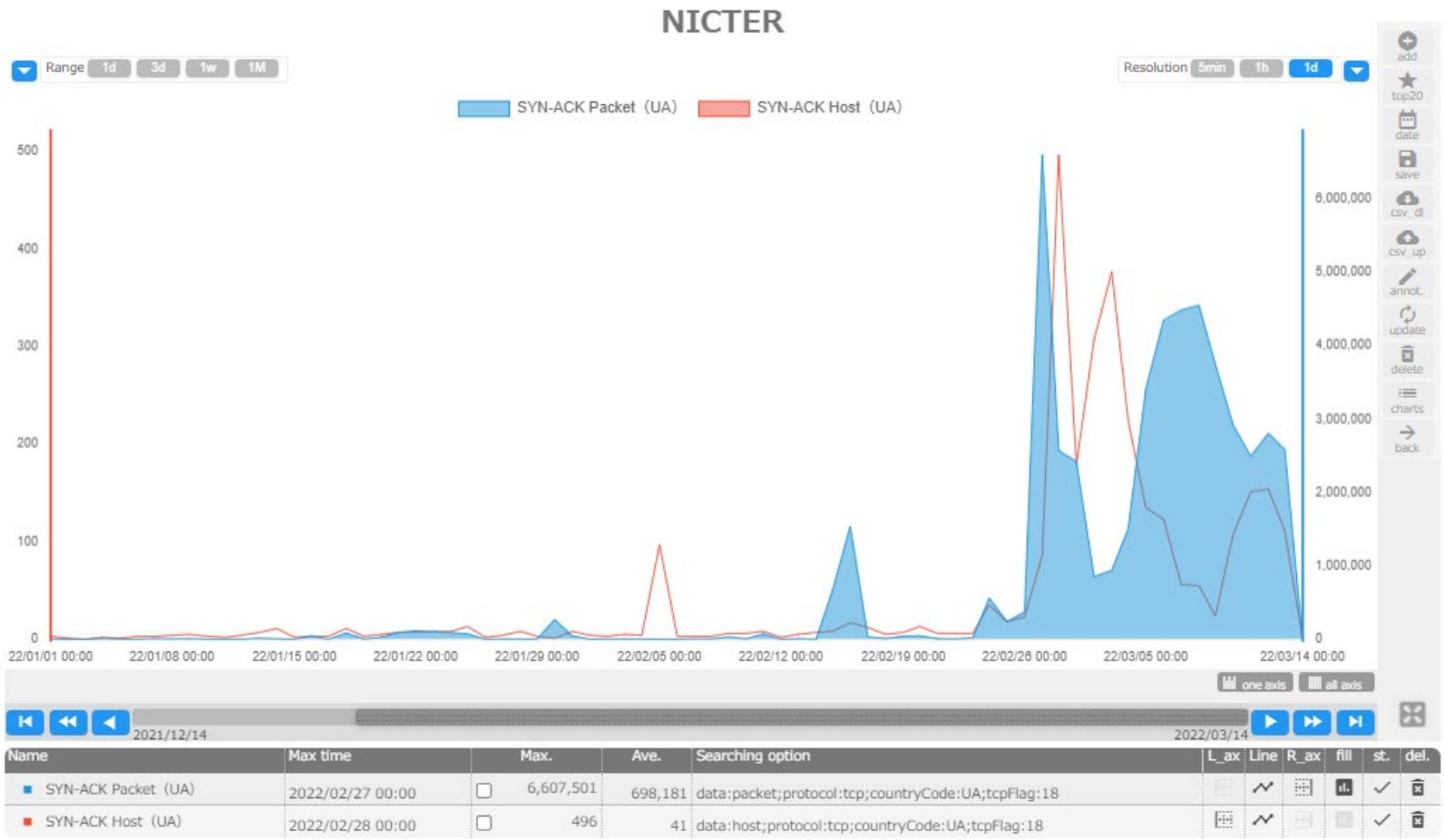
(https://github.com/nict-csl/survey-scanner)

