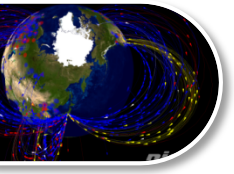
大規模観測から見るサイバー攻撃の動向: 狙われ続けるIoT機器

伊沢 亮一
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

オープンハウス2019 in 小金井
研究者講演

サイバーセキュリティ研究室 研究マップ



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改

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）

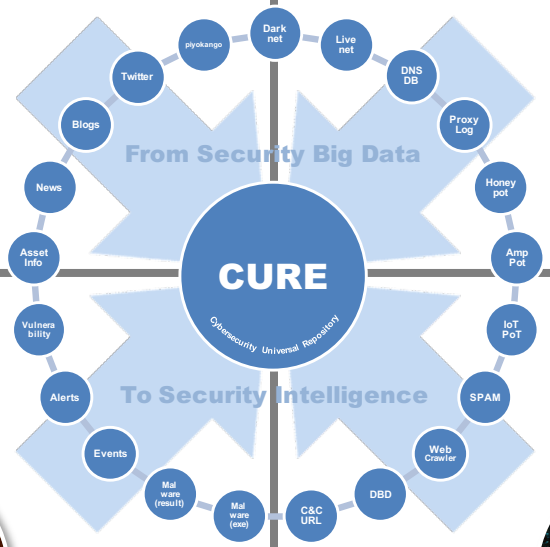
NIRVANA改弐

Global (無差別型攻撃対策)

(標的型攻撃対策) Local

全

局



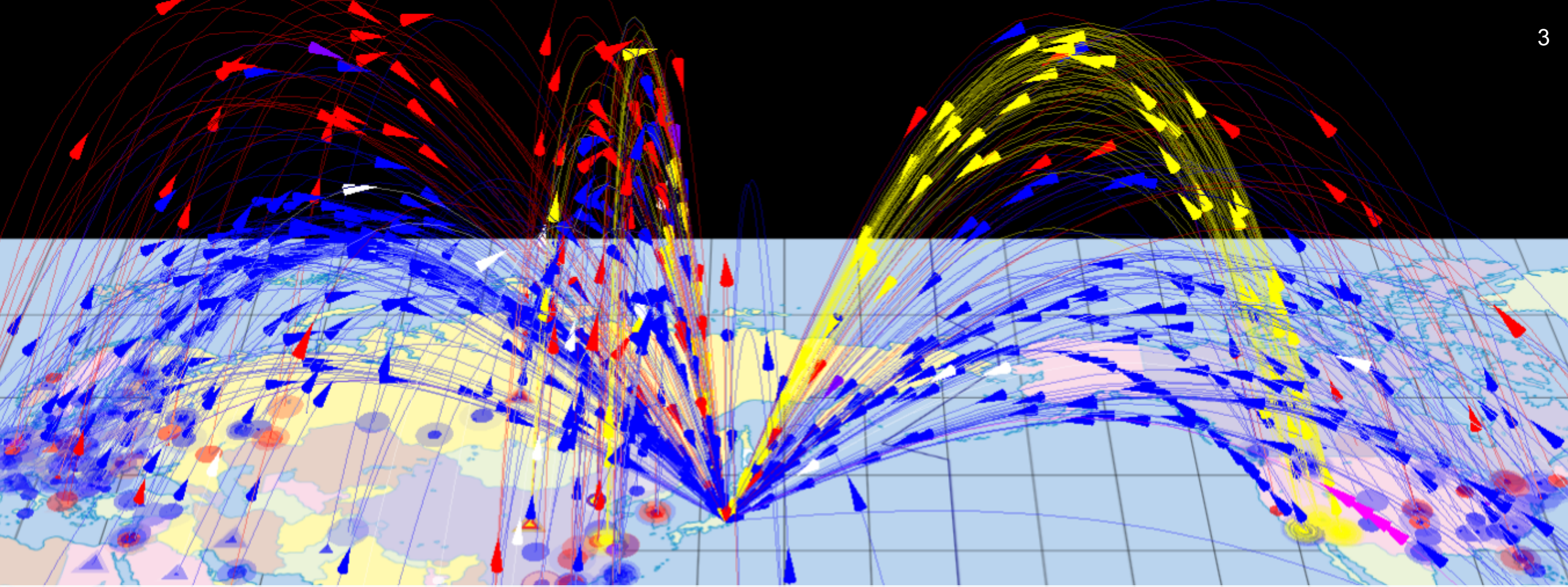
サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

