サイバー攻撃の現状と
サイバーセキュリティ研究の最前線

井上 大介
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

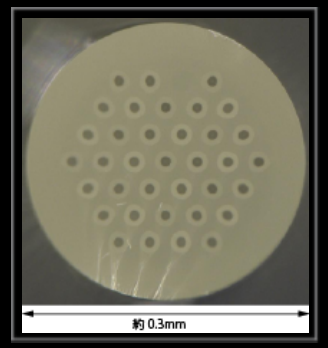
NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

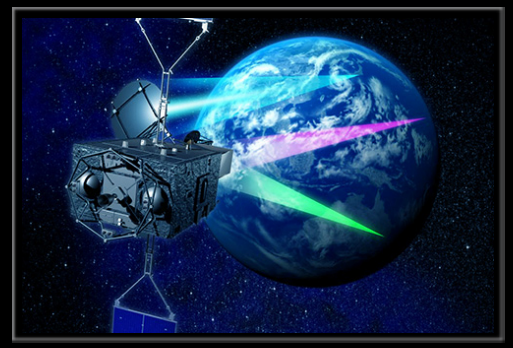
国立研究開発法人 情報通信研究機構とは？

● 情報通信分野を専門とする日本で唯一の公的研究機関

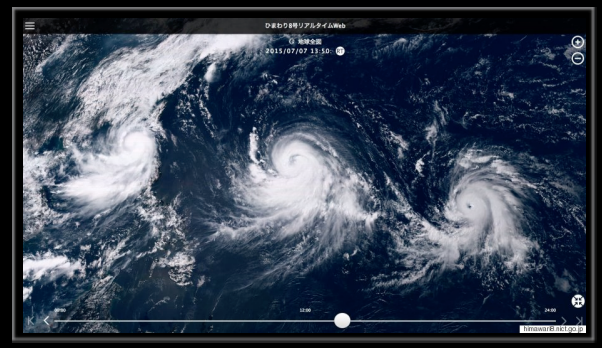
日本標準時の生成・配信
（うるう秒挿入）



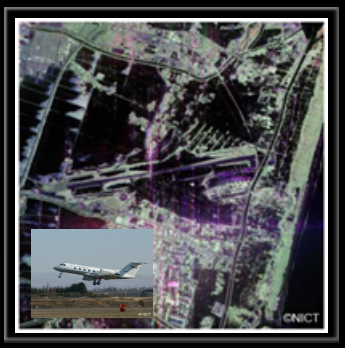
光通信システム
（ペタbps級 マルチコアファイバ）



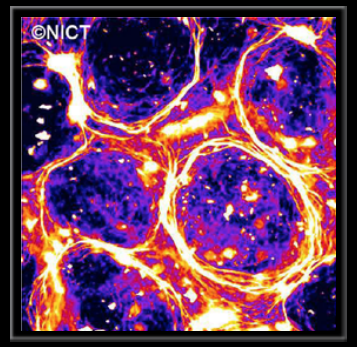
宇宙通信システム
（超高速インターネット衛星きずな）



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）

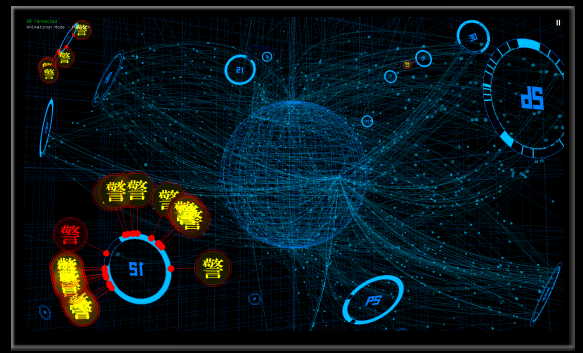


バイオ・ナノICT
（生体分子の自己組織化）

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）

サイバー攻撃の変遷

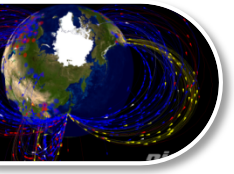
- 20世紀：愉快犯/自己顕示

Richard Skrenta
世界初のウイルス作成者（当時高校生）
(http://www.skrenta.com)

- 21世紀：経済犯
  示威活動（Hacktivism）
  諜報活動（Cyber Espionage）

Anonymous
(Vincent Diamante - originally posted to Flickr as Anonymous at Scientology in Los Angeles)

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）

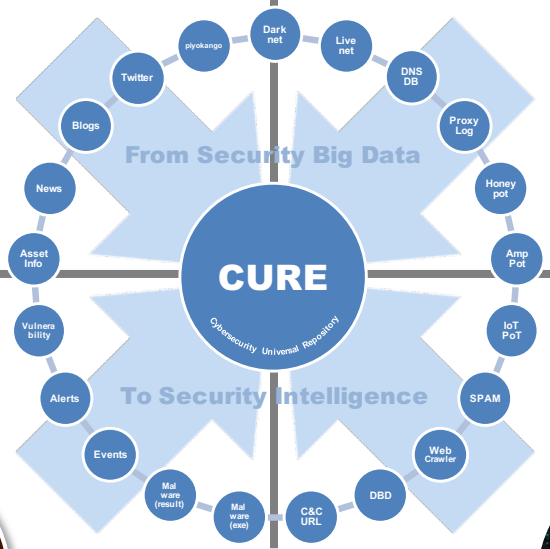
NIRVANA改弐

Global (無差別型攻撃対策)

(標的型攻撃対策) Local

全

局



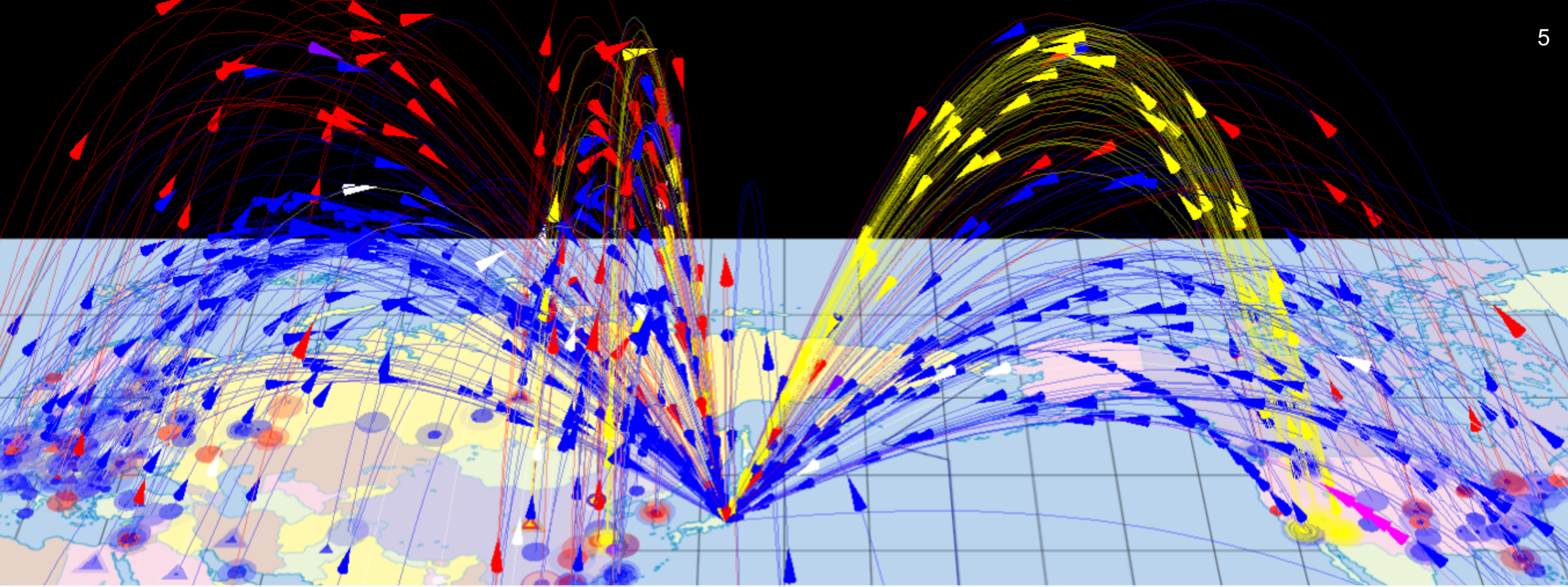
サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

能

Active

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response



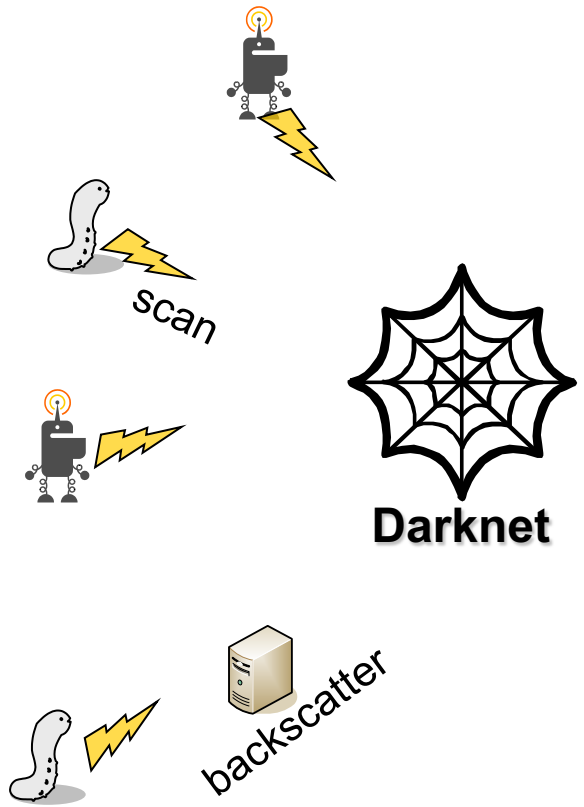
NICTER

- 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

ダークネットとは？

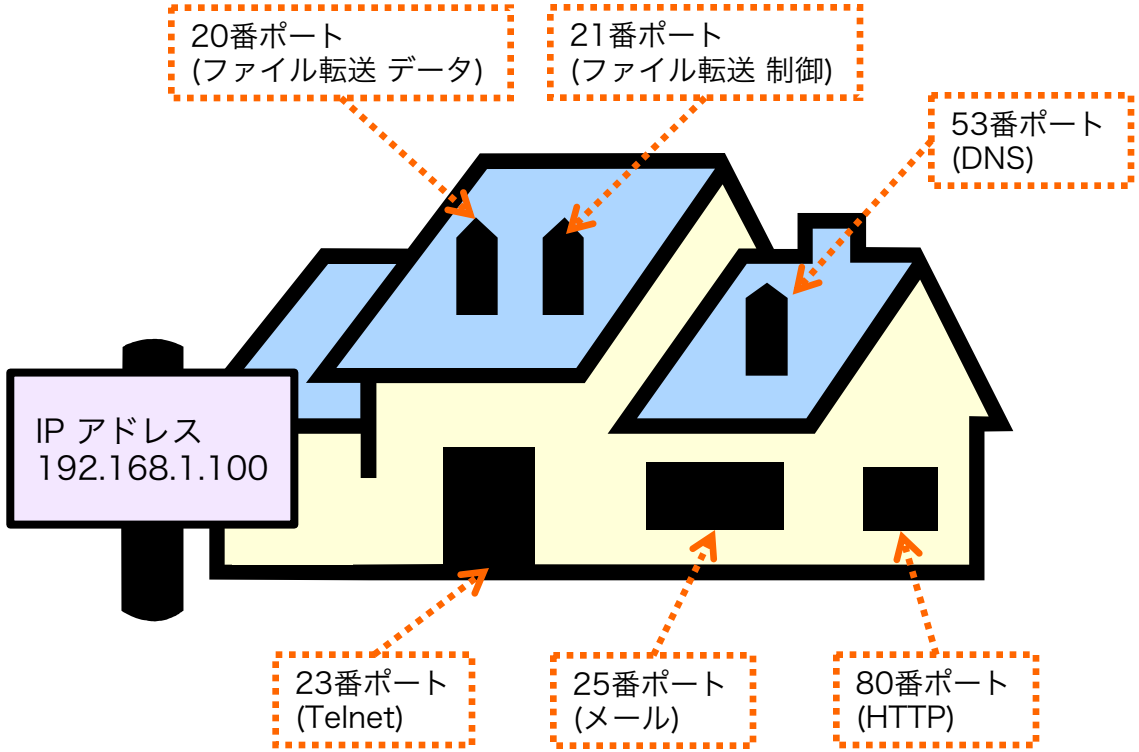
- **ダークネット = 未使用IPアドレスブロック**
  - ✓何もない所にパケットが飛んでくること自体おかしい

- **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
  - ✓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