ロシア・ウクライナ情勢関連

- **ウクライナからのSYN-ACKパケット(DDoS攻撃の跳ね返り)の増加を2022/2/24頃から観測**
  - ✓ 最大で単一のアドレスから660万パケット/日を観測
- **SYN-ACK送信元ホストも同様に増加し継続中**



送信元ポートの分布
（DDoS攻撃を受けているサービス）



DDoSの攻撃対象となっていたサーバ（ウクライナ）

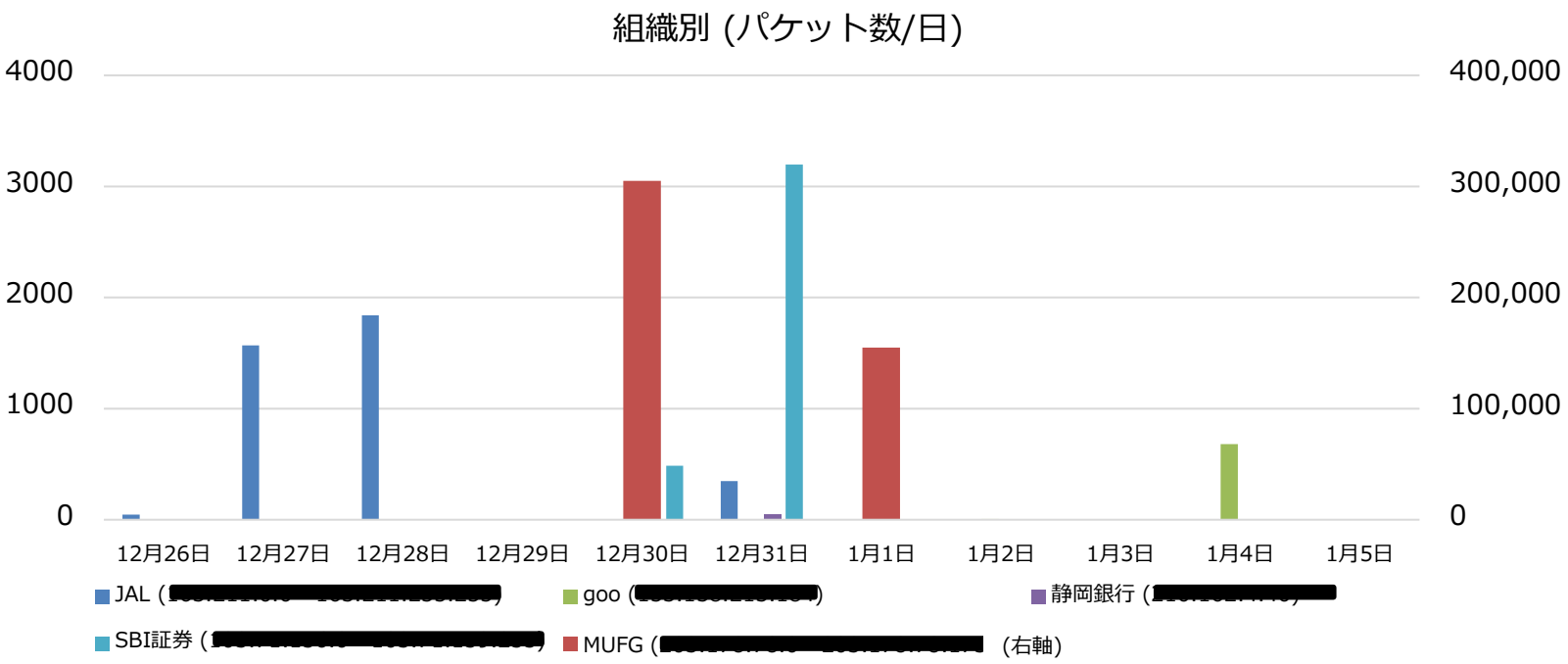
- **イバノフランコフスク州の公式ウェブサイト**
  - ✓ www.new.if.gov.ua（CLDAP）
  - ✓ [redacted]
- **政府ポータルサイト**
  - ✓ old.kmu.gov.ua（ CLDAP ）
  - ✓ [redacted]
- **オシャド銀行**
  - ✓ online.oschadbank.ua（ CLDAP ）
  - ✓ [redacted]
- **外務省**
  - ✓ mfa.gov.ua（ CLDAP ）
  - ✓ [redacted]
- **ウクライナ国立銀行**
  - ✓ bank.gov.ua（NTP）
  - ✓ [redacted]
- **イバノフランコフスク州の公式ウェブサイト**
  - ✓ www.new.if.gov.ua（ 41794 ）
  - ✓ [redacted]
- **年金基金**
  - ✓ pfu.gov.ua（ NTP ）
  - ✓ [redacted]
- **年金基金ポータル**
  - ✓ portal.pfu.gov.ua（ NTP ）
  - ✓ [redacted]
- **大統領サイト**
  - ✓ president.gov.ua（ NTP ）
  - ✓ [redacted]
- **ウクライナ国立銀行**
  - ✓ nbu-net.bank.gov.ua（ NTP ）
  - ✓ [redacted]
- **大統領サイト**
  - ✓ president.gov.ua （ NTP ）
  - ✓ [redacted]
- **外務省**
  - ✓ ns.mfa.gov.ua （ NTP ）
  - ✓ [redacted]
  - ✓ mfa.gov.ua （ NTP ）
  - ✓ [redacted]
- **イバノフランコフスク州の公式ウェブサイト**
  - ✓ www.new.if.gov.ua （ NTP ）
  - ✓ [redacted]
- **ウクライナ国立銀行**
  - ✓ bank.gov.ua （ NTP ）
  - ✓ [redacted]
- **外国諜報機関FISU**
  - ✓ fisu.gov.ua （SNMP）
  - ✓ [redacted]