能

Active

NICT National Institute of Information and Communications Technology

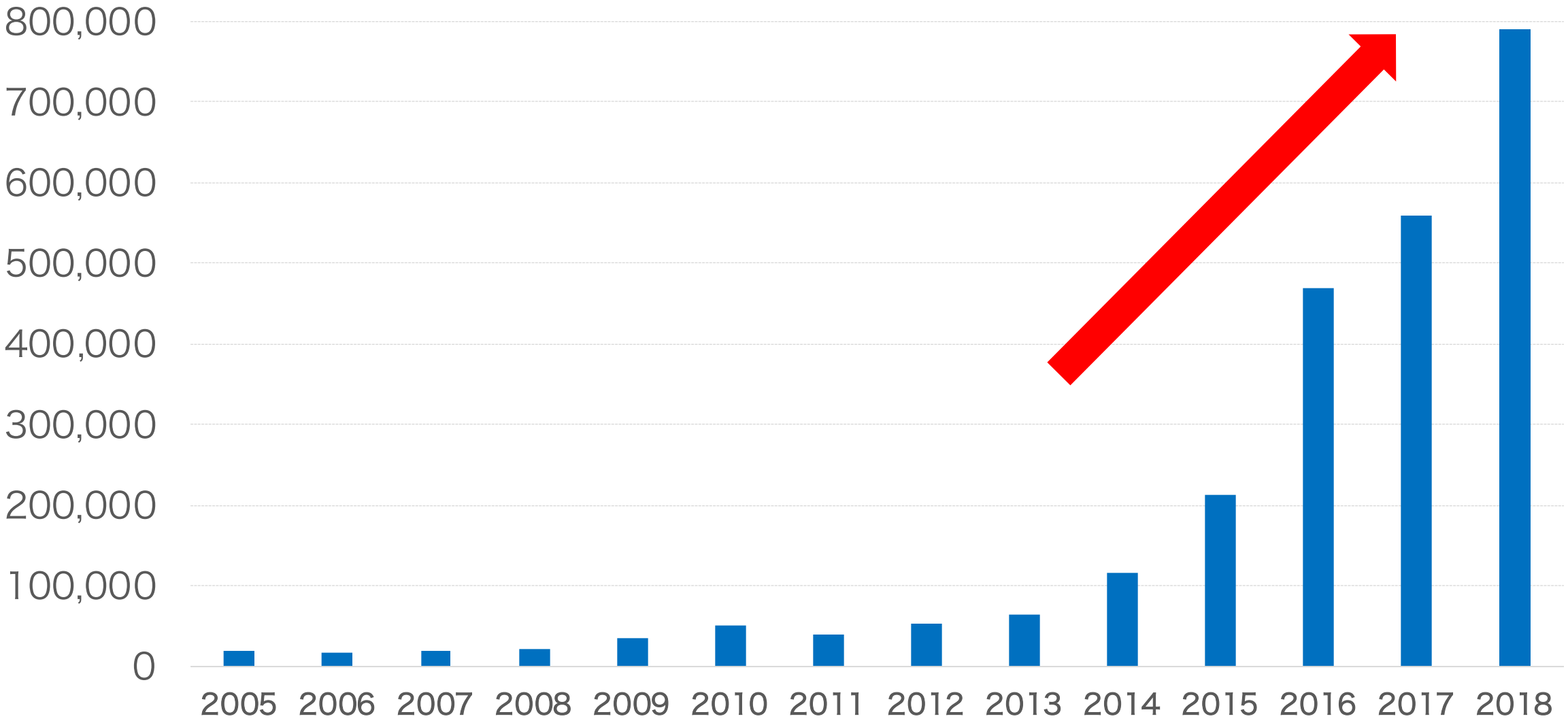
NICTER Network Incident analysis Center for Tactical Emergency Response