IPアドレス と ポート番号

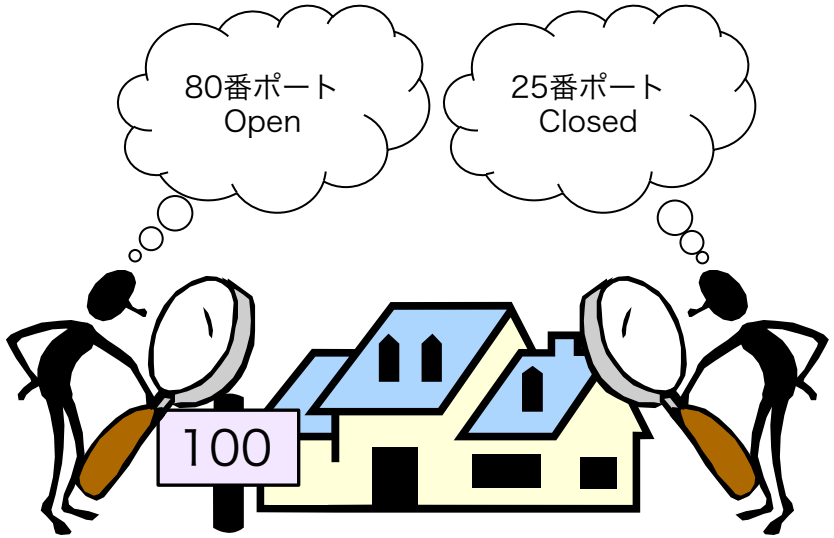
- IPアドレス： インターネット上の一意の識別子（住所）
- ポート番号： サービスを特定するための番号（窓）



ポートスキャンとネットワークスキャン

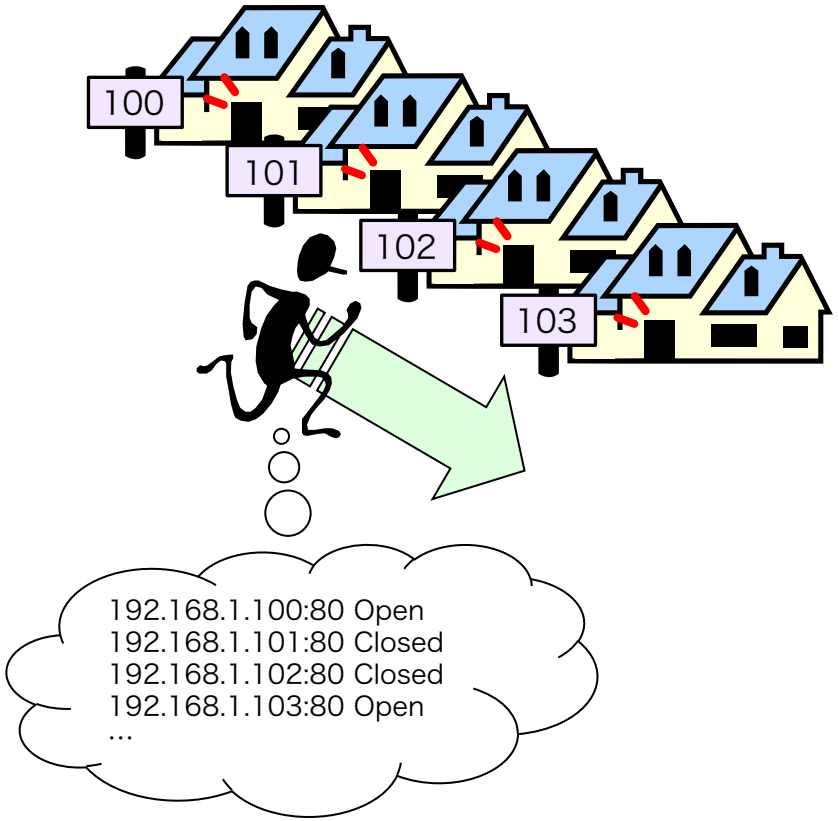
● ポートスキャン

1ホストに対して複数のポートをスキャン



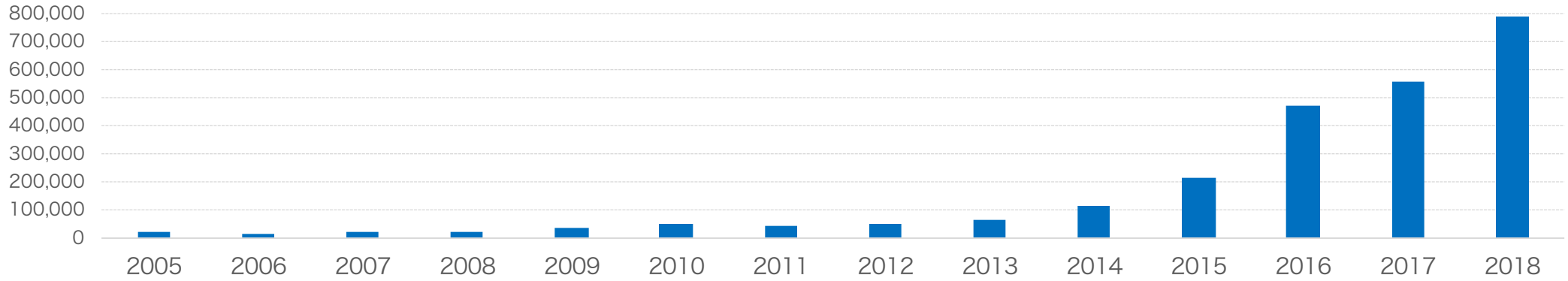
● ネットワークスキャン

複数のホストの特定のポートをスキャン



NICTER観測統計（2005-2018）

年	年間総観測パケット数	観測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
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
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**

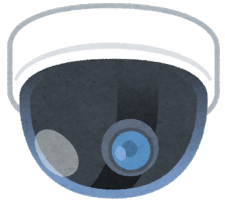


1 IPアドレスあたりの年間総観測パケット数


IoT
Internet of Things
横浜国立大学
吉岡研究室による調査
YOKOHAMA National University
YNU
10
HG8245
HUAWEI
嵌入式電話錄音主機WEB管理系統
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
Web Application
pandora
BUSINESS SUITE
HOT box
Login
Password
Save login and password
Apply
Record System Copyright2008
BISBOX
BUSINESS INTERNET
RouterOS v5.22
WebFig Login:
Winbox
Telnet
Graphs
License
Help
Username
Password
Login
DiskStationPlay
Aanmelden
11n 150Mbps WLAN ADSL2+ Modem Router
Status
Network
Wireless
Уровень безопасности:
WPA2-Personal
DrayTek
ZTE中兴
F460
Please login...
Welcome To
Streamyx Connection
Setup
Quick Setup mode
Network video client
LOGIN
VoIP ITA

感染IoT機器をさがせ！

問題：あなたの身の回りでマルウェアに感染する可能性のある機器はどれ？



Webカメラ

IP電話

ホームルータ

モバイルルータ

ビデオレコーダ(DVR)

複合機

記憶媒体(NAS)

感染IoT機器の分類（2016年9月）

- 横浜国立大学 吉岡研究室による調査結果 -

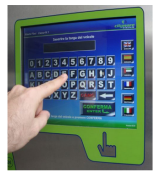
- **Surveillance camera**
  - IP camera
  - DVR

- **Network devices**
  - Router, Gateway
  - Modem, bridges
  - WIFI routers
  - Network mobile storage
  - Security appliances




- **Telephone**
  - VoIP Gateways
  - IP Phone
  - GSM Routers
  - Analog phone adapters


- **Infrastructures**
  - Parking management system
  - LED display controller


- **Control system**
  - Solid state recorder
  - Sensors
  - Building control system (bacnet)

- **Home/individuals**
  - Web cam, Video recorders
  - Home automation GW
  - Solar Energy Control System
  - Energy demand monitoring system

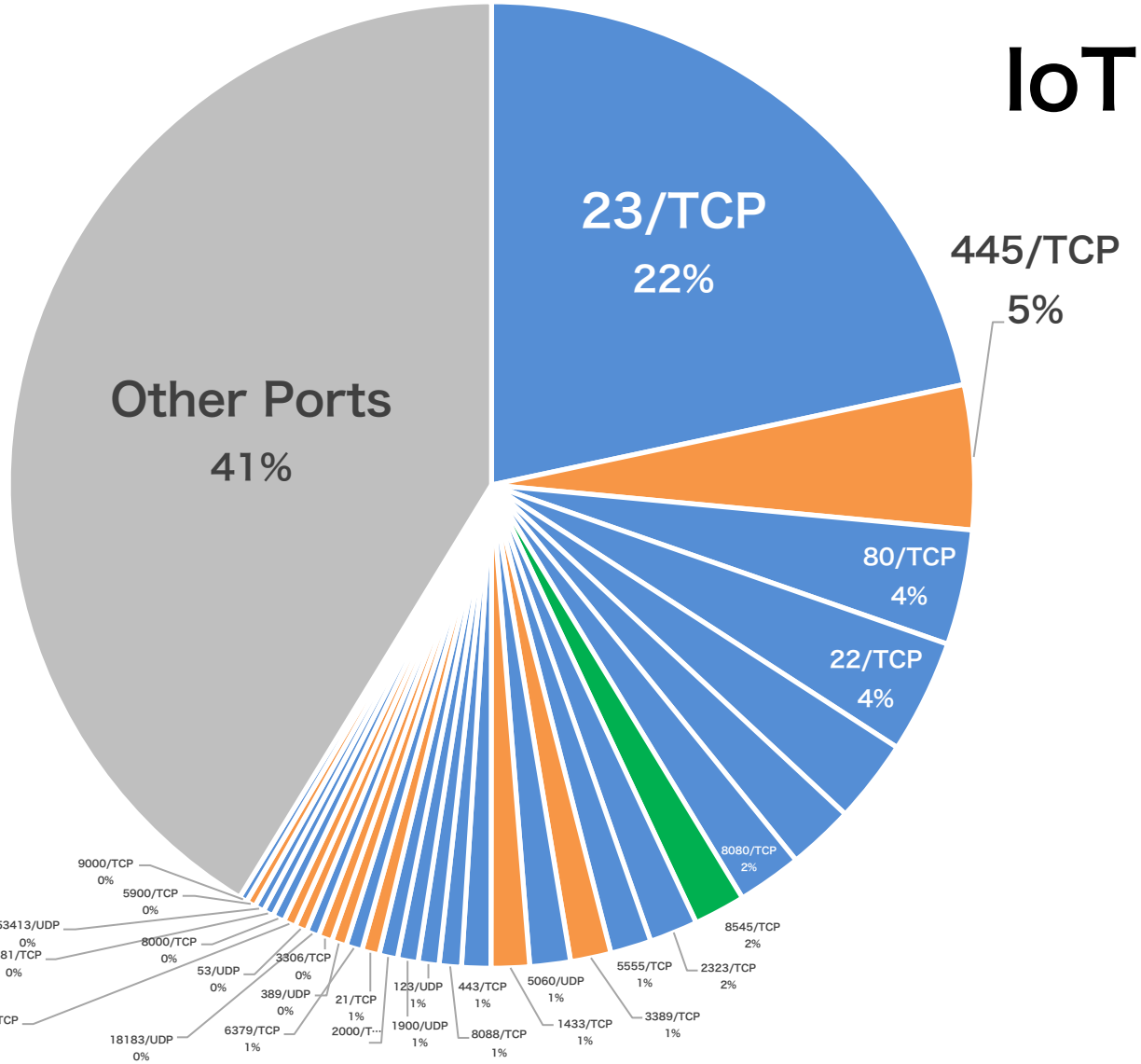
- **Broadcasting**
  - Media broadcasting
  - Digital voice recorder
  - Video codec
  - Set-top-box


- **Etc**
  - Heat pump
  - Fire alert system
  - Medical device(MRI)
  - Fingerprint scanner