- **イバノフランコフスク州の公式ウェブサイト**
  - ✓ www.new.if.gov.ua （DNS）
  - ✓ [redacted]
- **外務省**
  - ✓ mfa.gov.ua （ DNS ）
  - ✓ [redacted]
- **電子政府サイト**
  - ✓ itd.rada.gov.ua （ DNS ）
  - ✓ [redacted]
- **政府ポータル**
  - ✓ old.kmu.gov.ua （ DNS ）
  - ✓ [redacted]
- **ウクライナ最高議会**
  - ✓ rada.gov.ua （ DNS ）
  - ✓ [redacted]
- **大統領サイト**
  - ✓ president.gov.ua （ DNS ）
  - ✓ [redacted]
- **ウクライナセキュリティサービスSBU**
  - ✓ sbu.gov.ua （ DNS ）
  - ✓ [redacted]
- **年金基金**
  - ✓ pfu.gov.ua （ CLDAP ）
  - ✓ [redacted]
- **年金基金ポータル**
  - ✓ portal.pfu.gov.ua （DVR DHCPDiscover service、 CLDAP ）
  - ✓ [redacted]
- **大統領サイト**
  - ✓ president.gov.ua（WSD）
  - ✓ [redacted]
- **大統領サイト**
  - ✓ president.gov.ua （ SNMP ）
  - ✓ [redacted]
- **外国諜報機関FISU**
  - ✓ fisu.gov.ua （NTP）
  - ✓ [redacted]
- **防衛省**
  - ✓ mail.mil.gov.ua （ DNS ）
  - ✓ [redacted]
- インフラ？
  - ✓ [redacted]（ WSD ）
  - ✓ [redacted]（ DNS 、 WSD 、 CLDAP ）
- **ウクライナ国立銀行**
  - ✓ nbu-net.bank.gov.ua（ NTP ）
  - ✓ [redacted]
- **イバノフランコフスク州の公式ウェブサイト**
  - ✓ www.new.if.gov.ua（ CLDAP ）
  - ✓ [redacted]
- **国家通信サービス**
  - ✓ ns2.dsszzi.gov.ua（ NTP ）
  - ✓ [redacted]
- **ウクライナ最高議会**
  - ✓ static.rada.gov.ua（ARMS、 CLDAP 、 DNS）
  - ✓ [redacted]
- **国家安全保障防衛評議会NDSC**
  - ✓ ns.nsdc.gov.ua（ NTP ）
  - ✓ [redacted]