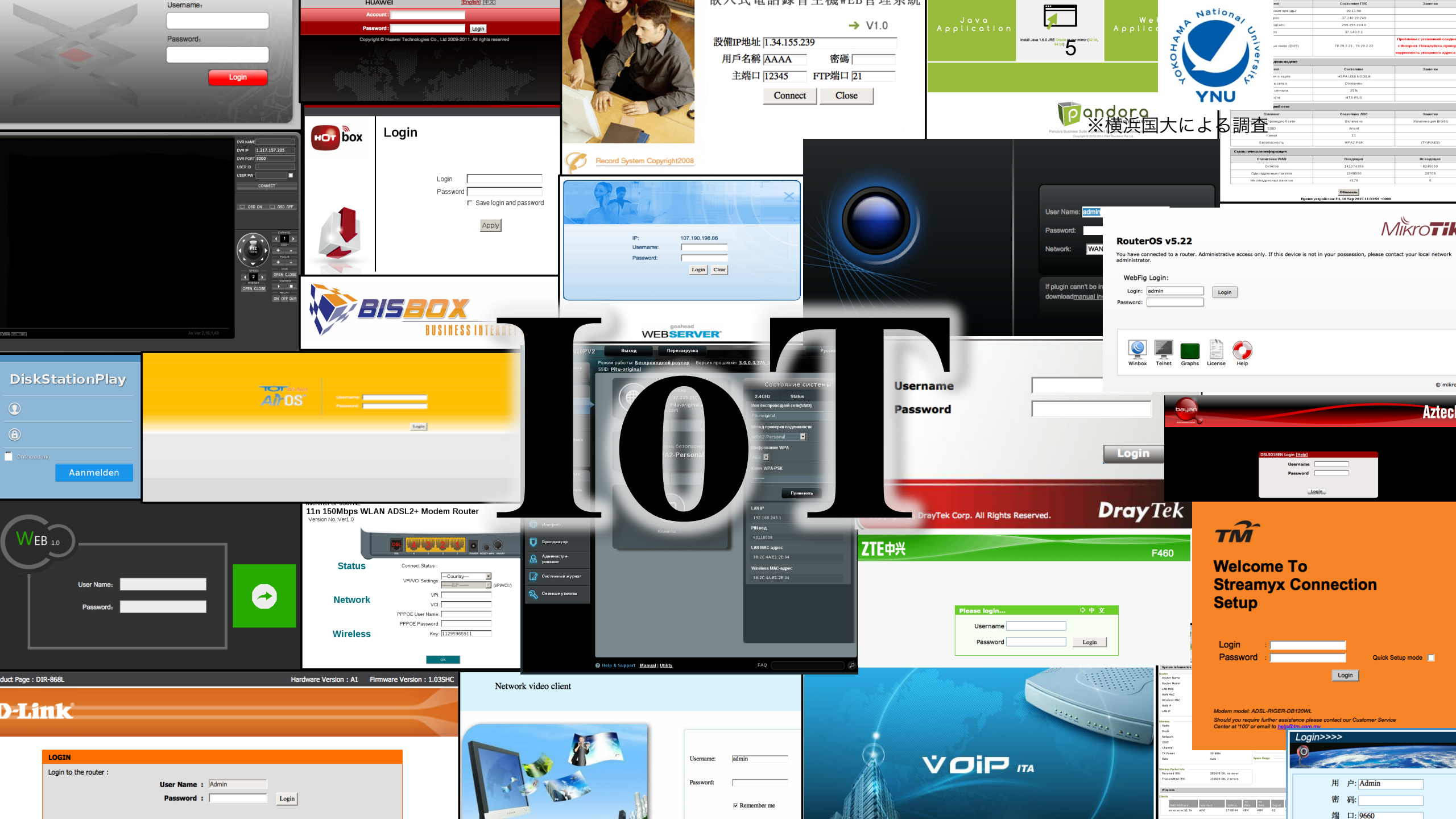
NICTER

- 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

NICTER観測統計（2005-2018）



1 IPアドレスあたりの年間総観測パケット数


※横浜国大による調査
IoT
Username:
Password:
Login
HUAWEI
Account:
Password:
Login
Copyright © Huawei Technologies Co., Ltd 2009-2011. All rights reserved
V1.0
設備IP地址 1.34.155.239
用戶名稱 AAAA
密碼
主端口 12345
FTP端口 21
Connect
Close
Java Application
5
YOKOHAMA National University
YNU
pandora
HOT box
Login
Login
Password
Save login and password
Apply
Record System Copyright2008
DVR NAME
DVR IP 1.217.157.205
DVR PORT 3000
USER ID
USER PW
CONNECT
OSD ON
OSD OFF
IP:
107.190.198.86
Username:
Password:
Login
Clear
User Name: admin
Password:
Network:
MikroTik
RouterOS v5.22
You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.
WebFig Login:
Login: admin
Password:
Login
Winbox
Telnet
Graphs
License
Help
BISBOX
BUSINESS INTERNET
goahead
WEBSERVER
DiskStationPlay
Ontheud mij
Aanmelden
AirOS
Username
Password
Login
DrayTek Corp. All Rights Reserved.
DrayTek
Aztech
DSL5018EN Login [Help]
Username
Password
Login
WEB 1.0
User Name:
Password:
11n 150Mbps WLAN ADSL2+ Modem Router
Version No.:Ver1.0
Status
Network
Wireless
Connect Status :
VPI/VCI Settings :
VPI:
VCI:
PPPOE User Name:
PPPOE Password:
Key: 11295965911
ok
ZTE中兴
F460
Please login...
Username
Password
Login
TM
Welcome To Streamyx Connection Setup
Login :
Password :
Quick Setup mode
Login
Modem model: ADSL-RIGER-DB120WL
Should you require further assistance please contact our Customer Service Center at '100' or email to help@tm.com.my
duct Page : DIR-868L
Hardware Version : A1
Firmware Version : 1.03SHC
D-Link
LOGIN
Login to the router :
User Name : Admin
Password :
Login
Network video client
Username: admin
Password:
Remember me
VoIP ITA
Login>>>>
用 户: Admin
密 码:
端 口: 9660

攻撃元IoT機器

- 横浜国立大学 吉岡研究室による調査結果 -

- **監視カメラ等**
  - **IP カメラ**
  - **デジタルビデオレコーダ**

- **ネットワーク機器**
  - **ルータ・ゲートウェイ**
  - **モデム**
  - **ブリッジ**
  - **無線ルータ**
  - **セキュリティアプライアンス**

- **電話関連機器**
  - **VoIPゲートウェイ**
  - **IP電話**
  - **GSMルータ**
  - **アナログ電話アダプタ**

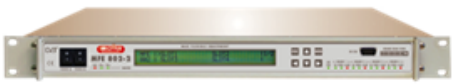
- **インフラ**
  - **駐車管理システム**
  - **LEDディスプレイ制御システム**

- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール
  - センサ監視装置
  - ビル制御システム