NOTE: Devices are inferred by telnet/web banners

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 -

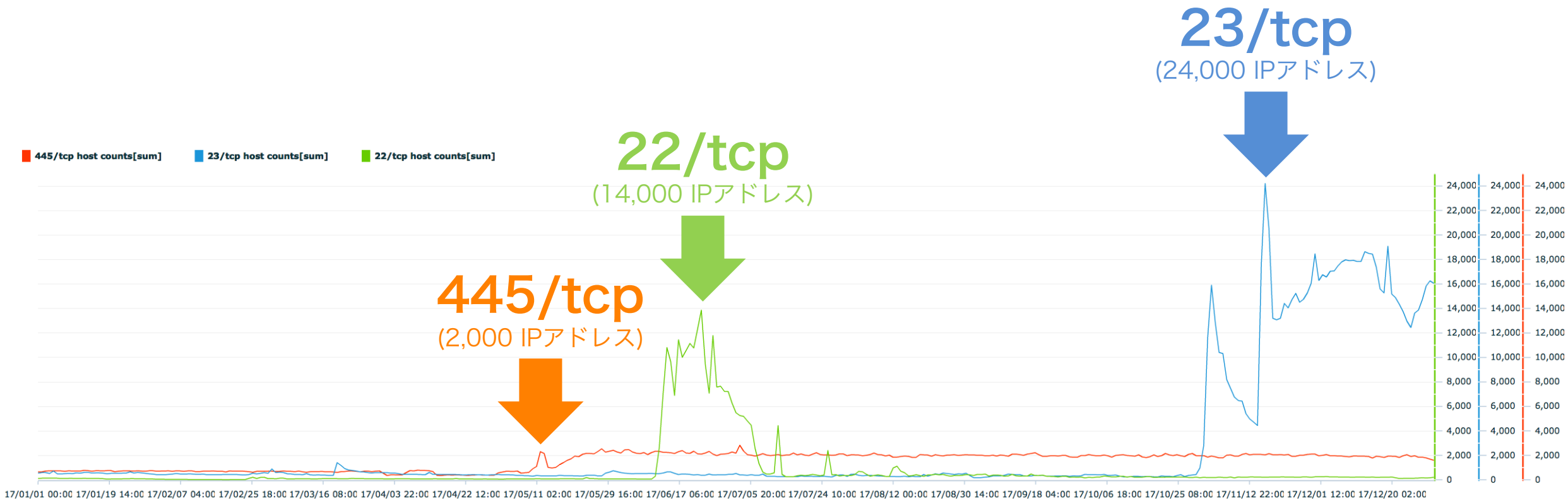


IoT = 47.7%（上位30ポート中）

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）

日本国内の大規模感染 Top 3（2017）

- 日本国内の送信元IPアドレス数/日 -



２０１７年1月1日～12月31日

国内の主な感染端末（2017）

- **445/tcp (SMB)**
  - ✓ 2017年5月～
  - ✓ Windows（WannaCry）

出典：Symantec

https://www.symantec.com/security_response/writeup.jsp?docid=2017-051310-3522-99

- **22/tcp (SSH)**
  - ✓ 2017年6月～
  - ✓ 国内モバイルルータ

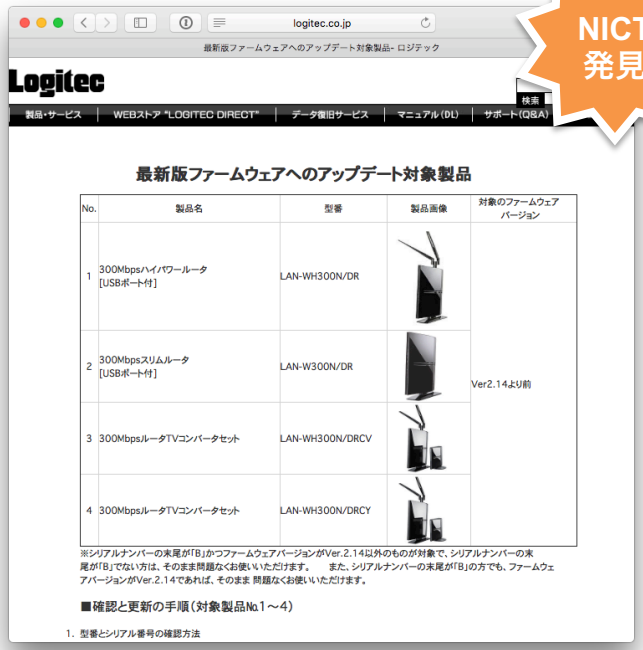
NICT 発見

出典：週刊アスキー

http://weekly.ascii.jp/elem/000/000/404/404196/

- **23/tcp (telnet)**
  - ✓ 2017年11月～
  - ✓ 国内ホームルータ

NICT 発見



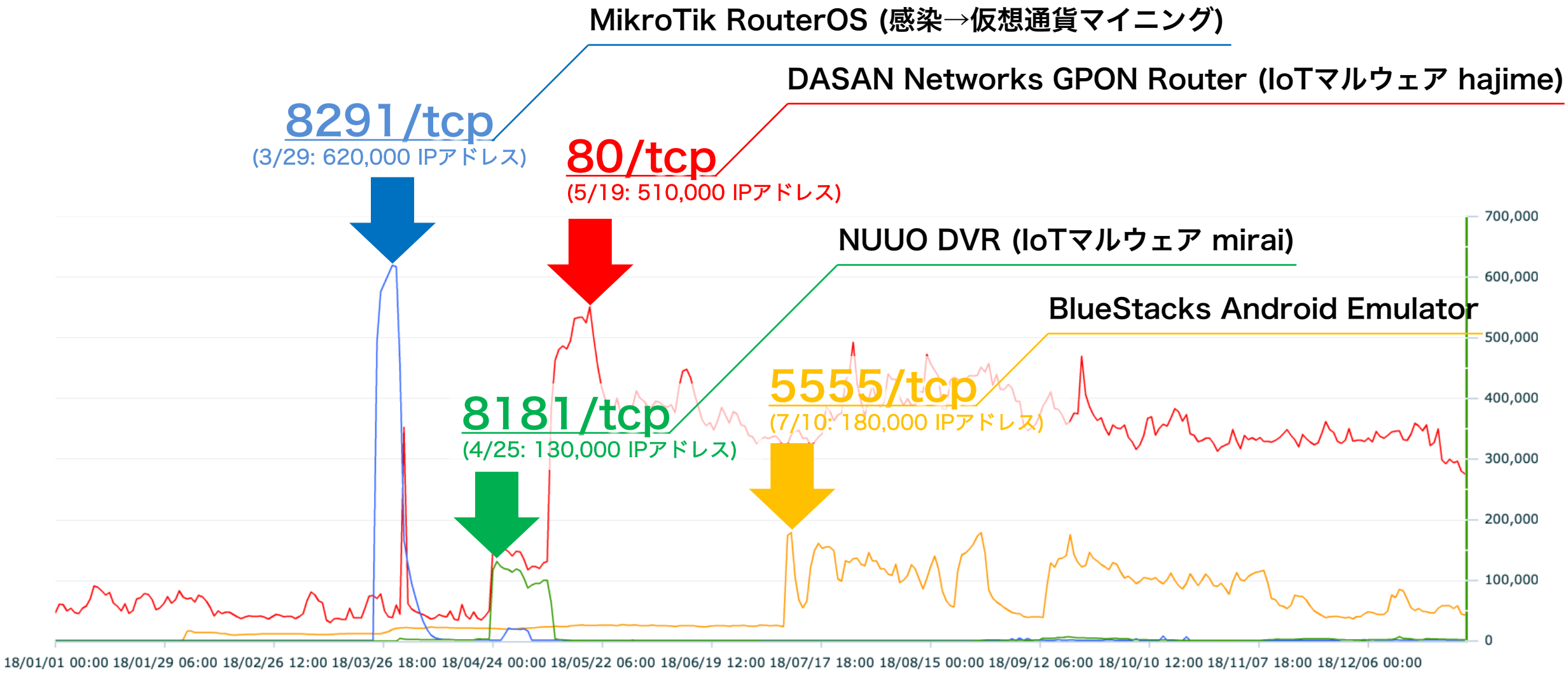
出典：Logitec

http://www.logitec.co.jp/info/wireless-router.html

国内における脆弱性ハンドリング

- Coordinated Vulnerability Disclosure -

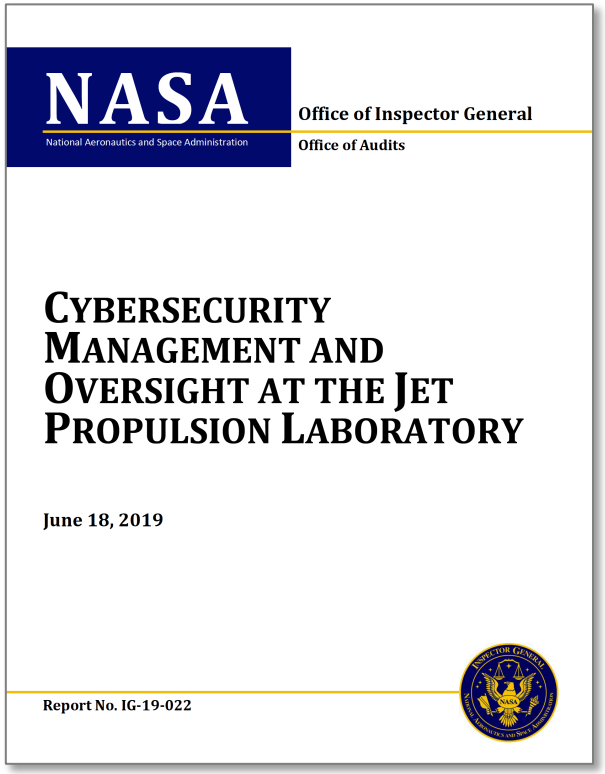
2018年の主な大規模感染事例



ユニークホスト数/日（2018年1月～12月）

NASAへのサイバー攻撃（2019）

- 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

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。

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://www.flickr.com/photos/biglesp/14234773312/"を新規タブで開く

https://oig.nasa.gov/docs/IG-19-022.pdf
https://www.itmedia.co.jp/news/articles/1906/23/news012.html
https://gigazine.net/news/20190625-nasa-hacked-raspberry-pi/

今すぐできる！ IoT機器セキュリティ対策 6選

1. **IoT機器の再起動**（揮発型のマルウェアを消滅させる）
2. **ファームウェアのアップデート**（脆弱性を塞ぐ）
3. **ID/パスワードを変更**（初期パスワードでの侵入を防ぐ）

4. **インターネット側からのアクセス拒否設定**（外から繋がせない）
5. **ゲートウェイ機器の内側に設置**（直接インターネットに繋がない）
6. **古い機器は買い換える**（自動アップデート機能がない機器はNG）

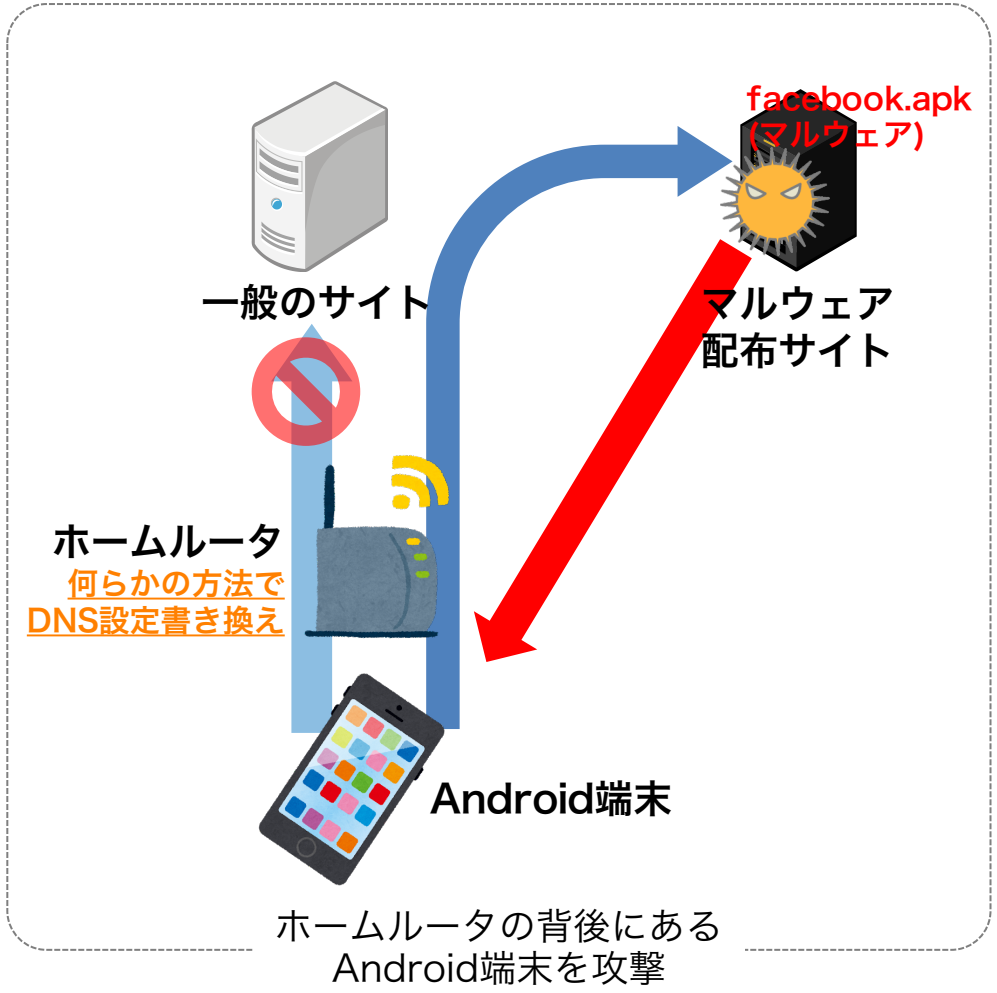
IoT機器ベンダにおけるセキュリティ対策

- **セキュアコーディングの徹底**
- **セキュリティ開発ライフサイクルの整備**
- **OEMの受入検査強化**（例：ペネトレーションテスト、ファジング）
- **IoT機器導入時のマニュアルの整備**（例：グローバルIPアドレスを付与しない）

- **参考資料**
  - ✓ JPCERT/CC 『セキュアコーディング』
    https://www.jpcert.or.jp/securecoding/
  - ✓ JPCERT/CC 『IoTチェックリスト』
    https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html
  - ✓ 日本マイクロソフト 『信頼できるコンピューティングのセキュリティ開発ライフサイクル』
    https://msdn.microsoft.com/ja-jp/library/ms995349.aspx
  - ✓ IoT 推進コンソーシアム 『IoT セキュリティガイドラインver 1.0』
    http://www.soumu.go.jp/main_content/000428393.pdf

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)