DDoSの攻撃対象となっていたサーバ（ロシア）

- **最高裁判所**
  - ✓ vsrf.ru [redacted]
- **軍事連邦サービス**
  - ✓ fsvts.gov.ru [redacted]
- **ロシア連邦国家警備隊**
  - ✓ rosguard.gov.ru [redacted]
- **連邦保安局**
  - ✓ http://www.fsb.ru/ [redacted]（NTP）
- **連邦国防組織**
  - ✓ rfn.ru [redacted]
- **ロシア政府**
  - ✓ lib.gov.ru [redacted]
  - ✓ mx3.gov.ru [redacted]（CLDAP）
  - ✓ mx4.gov.ru [redacted]（CLDAP）
  - ✓ mx2.gov.ru [redacted]（CLDAP）
  - ✓ [redacted]
  - ✓ data.gov.ru [redacted]
  - ✓ .roszdravnadzor.gov.ru [redacted]
- **大統領サイト**
  - ✓ kremlin.ru [redacted]（NTP）
- **ロシア国際問題評議会**
  - ✓ russiancouncil.ru [redacted]（NTP）
- **財務省**
  - ✓ minfin.ru [redacted]（CLDAP）
- **国家システムペイメントPF**
  - ✓ [redacted]（NTP）
- **税金関係**
  - ✓ lkfl.nalog.ru [redacted]（CLDAP）
- **INBANK**
  - ✓ in-bank.ru [redacted]
- **VTB Bank**
  - ✓ vtb.ru [redacted]（NTP、ARMS、 DVR DHCPDiscover service 、WSD）
- **SberBank**
  - ✓ sberbank.ru [redacted]（NTP）
- **Unicreditカード**
  - ✓ unicredit.ru [redacted]
- **Tinkoff Bank JSC**
  - ✓ tcsbank.ru [redacted]
- **ロシア銀行**
  - ✓ cbr.ru [redacted]（NTP）
- **QIWI**
  - ✓ qiwi.com [redacted]
- **Yandex**
  - ✓ yandex.ru [redacted]
- **NPO法人RusBITech（科学生産協会ロシア基礎情報技術）**
  - ✓ rusbitech.ru [redacted]

国内組織宛の昨年末以降のDDoS攻撃

- **2024年の年末から年始にかけて国内の航空会社など多数の組織を対象としたDDoS攻撃が発生**
  - ✓ 日本航空ではシステム障害により航空便に遅れや欠航が発生
  - ✓ 三菱UFJ銀行ではネットバンキングにアクセスできない障害