- 家庭・個人向け
  - Webカメラ
  - ビデオレコーダ
  - ホームオートメーションGW

- 放送関連機器
  - 映像配信システム
  - デジタル音声レコーダ
  - ビデオエンコーダ/デコーダ
  - セットトップボックス・アンテナ

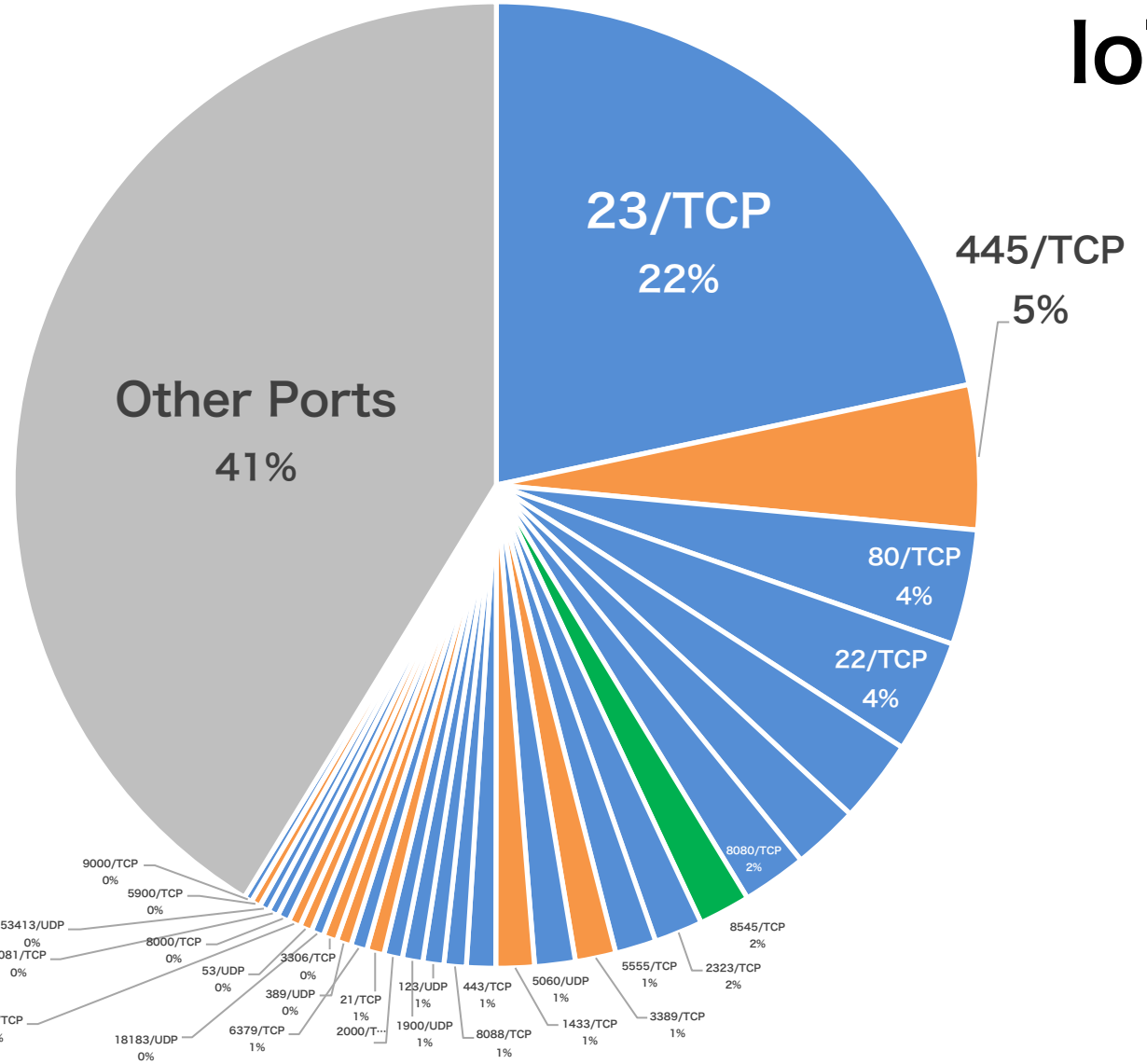
- その他
  - ヒートポンプ
  - 火災報知システム
  - ディスク型記憶装置
  - 指紋スキャナ