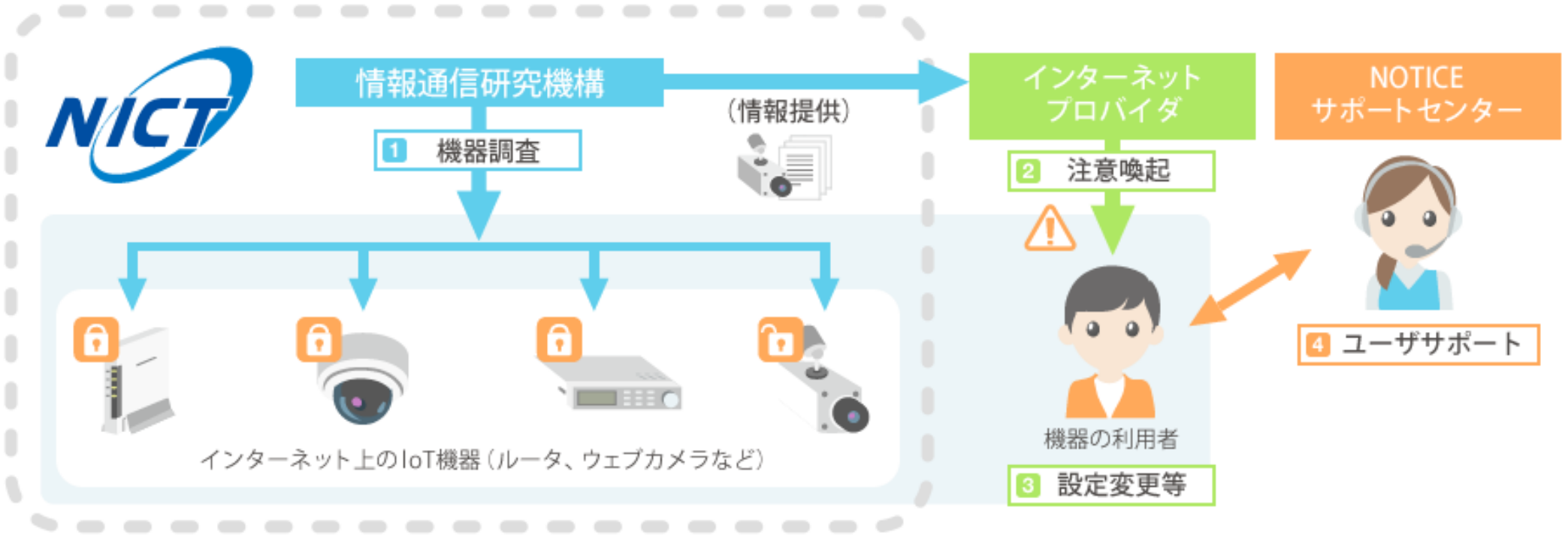
まずは…

容易に推測されるID/パスワード

で動いているIoT機器をなんとかしたい！

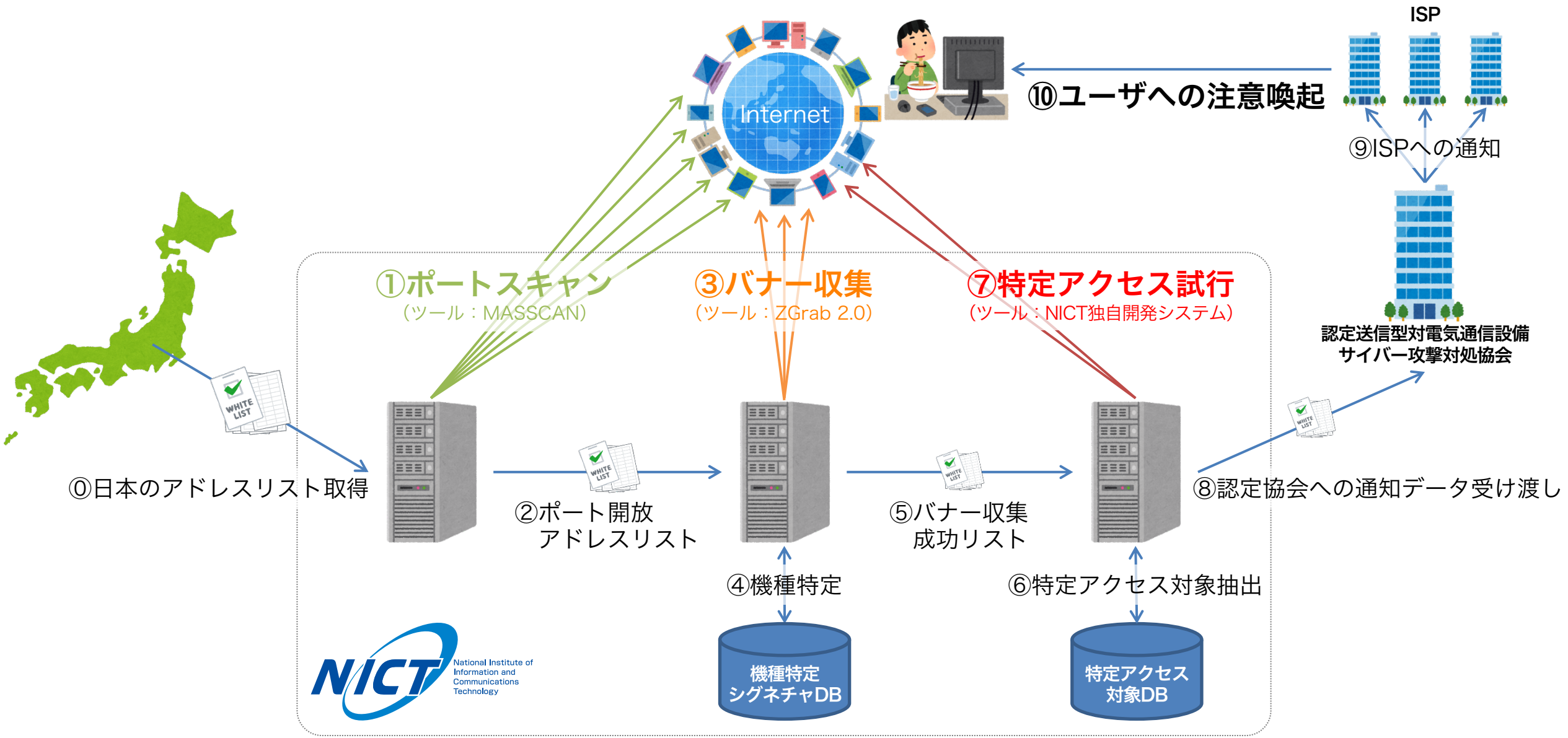
NOTICE

- 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/

NICTによるIoT機器調査の技術詳細



能動的対策と受動的対策

能動的対策

パスワード設定等に
不備があるIoT機器

能動的観測

NOTICE
National Operation Towards IoT Clean Environment

通知

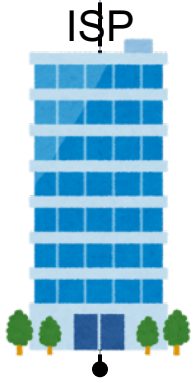
受動的対策

感染IoT機器

受動的観測

NICTER

通知



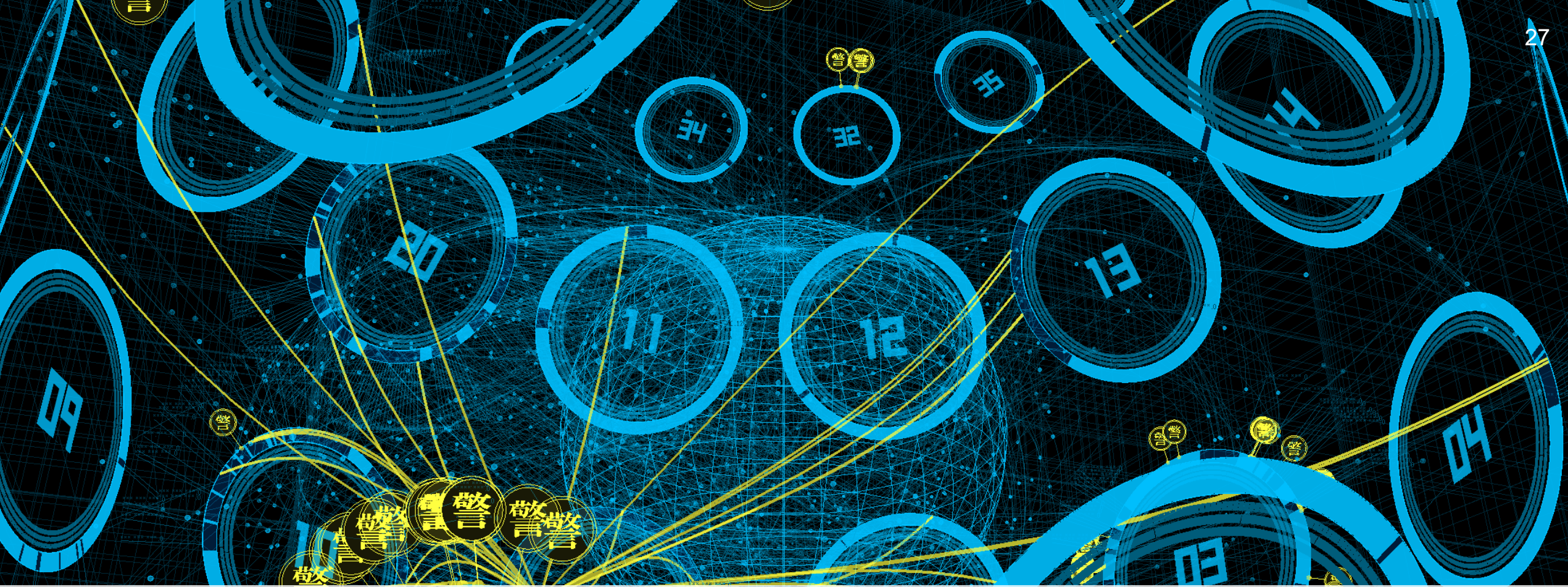
ISP

NOTICE 注意喚起の実施状況（2019年10月25日）

NOTICE National Operation Towards IoT Clean Environment（アクティブスキャン）　NICTER（パッシブモニタリング）

NOTICE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の取組結果
調査対象となったIPアドレスのうち、 ID・パスワードが入力可能であったもの → **約111,000件** 上記の内、ID・パスワードによりログインでき、 注意喚起の対象となったもの → **延べ1,328件**	ISPに対する通知の対象となったもの → **1日当たり60～598件**

出典：総務省、NICT、ICT-ISAC “脆弱なIoT機器及び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の実施状況（2019年度第3四半期）”
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00058.html