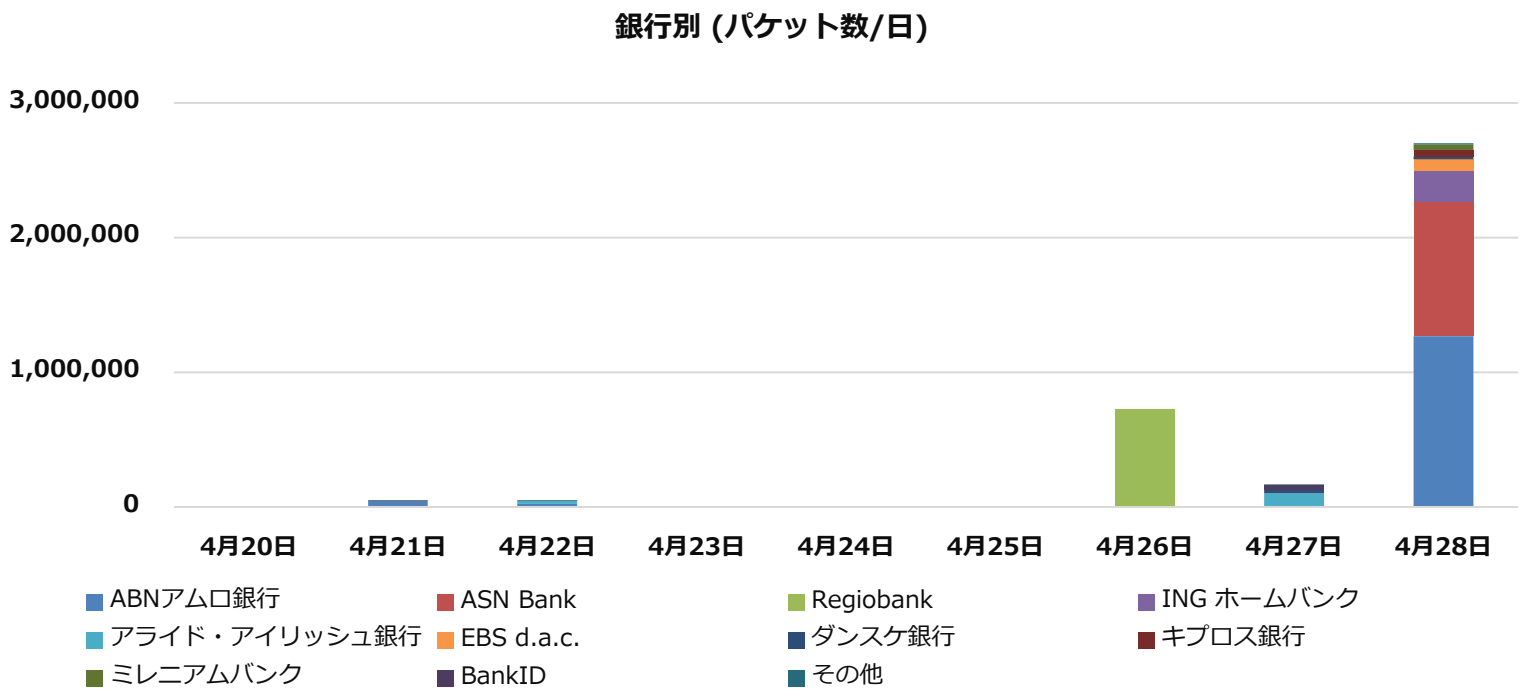


NICTERで観測されたバックスキャッタの統計

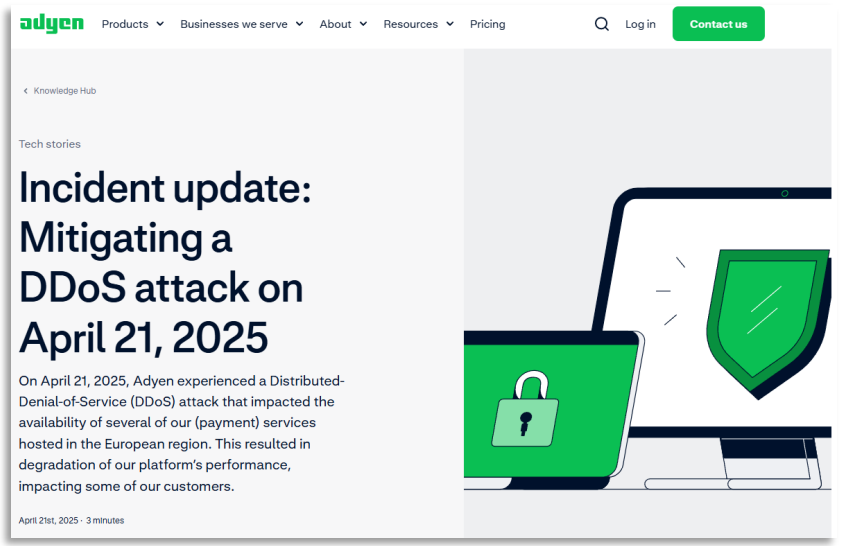
[出典] NHK, https://www3.nhk.or.jp/news/html/20250112/k10014691191000.html