※ デバイスはWebおよびTelnetの応答から判断

感染機器の分布（2018年）

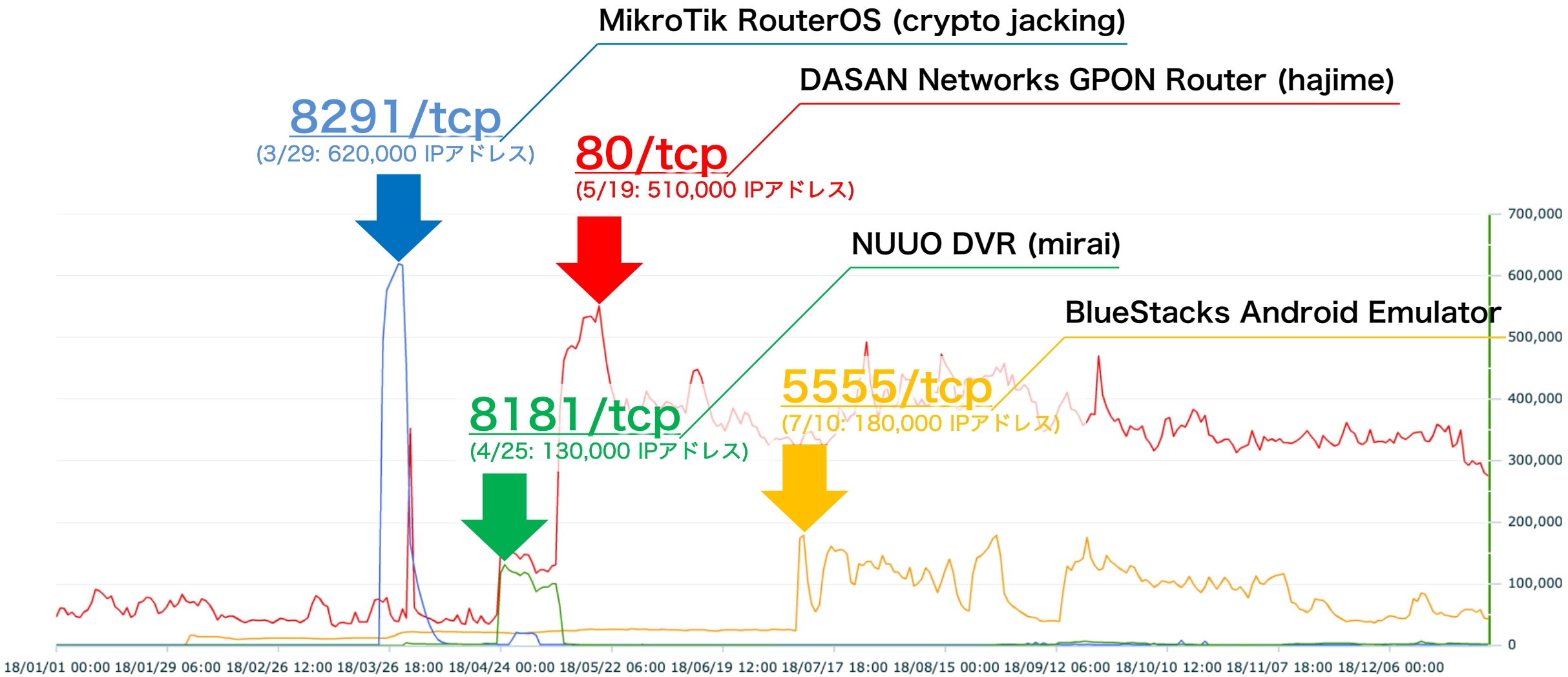
- NICTER 観測レポート 2018：宛先ポート番号別パケット数分布 -



IoT = 47.7%（上位30ポート中）

ポート番号	攻撃対象
23/TCP	IoT機器 （Webカメラ等）
445/TCP	Windows（サーバサービス）
80/TCP	Webサーバ（HTTP）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
52869/TCP	IoT機器（ホームルータ等）
81/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
8545/TCP	イーサリアム（仮想通貨）
2323/TCP	IoT機器（Webカメラ等）
5555/TCP	Android機器 （セットトップボックス等）

2018年の主な大規模感染事例



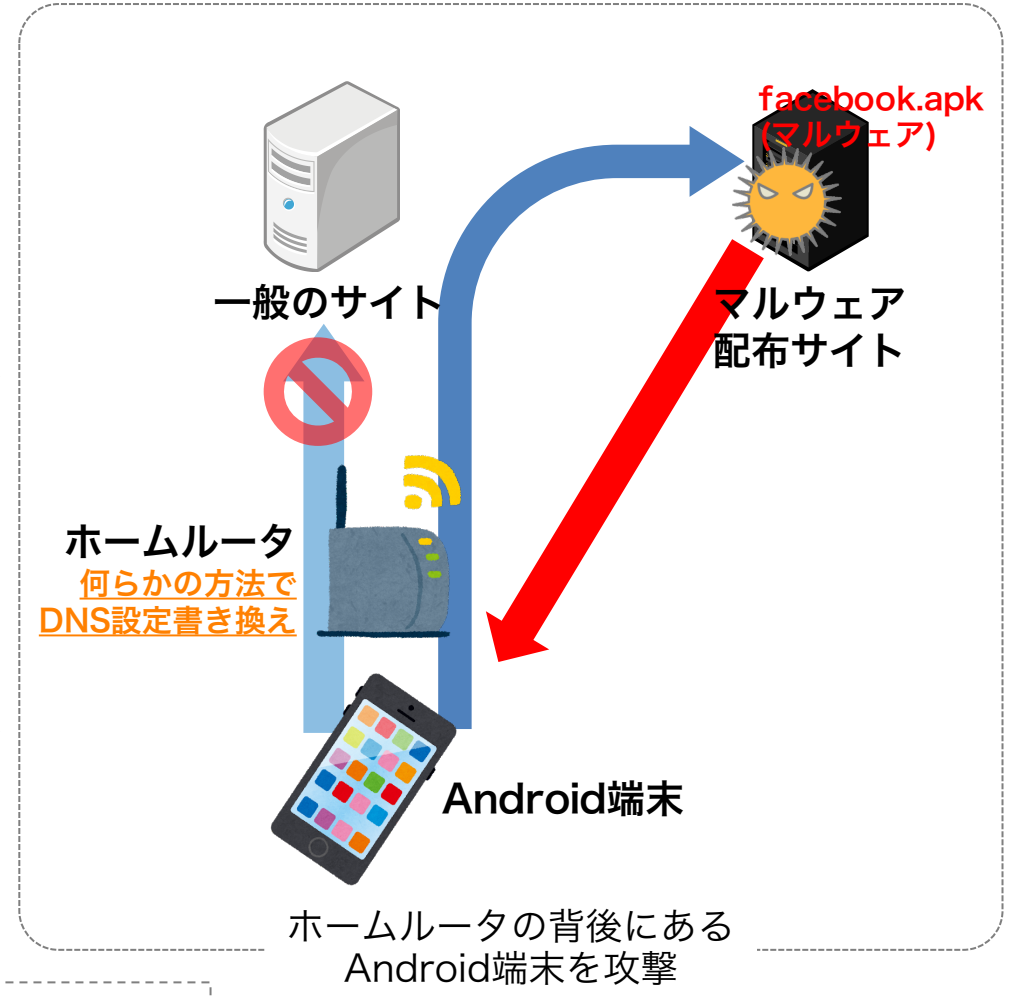
ユニークホスト数/日（2018年1月～12月）

事例: 23/TCPを狙う機器数（日本国内）

NICTER
Network Incident analysis Center for Tactical Emergency Response

高度化するIoT機器への攻撃

- **2016年以前**
  - デフォルトID/パスワードでログインし感染
- **2017年**
  - デフォルトID/パスワードでログインし感染
  - IoT機器の**脆弱性を攻撃**して感染
- **2018年**
  - デフォルトID/パスワードでログインし感染
  - IoT機器の脆弱性を攻撃して感染
  - IoT機器の**背後にある機器を攻撃**