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

境界防御技術とDAEDALUS

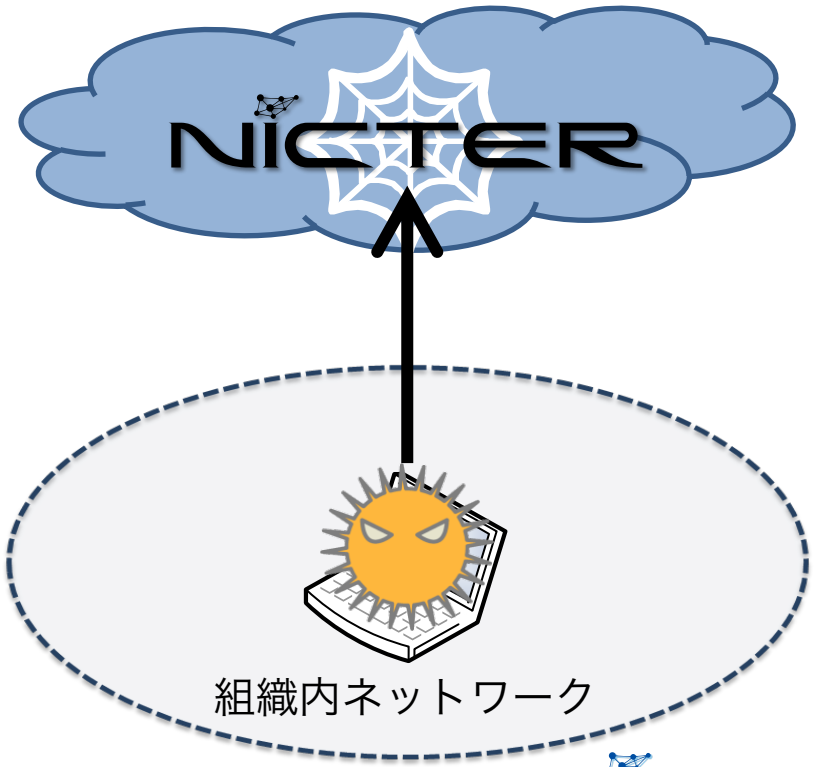
境界防御技術（従来技術）

組織外からの攻撃をネットワーク境界で検出

相補的

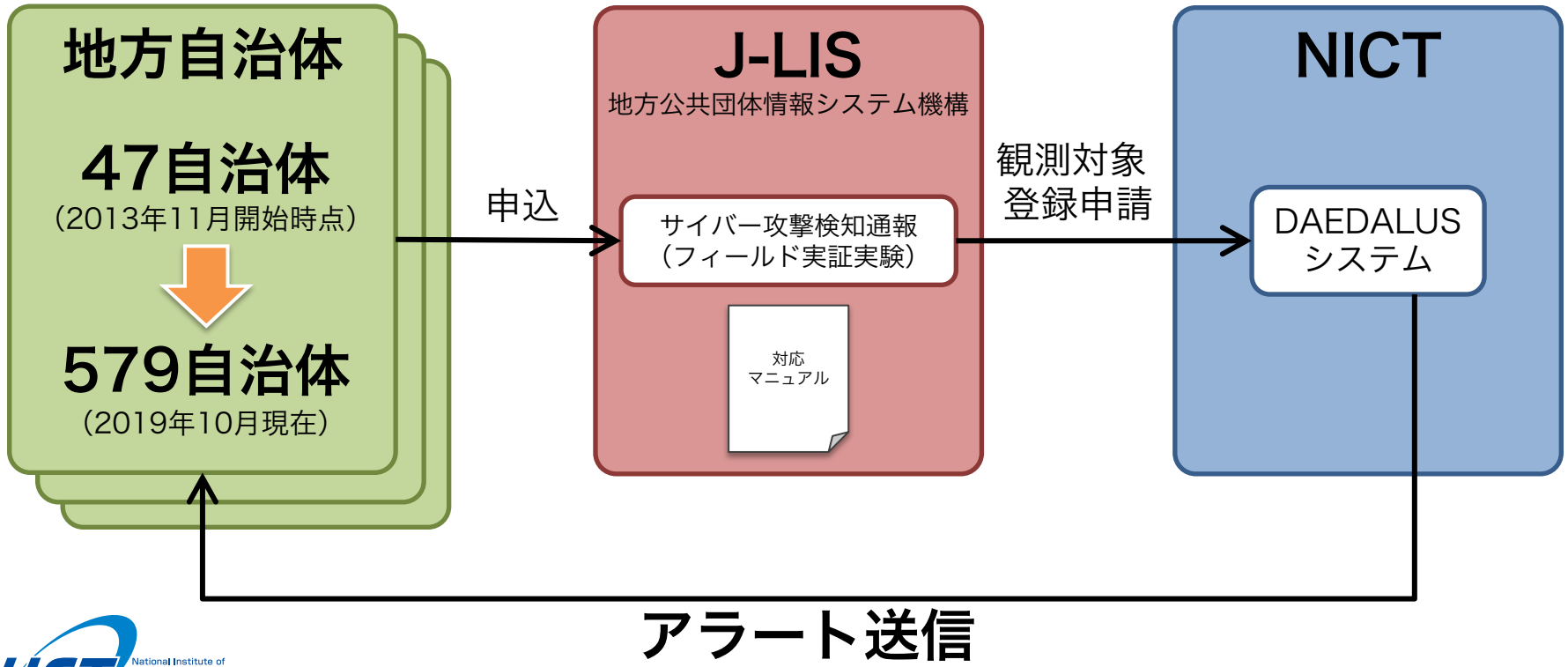
DAEDALUS

組織内からの攻撃をネットワーク広域で検出



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

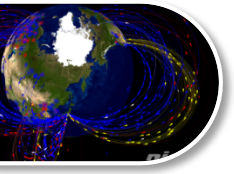
一般企業へのアラート提供

- **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）

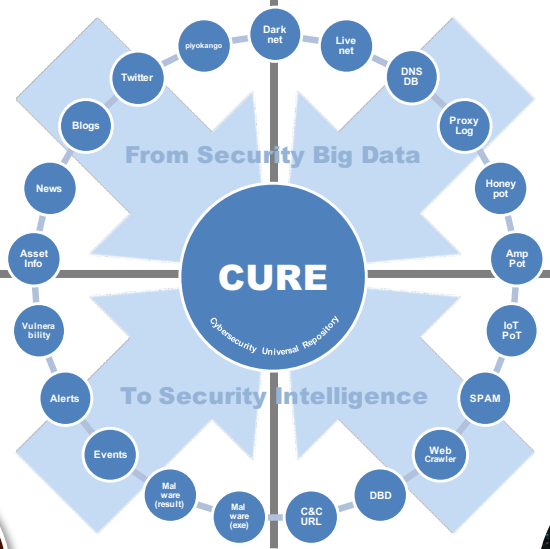
NIRVANA改弐

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

セキュリティオペレーション現場の悩み

- セキュリティ対策を頑張れば頑張るほど…

警告が増えすぎて
対応できない！

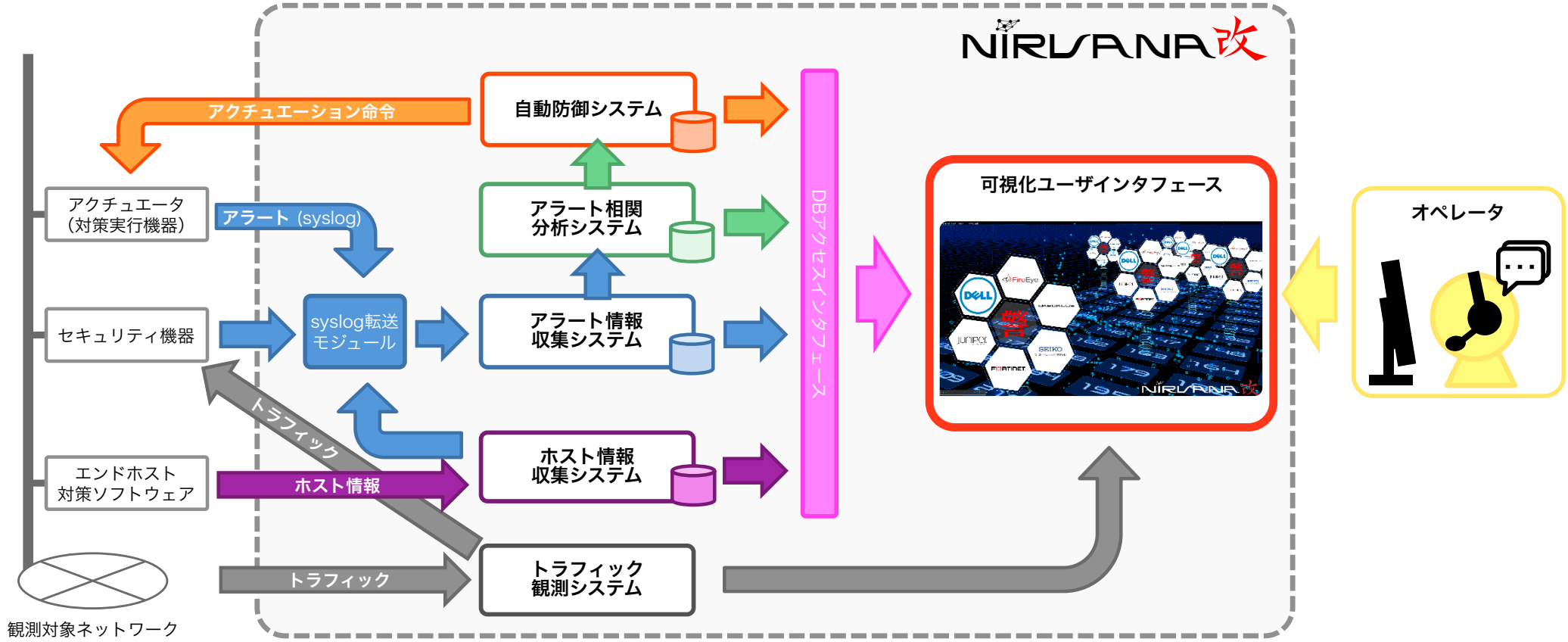
NIRVANA改

- 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 システム構成

NIRVANA改

＝ トラフィック観測・分析 ＋ アラート収集・分析 ＋ 自動対処 ＋ 可視化




SHOWNET
DIVE INTO THE NEXT
SHOWNET
DIVE INTO THE NEXT
HUAWEI
NEC
NTT
SCSK
YAMAHA
axsh
FURUNO SYSTEMS
SHOWNET
DIVE INTO THE NEXT
Interop® Tokyo
13 – 15 JUNE 2018 | MAKUHARI MESSE | JAPAN
25th
Interop セミナー
Tokyo
IoT・5G・V2X

NIRVANA改 2019

- セキュリティ・オーケストレーション@Interop Tokyo 2019 -

● アラート連携アプライアンス・ソフトウェア：23種（12社）

Vendor Name	Product Name
NICT	DAEDALUS
	CURE Flow
Future	Vuls
FFRI	yarai
TrendMicro	TippingPoint TPS
	TippingPoint SMS
	Deep Discovery Inspector
	Deep Discovery Analyzer
Check Point	Security Appliances
	Smart-1 525
	SandBlast TE2000X
DAMBALLA	Network Insight

Vendor Name	Product Name
FireEye	NX5500
Fortinet	FortiGate 3601E
	FortiGate 601E
	FortiSandbox 3000E
	FortiDeceptor 1000F
Juniper Networks	JATP400
Lastline	Defender
Palo Alto Networks	PA-5280
	PA-5260
	M-600
A10 Networks	Thunder 3230 CFW

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』

NIRVANA改の実用事例

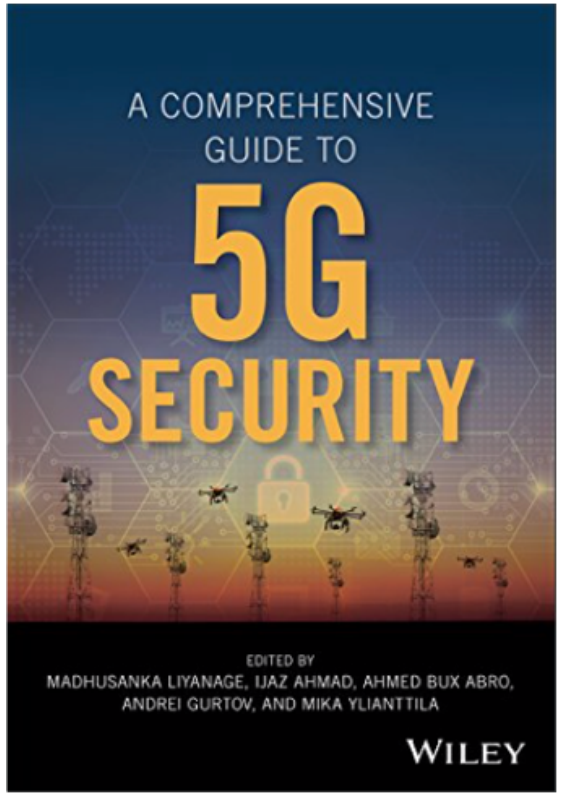
長崎県立大学
（大学ネットワーク）

日立造船
（制御系システム）

5Gセキュリティ

セキュリティの脅威：1Gから5G

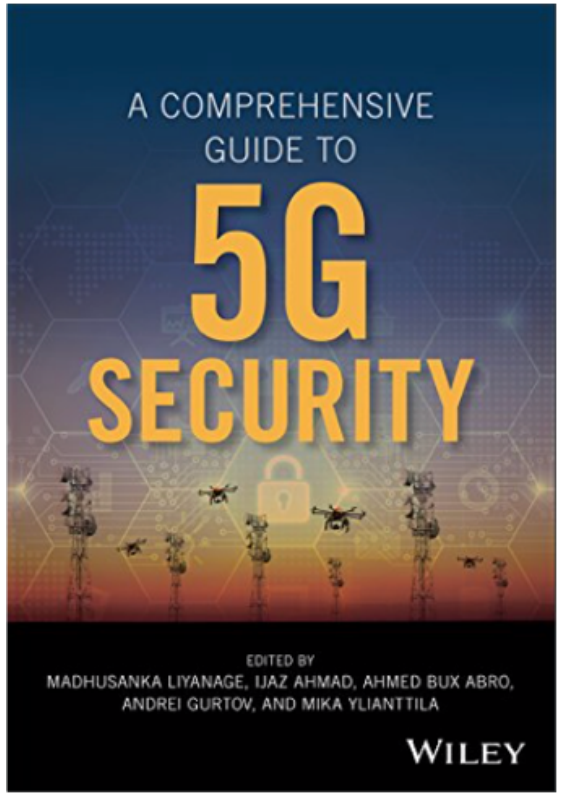
	年	アプリケーション	脅威
1G	1970-1980	音声通話	物理的盗聴, 詐欺
2G	1990-2004	音声通話 + テキスト	スパム, 不正基地局
3G	2004-2010	音声通話 + インターネット	ウイルス, スパイウェア, 不正アプリ
4G	2011-2015	音声通話 + ビデオ + インターネット	モバイルウェア, 標的型攻撃, DDoS攻撃
5G	2020	コネクテッド・ワールド	サイバー戦, スパイ活動, 重要インフラ攻撃



出典: “A Comprehensive Guide to 5G Security,” Wiley, Jan 2018.