欧州の決済サービスへのDDoS攻撃

- **2025年4月21日から25日にかけての週に**
  欧州を対象に大規模なDDoS攻撃が発生
  - ✓ 大手決済サービスプロバイダの取引処理に影響
  - ✓ NICTERでも同時期にバックスキャッタの増加を観測



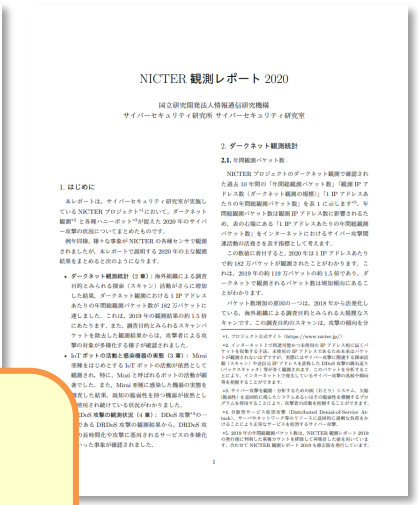
同タイミングでNICTERで観測されたバックスキャッタの統計



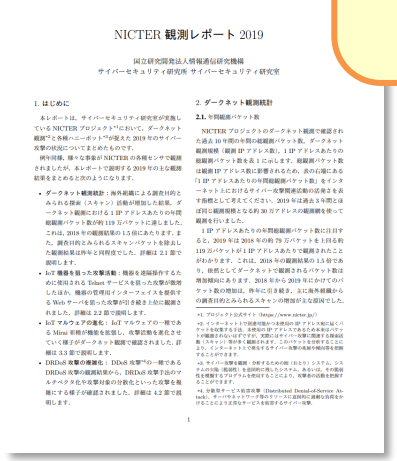
[出典] https://www.adyen.com/knowledge-hub/mitigating-a-ddos-april-2025

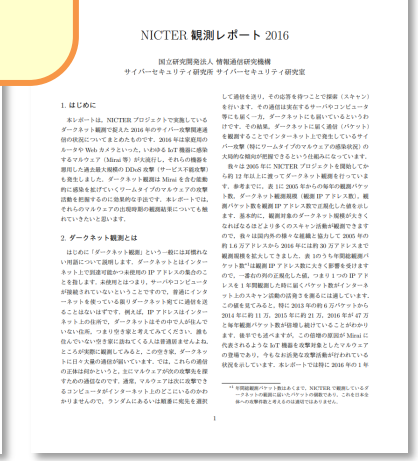
[出典] https://blog.riskrecon.com/ddos-attacks-disrupt-vital-payment-services-across-europe-a-wake-up-call-for-financial-infrastructure

NICTER 観測レポート（毎年2月頃発行）



NICTERWEBで公開中
(https://nicter.jp)





おわりに

- **サイバー攻撃手法・攻撃対象は多様化**
  - ✓一方で、どの攻撃も根絶には至っていないOngoingな脅威
- **サイバー攻撃の実態を観測・可視化し、傾向を把握することは重要**
  - ✓サプライチェーンリスク、物理空間の紛争はサイバー空間にも影響
- **金融分野はサイバー攻撃の格好の対象**
  - ✓サイバー攻撃によるマネタイズの容易さ（フィッシング詐欺等）
  - ✓国民生活への直接的な影響の大きさ