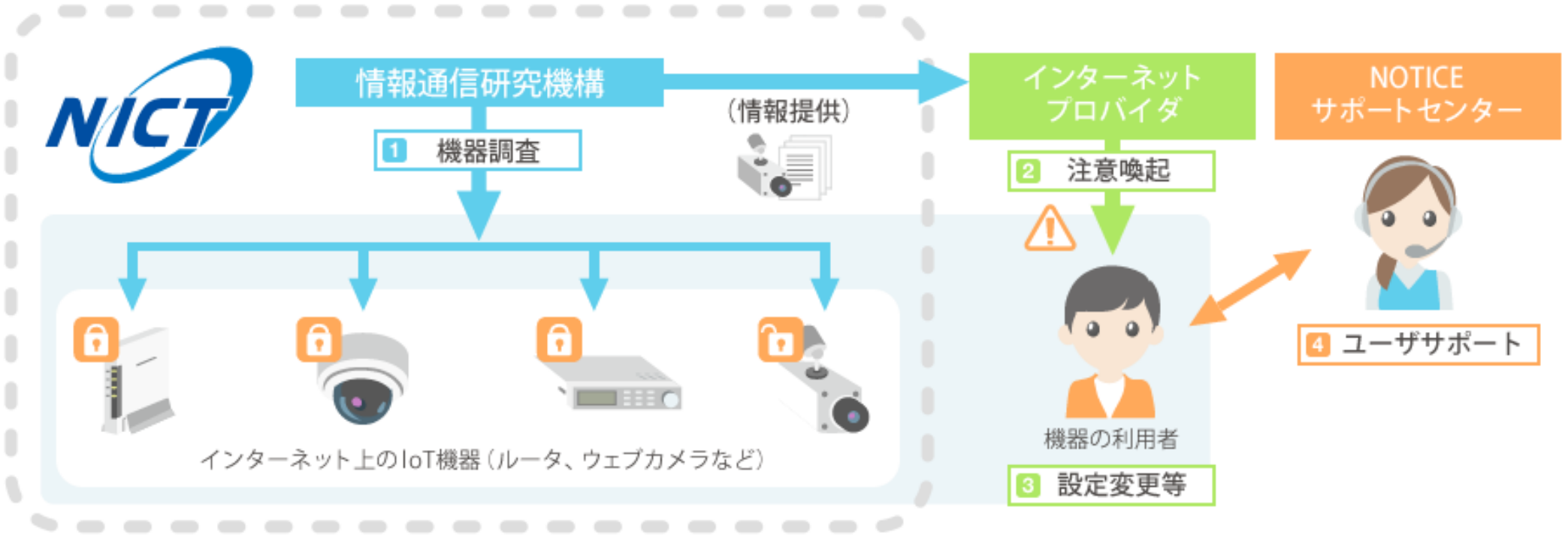


ホームルータの背後にある
Android端末を攻撃

NICTER Blog
"Wi-Fi ルータの DNS 情報の書換え後に発生する事象について,"
https://blog.nicter.jp/2018/03/router-dns-hack/ (Posted on 2018-03-26)

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



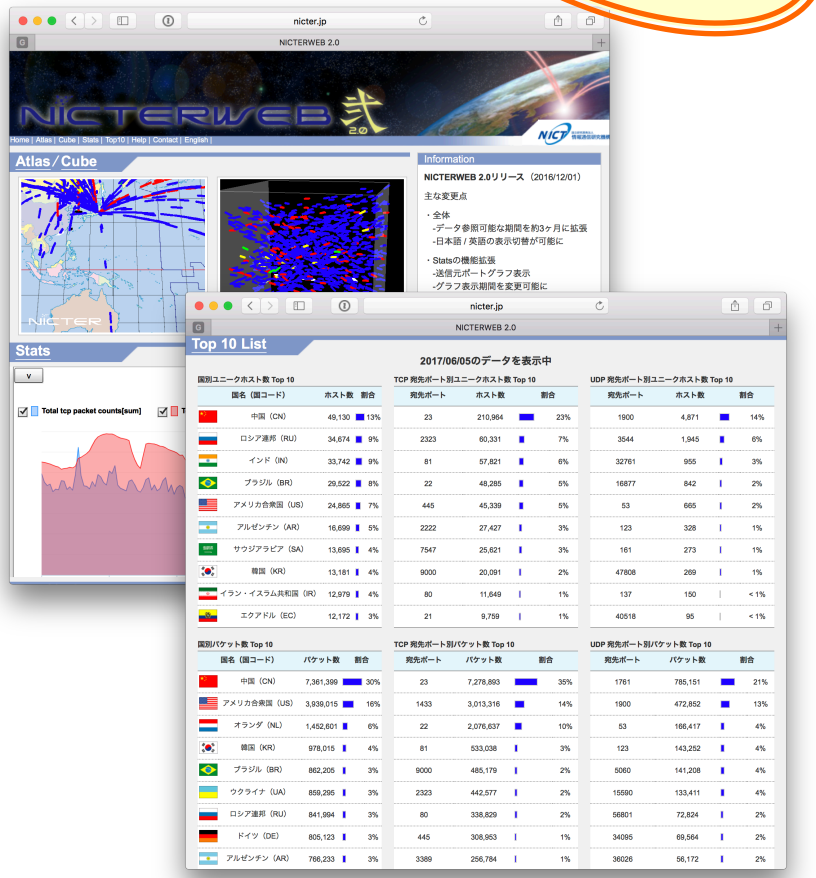
https://notice.go.jp/

NICTER観測情報の利活用

nicter.jp

● セキュリティ関連組織への観測情報提供

- ✓ **SIGMON**（定点観測友の会）
  - JPCERT/CC、IPA、@Police等との観測結果共有（2004年～）
- ✓ **ICT-ISAC Japan**（DoS攻撃即応-WG）
  - DoS攻撃関連情報共有（2011年～）
- ✓ **オリパラ体制検討会**（NISC、オリパラ組織委員会、関連組織、他）
  - DoS攻撃関連情報共有（2015年～）