5Gセキュリティのトピック

- **Part II: 5Gネットワークセキュリティ**
  - ✓ Physical Layer Security
  - ✓ 5G-WLAN Security
  - ✓ Safety of 5G Network Infrastructure
  - ✓ Customer Edge Switching: A Security Framework for 5G
  - ✓ Software Defined Security Monitoring in 5G Networks
- **Part III: 5Gデバイス＆ユーザセキュリティ**
  - ✓ IoT Security
  - ✓ User Privacy, Identity and Trust in 5G
  - ✓ 5G Positioning: Security and Privacy Aspects
- **Part IV: 5Gクラウド＆仮想ネットワークセキュリティ**
  - ✓ Mobile virtual Network Operators (MVNO) Security
  - ✓ NFV and NFV-based Security Services
  - ✓ Cloud and MEC Security
  - ✓ Regulatory Impact on 5G Security and Privacy

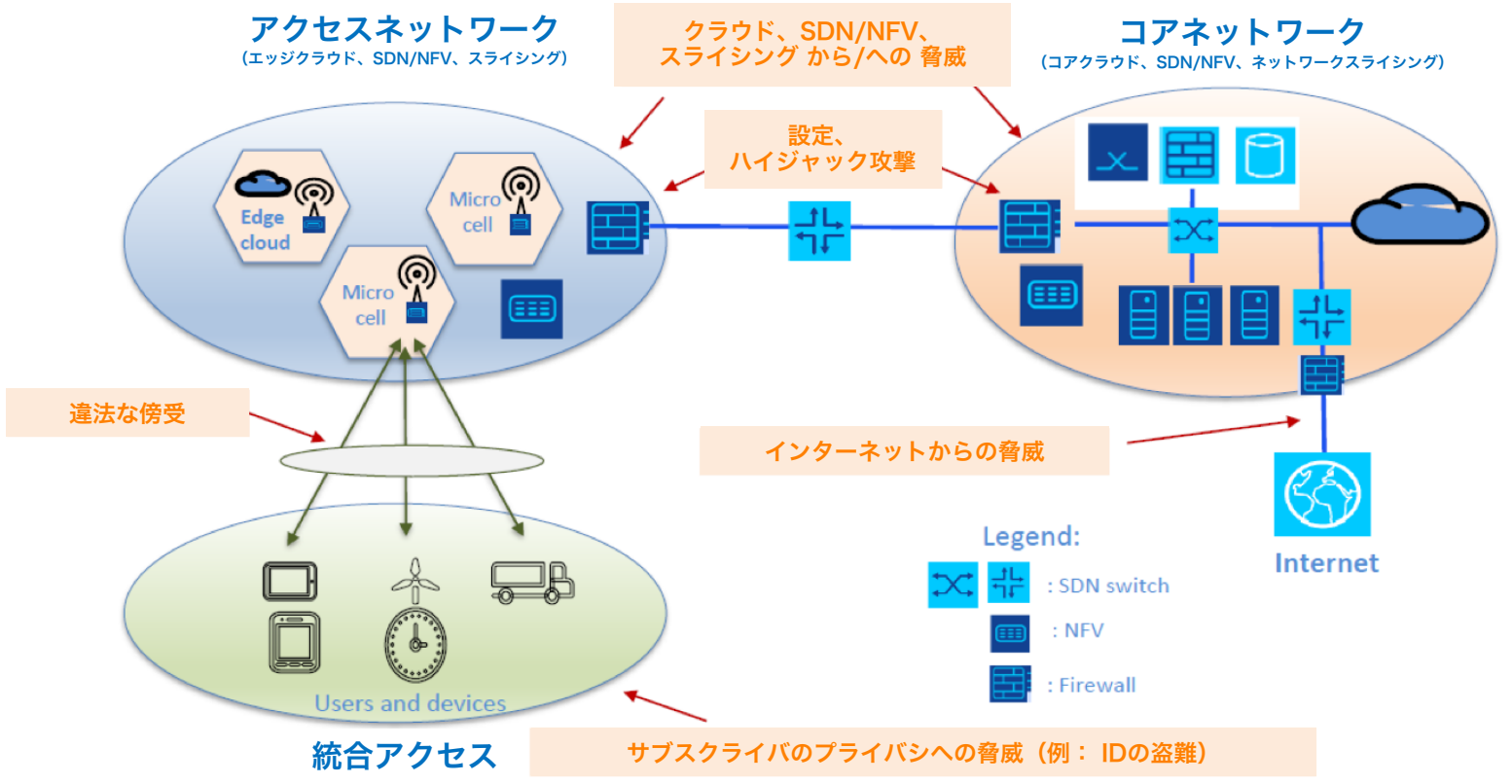


出典: “A Comprehensive Guide to 5G Security,” Wiley, Jan 2018.

ITU-Tでの5Gセキュリティの議論

Study Group Leadership Assembly 2019

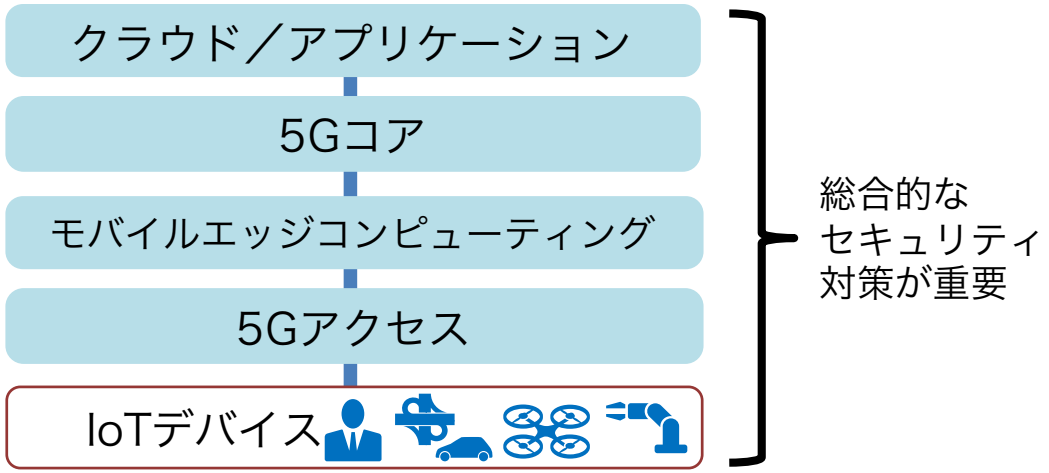
5G security overview - A flexible and dependable 5G network and threats landscape

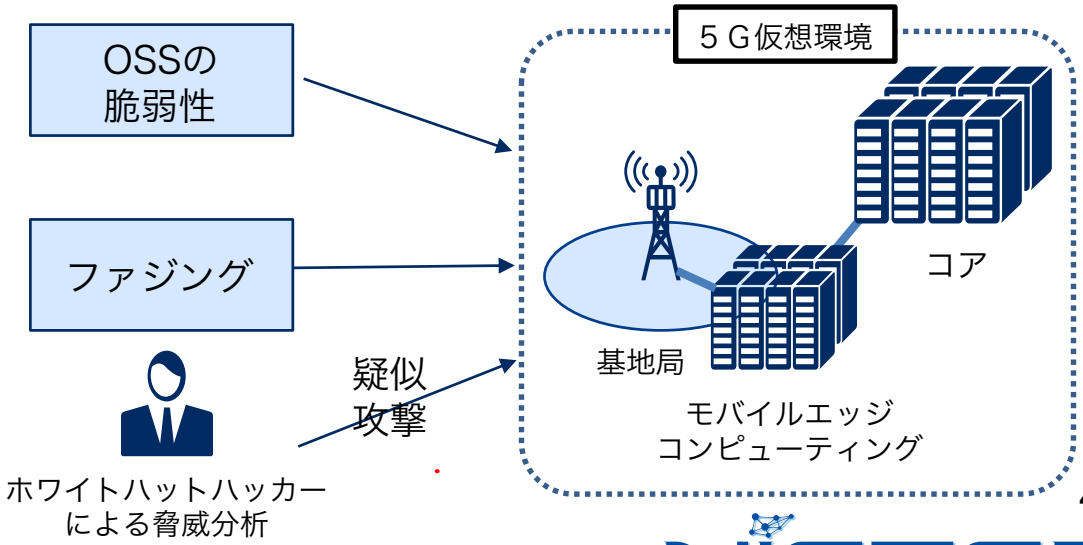


国内における5Gセキュリティの検討

- **総務省直轄プロジェクト** (2020年1月～)
  - ✓ ５Ｇネットワークにおける
    セキュリティ確保に向けた調査・検討
  - ✓ KDDI, NTTドコモ、 NEC、 NICT
- **5Gセキュリティ 動向調査**
- **5Gセキュリティ リスク分析**
- **5Gセキュリティ 検証環境構築**
- **5Gセキュリティ 脆弱性調査/脅威分析**
- **5Gセキュリティ ガイドラインβ版**

<5Gネットワークのイメージ>





サイバーセキュリティの研究開発における
今後の重点課題

● データドリブンなサイバーセキュリティ研究

- ✓ NICTを日本最大のセキュリティビッグデータの集積地に
- ✓ セキュリティビッグデータからセキュリティインテリジェンスへ

● AI x Cybersecurity

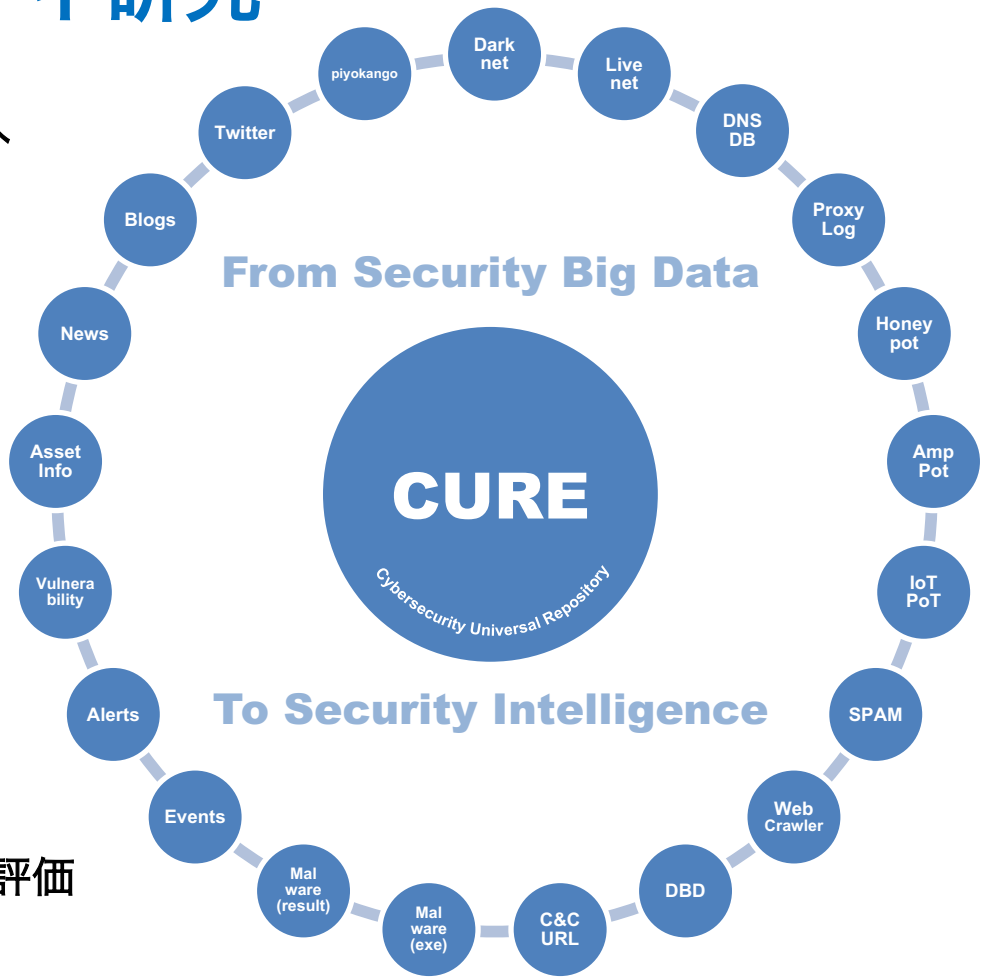
- ✓ 実データに基づくリアルタイム機械学習エンジン開発
- ✓ 機械学習技術を応用したセキュリティオペーレーション高速化

● 5Gセキュリティ

- ✓ 5Gネットワークのコア/エッジ/アクセスのセキュリティ検証
- ✓ NICT＋通信キャリア＋機器ベンダーによる検証体制構築

● セキュリティ自給率の向上

- ✓ NICT自身をテストベッドとした国産セキュリティ技術の検証・評価
- ✓ 国産セキュリティ技術を創り・育て・世界へ展開

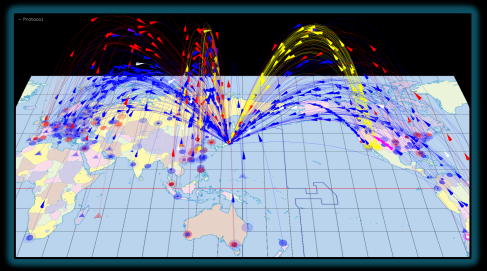


National Institute of Information and Communications Technology

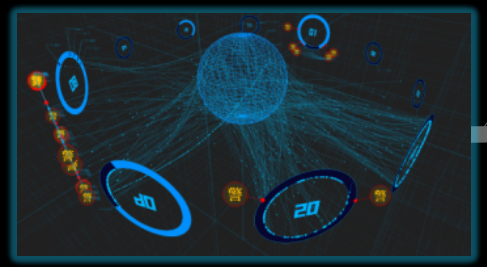
NICTER
Network Incident analysis Center for Tactical Emergency Response