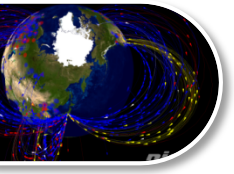


NICTERWEB

● 観測情報一般公開

- ✓ NICTERWEB (http://www.nicter.jp/)
- ✓ NICTER Blog (http://blog.nicter.jp)
- ✓ NICTER 観測レポート (http://www.nict.go.jp/cyber/report.html)

サイバーセキュリティ研究室 研究マップ



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改

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）

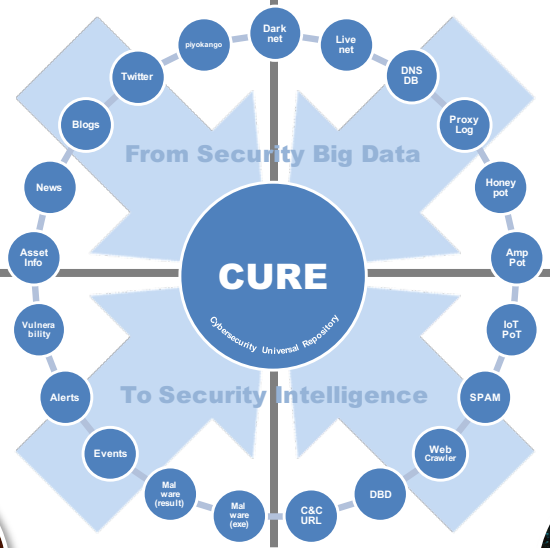
NIRVANA改弐

Global (無差別型攻撃対策)

(標的型攻撃対策) Local

全

局



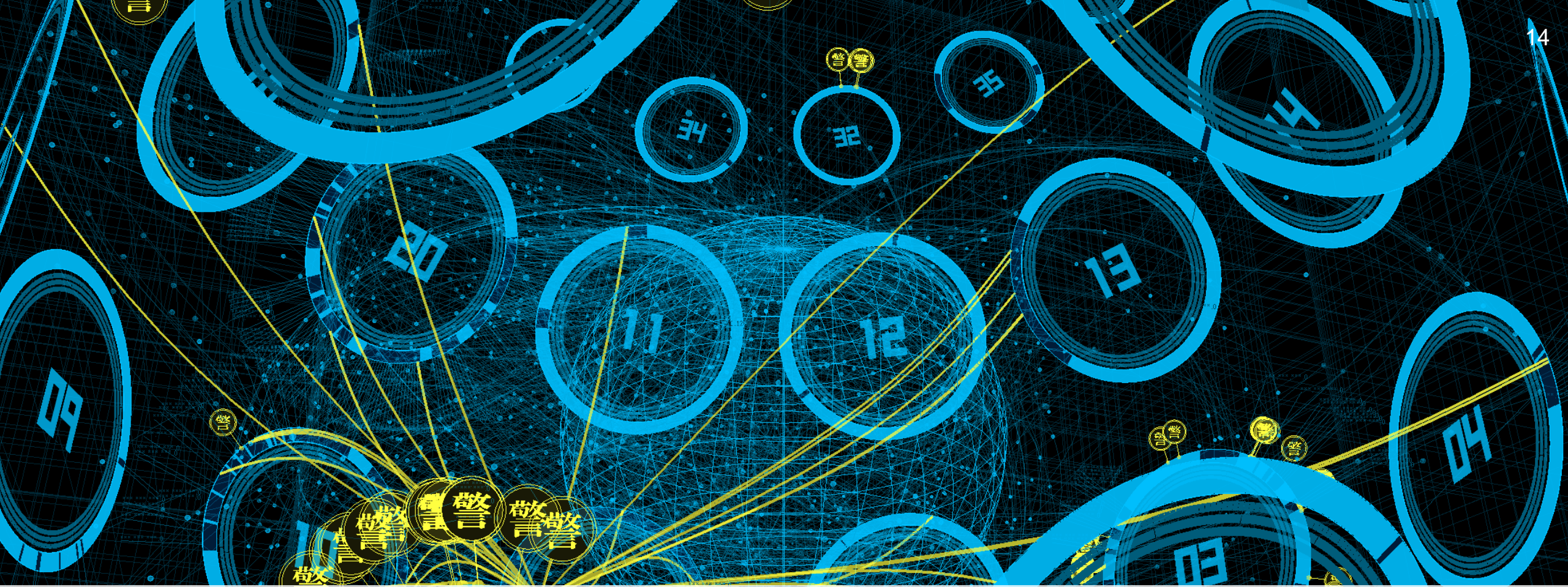
サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