[補足資料]

無差別型攻撃対策



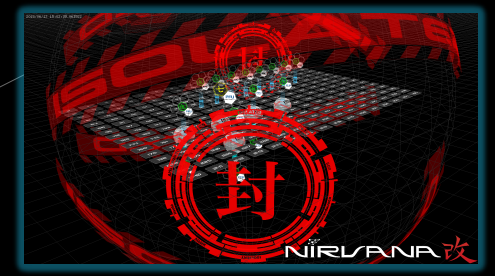
インシデント分析センタ
NICTER



対サイバー攻撃アラートシステム
DAEDALUS

Web媒介型攻撃対策

WARPDRIVE



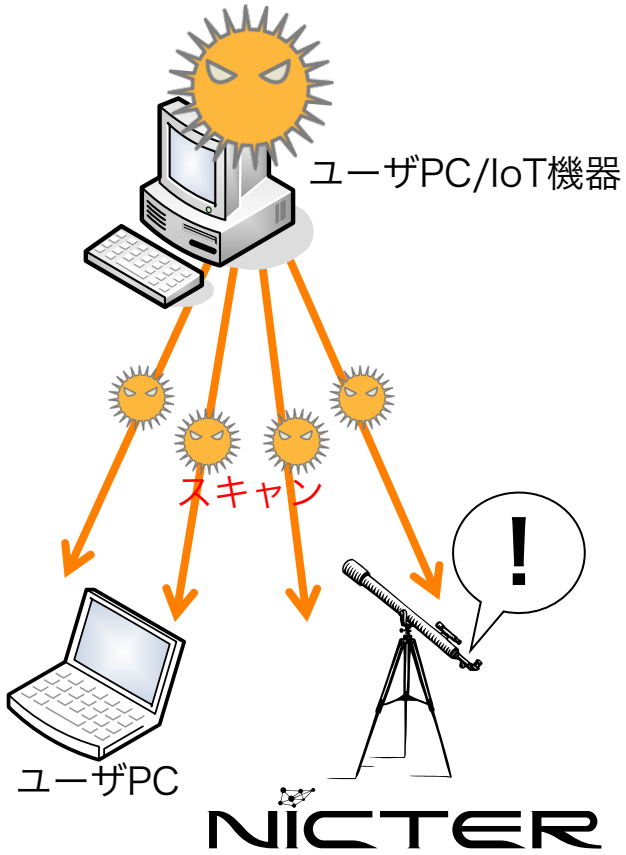
サイバー攻撃統合分析プラットフォーム
NIRVANA改

脆弱性管理プラットフォーム
NIRVANA改弐

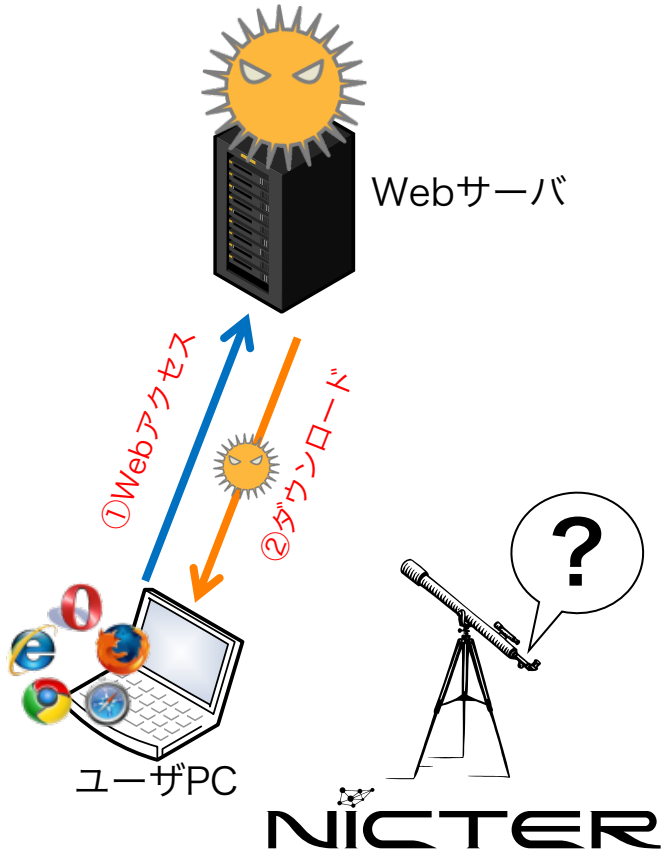
標的型攻撃対策

ワーム型マルウェアとWeb媒介型攻撃の違い

ワーム型マルウェア
（リモートエクスプロイト型マルウェア）



Web媒介型攻撃
（ドライブ・バイ・ダウンロード攻撃）



WARPDRIVE

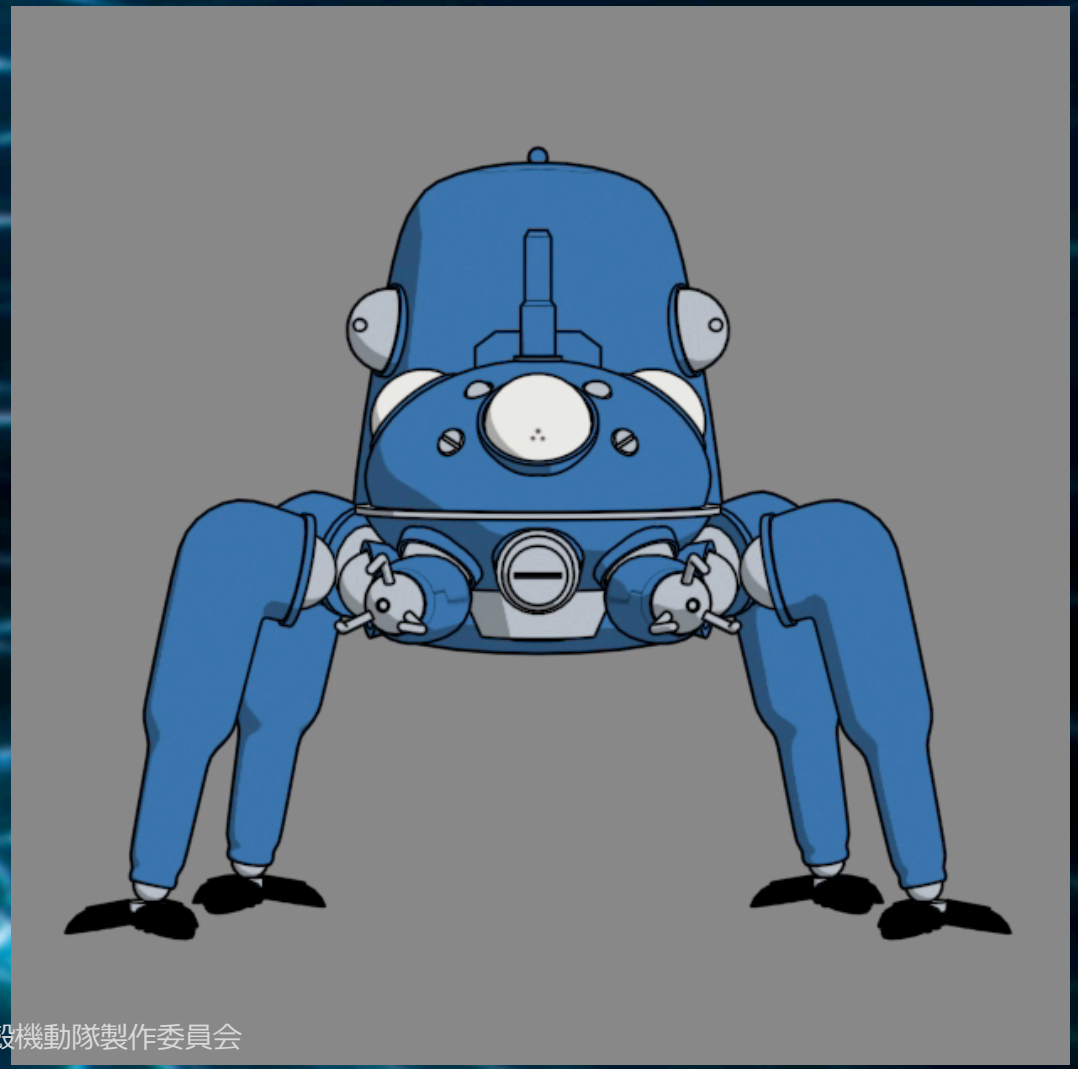
Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

タチコマ

士郎正宗によるSF漫画**「攻殻機動隊」**を原作とし制作されたアニメ「攻殻機動隊S.A.C.」シリーズに登場する自律走行可能な思考戦車。高度な人工知能を搭載しており、操縦者なしでも任務を遂行することができ、電脳空間においては情報収集や電脳戦のサポートを行う。



タチコマ as a ...

1. センサ
2. アクチュエータ
3. コミュニケータ

WarpDrive

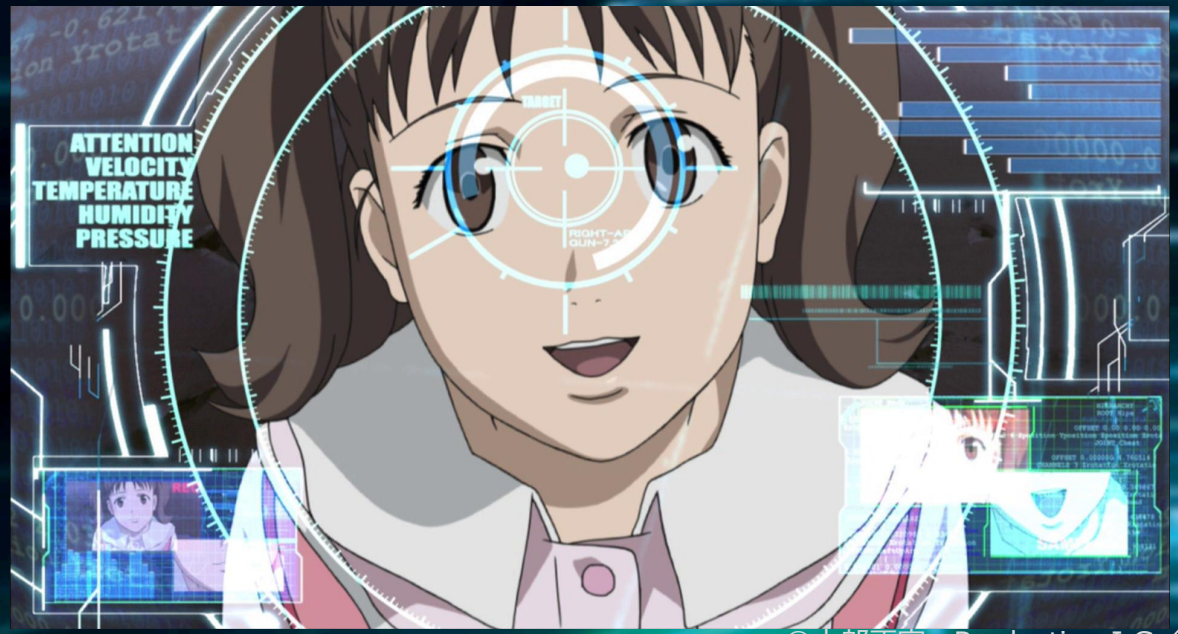
Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(1) ユーザのコンピュータに「タチコマ」をインストール

攻殻機動隊S.A.C.に登場するAI「タチコマ」を電脳空間にリアライズ。
Web媒介型攻撃対策用『タチコマ・セキュリティ・エージェント』を2018年6月1日より無償配布中！



WarpDrive

Web-based Attack Response with Practical and Deployable Research InitiatiVE

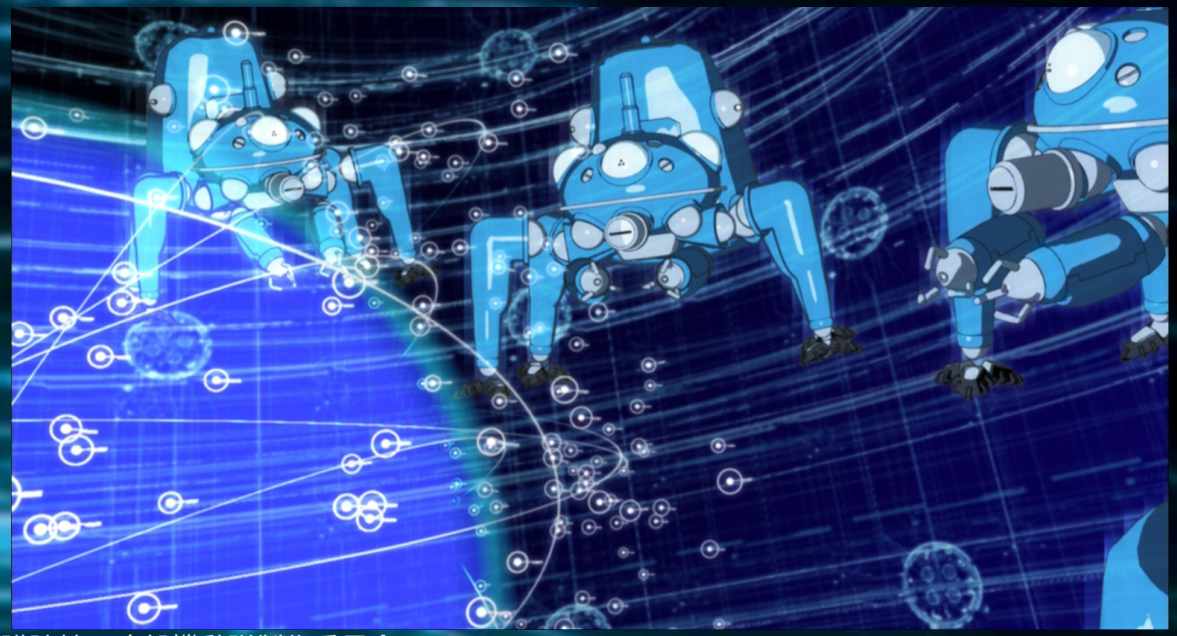
NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(2)「タチコマ」たちが並列化し Web空間を大規模観測

1万人規模のPCにインストールされた「タチコマ」たちがユーザのWebアクセスを大規模観測。

並列化（情報集約、横断分析、新機能展開等）により「タチコマ」が成長！



WarpDrive

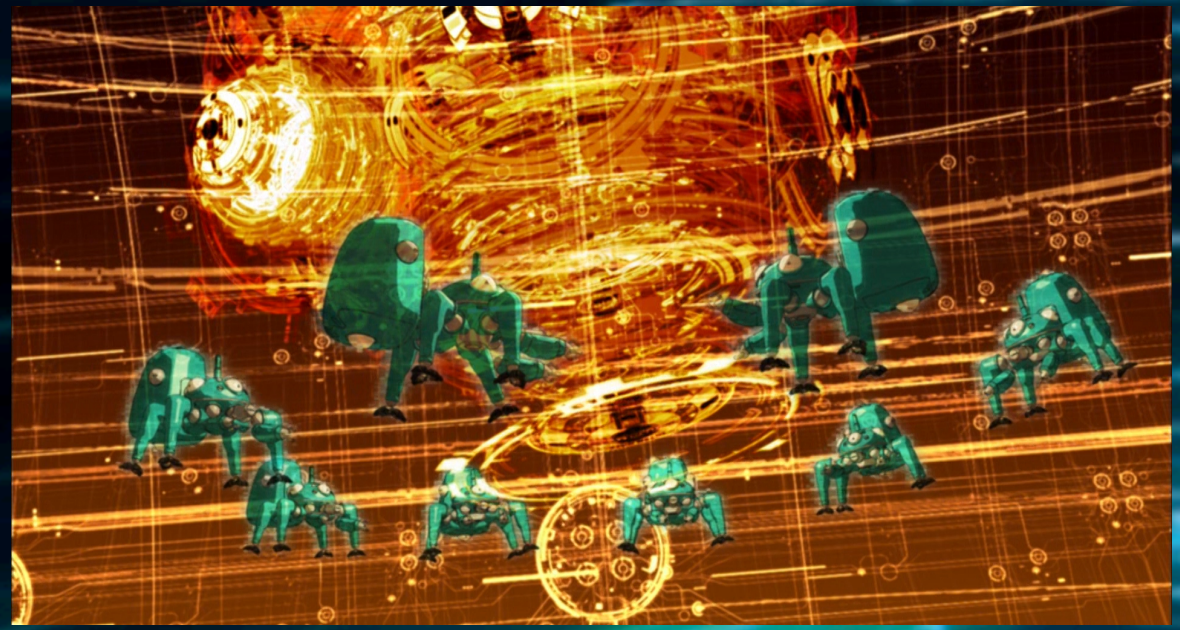
Web-based Attack Response with Practical and Deployable Research InitiatiVE

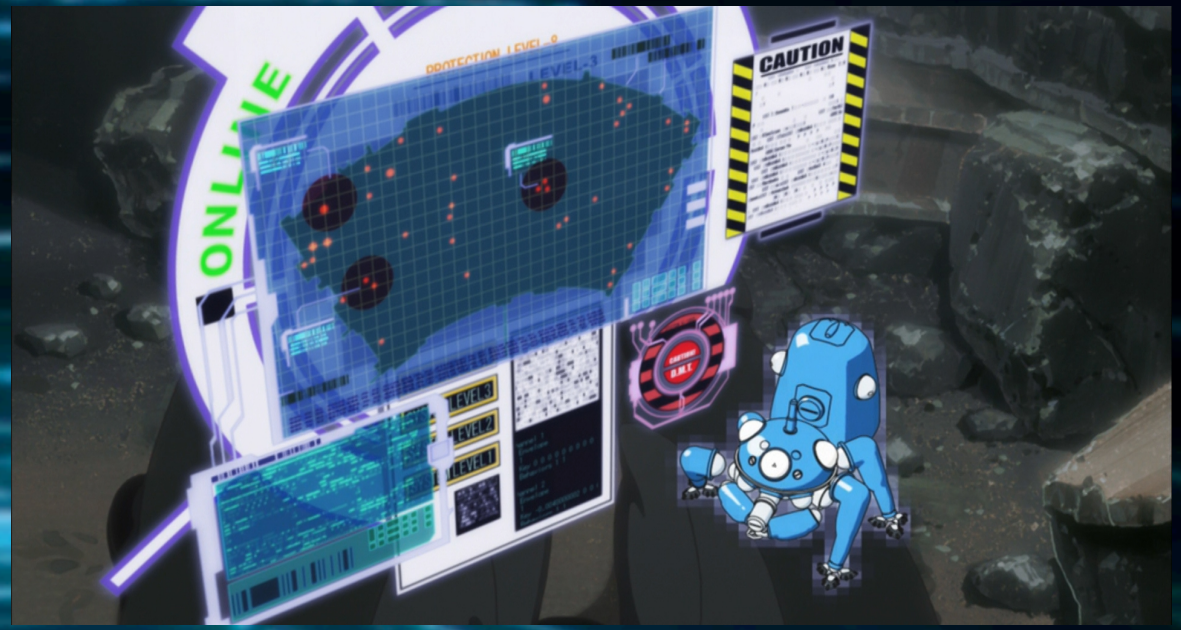
NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(3) 悪性サイト検知時には「タチコマ」が防壁展開 アクセスをブロックしユーザに警告

Web媒介型攻撃検知時には「タチコマ」が防壁展開し、悪性Webサイトへのアクセスをブロック。
「タチコマ」をインターフェイスにしてユーザに警告やアドバイスが届きます！





WarpDrive

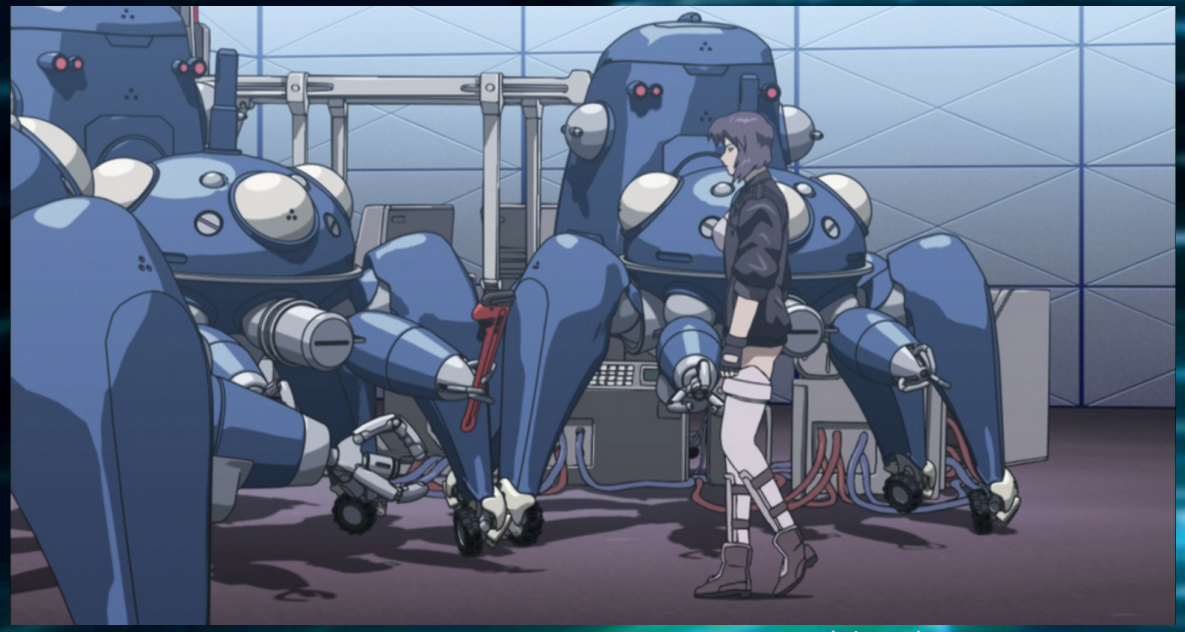
Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(4) スマートフォンやIoT機器にも順次展開

WarpDriveプロジェクトではスマートフォンやIoT機器（ホームルータ、Webカメラ等）にも
セキュリティ対策を順次展開。2020年を目処にサービス化を目指します！

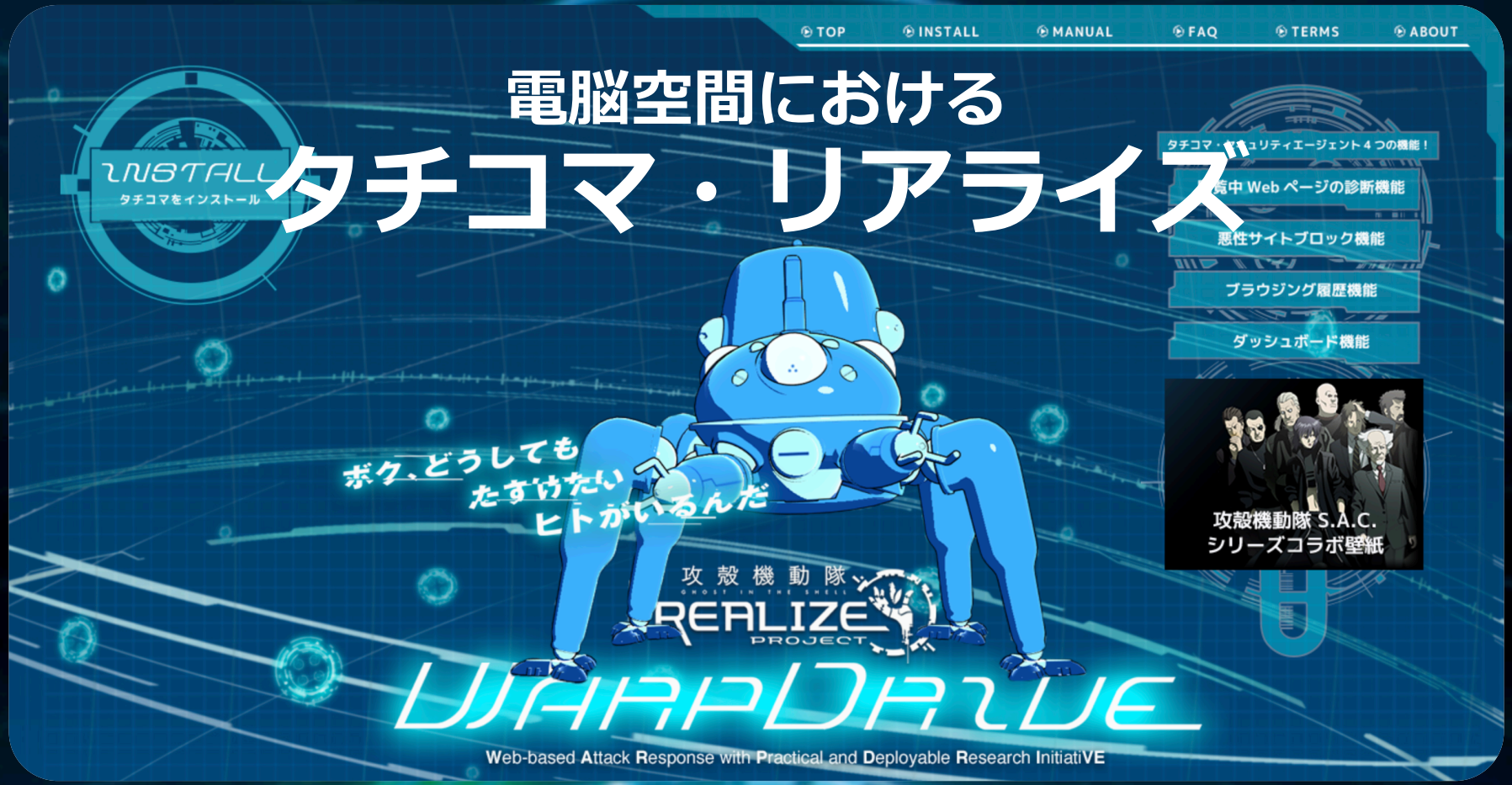


WARPDRIVE

Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学



https://warpdrive-project.jp/