能

Active

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response



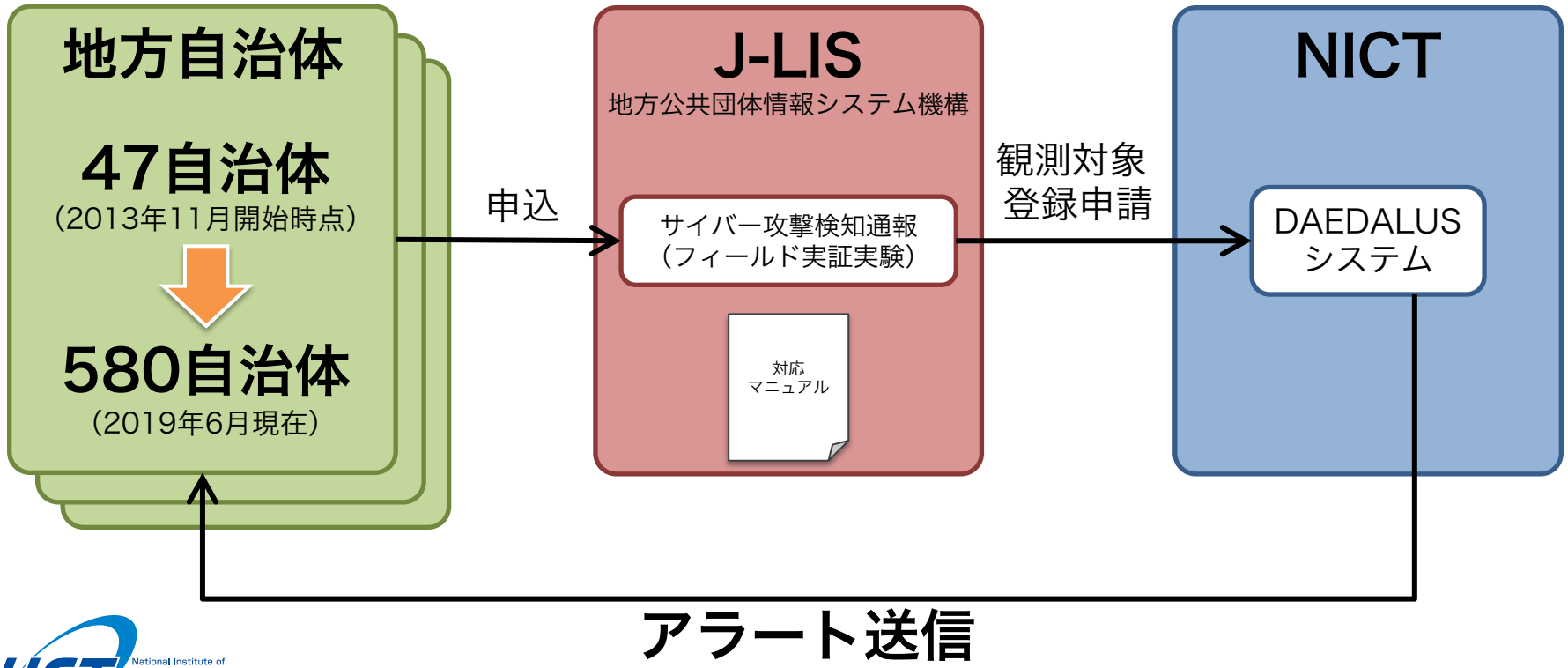
DAEDALUS

- 大規模ダークネット観測に基づく**アラートシステム**
- 組織内のウイルス感染端末からの攻撃を検知
- 約600の地方自治体にアラート無償提供中

DAEDALUSの成果展開：国内展開

地方自治体へのアラート提供

- **2013年11月1日より、地方自治体に向けてアラート送信開始**
  - 地方公共団体情報システム機構（J-LIS）を窓口として自治体より申込受付
  - アラート発生時の対応マニュアルをNICTとJ-LISで整備



サイバー攻撃検知通報

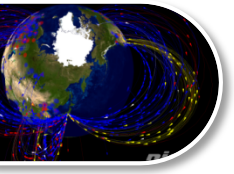
一般企業へのアラート提供

- **SiteVisor**：クルウィット社による商用アラートサービス
- **えぬえすはるか**：日鉄ソリューションズ社による商用アラートサービス

クルウィット
『SiteVisor』

日鉄ソリューションズ
『えぬえすはるか』

サイバーセキュリティ研究室 研究マップ



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改

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）

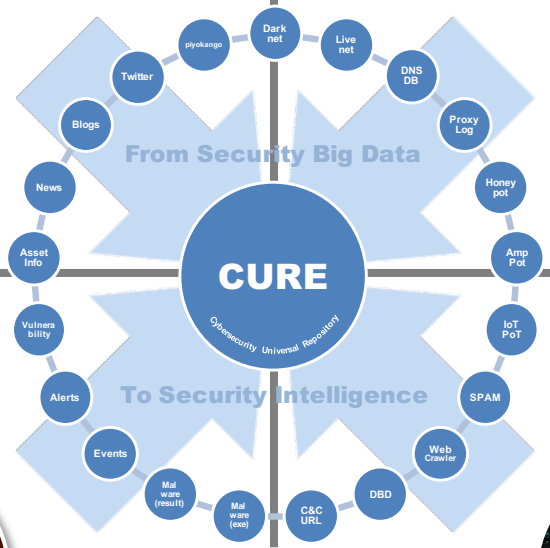
NIRVANA改弐

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

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

NIRVANA改

- セキュリティオペレーションを効率化する**統合分析プラットフォーム**
- セキュリティ機器群からのアラートを集約・分析・トリアージ
- 組織の末端までセンサを設置しトラフィック観測・分析・可視化

NIRVANA改の成果展開：商用展開

一般企業へのライセンス販売

- **WADJET（ウジャト）**：ディアイティ社によるセキュリティ製品
- **えぬえすみはる**：日鉄ソリューションズ社によるセキュリティ製品
- **CyNote**：構造計画研究所によるセキュリティ製品

DIT
『WADJET』

日鉄ソリューションズ
『えぬえすみはる』

構造計画研究所
『CyNote』

CURE

- サイバーセキュリティ関連情報を集約・分析する**セキュリティ情報融合基盤**
- 散在する多種多様な情報をつなぎ合わせてサイバー攻撃の隠れた構造を解明
- 外部の脅威情報を自組織と関連付けセキュリティ・オペレーションを効率化

サイバーセキュリティ技術に関する展示案内

- ５号館３階
- 展示・デモ
  - 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
  - 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改弐
  - サイバーセキュリティユニバーサル・リポジトリ
    CURE
- 説明員常駐