サイバーセキュリティに係る研究開発及び人材育成

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

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

社会を「守る」サイバーセキュリティ分野

サイバーセキュリティ研究室

井上大介 室長

- 研究チーム
  - 大規模データに基づく
  - 世界最先端の学術研究
- 開発チーム
  - 観測基盤から可視化まで
  - インハウスの組織的開発
- 解析チーム
  - 機構内外からの要請に応える
  - 異種データ大規模横断解析

セキュリティ基盤研究室

盛合志帆 室長

- 暗号技術の安全性評価
  - 暗号技術の安全性評価
    - 安心・安全な ICT システムの維持・構築
    - 新たな暗号技術の普及・標準化への貢献
  - 機能性暗号技術
    - 新たな機能を備えた機能性暗号や軽量暗号・認証技術の研究開発
- プライバシー保護技術
  - プライバシー保護技術
    - パーソナルデータの利活用に貢献するプライバシー保護技術の研究開発

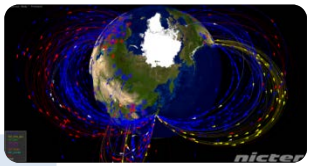
NICT National Institute of Information and Communications Technology
NICTER Network Incident analysis Center for Tactical Emergency Response

NICTERとスピンオフ技術

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

サイバー攻撃統合分析プラットフォーム

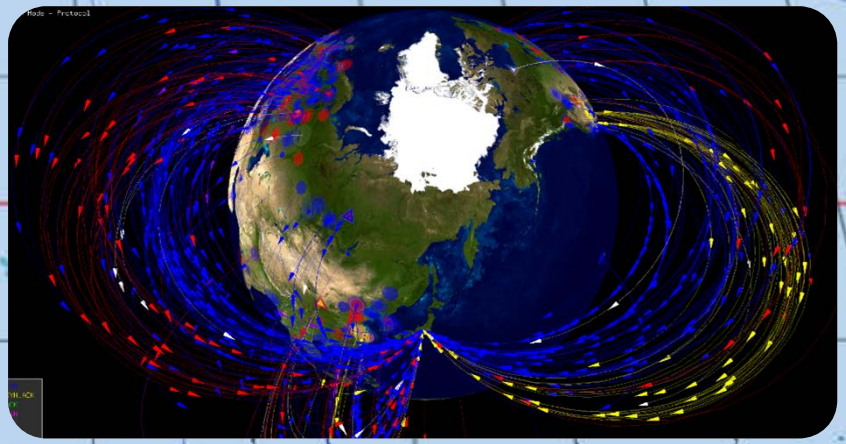
NIRVANA改

標的型攻撃対策

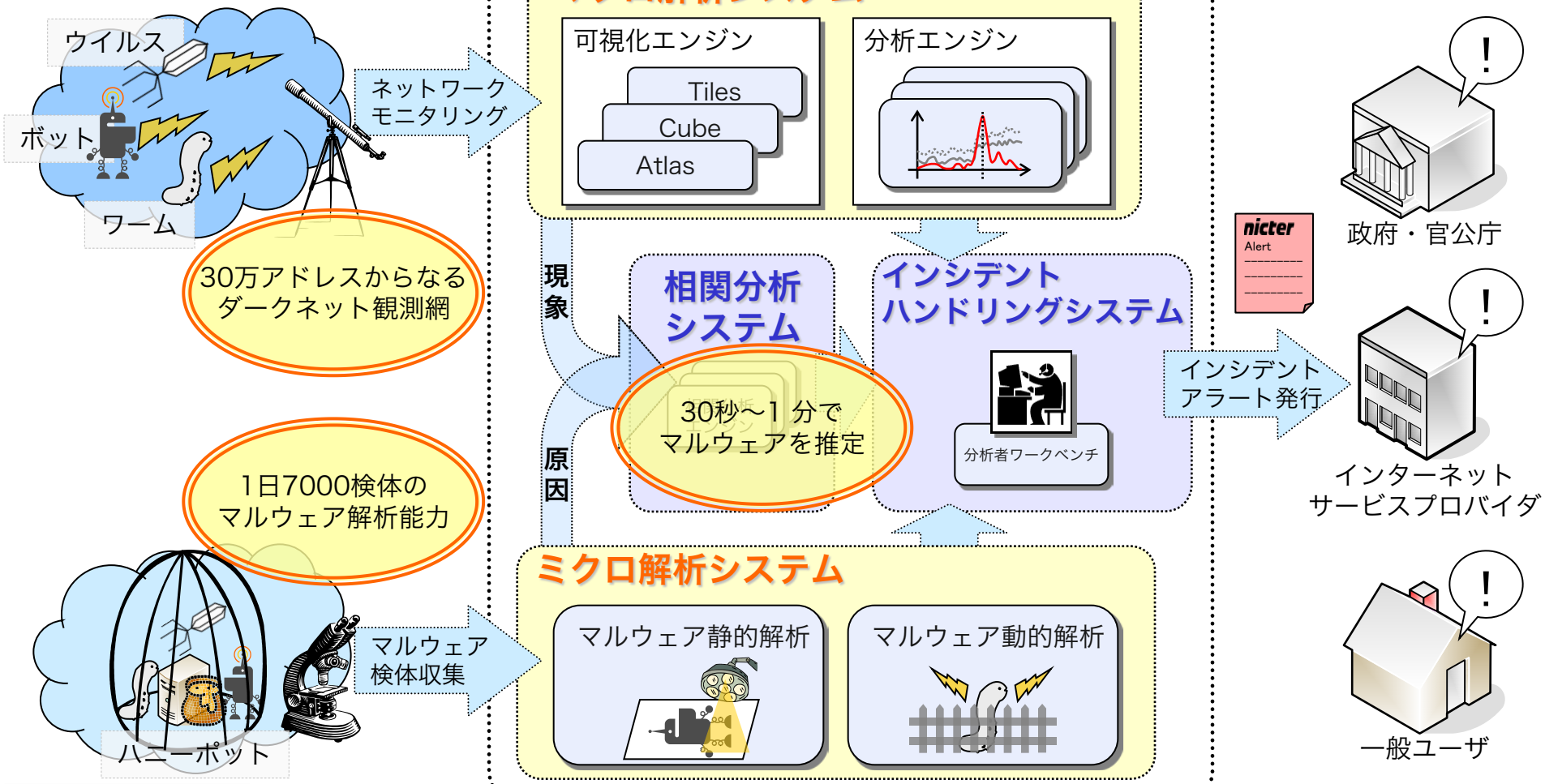
213,523

1つのIPアドレス（インターネット上の住所）に対して
2015年の1年間で届いた無差別型攻撃に関する通信の数

NICTER



NICTERの全体像

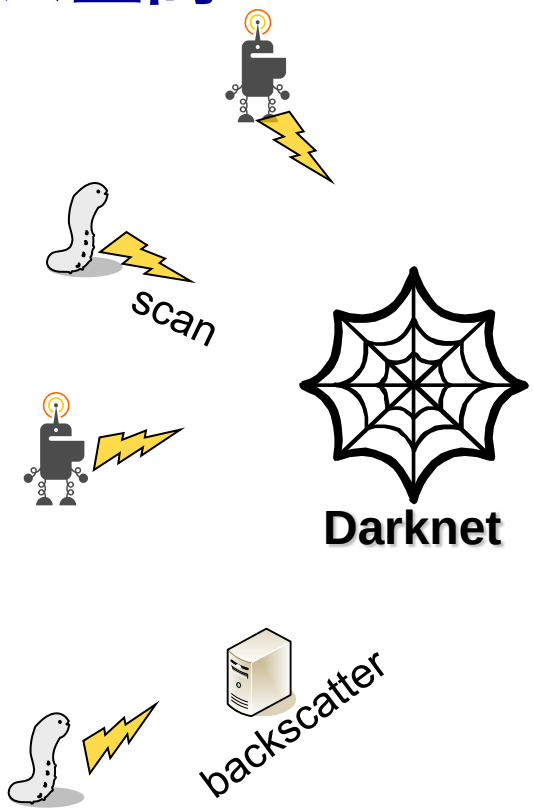


NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

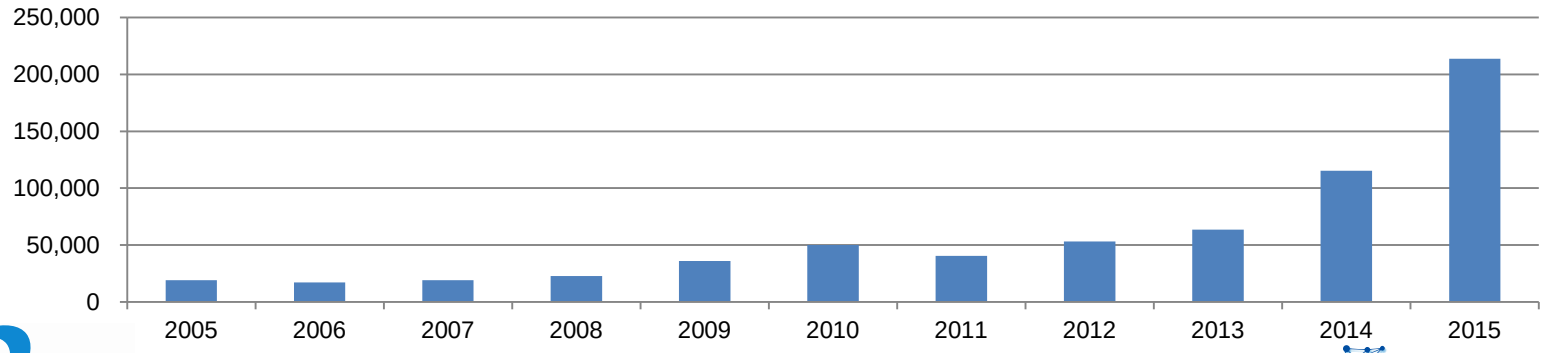
ダークネット観測とは？

- **ダークネット：未使用のIPアドレス空間**
  - ✓正常な通信は “基本的に” 届かない
- **実際は大量の通信が届く**
  - ✓ マルウェアによるスキャン
  - ✓ DDoS攻撃の跳ね返り
  - ✓ リフレクション攻撃の準備活動
  - ✓ etc.
- **ダークネットの観測によって パンデミックの兆候が分かる**
  - ✓ パンデミック：マルウェアの大量感染



NICTERダークネット観測統計

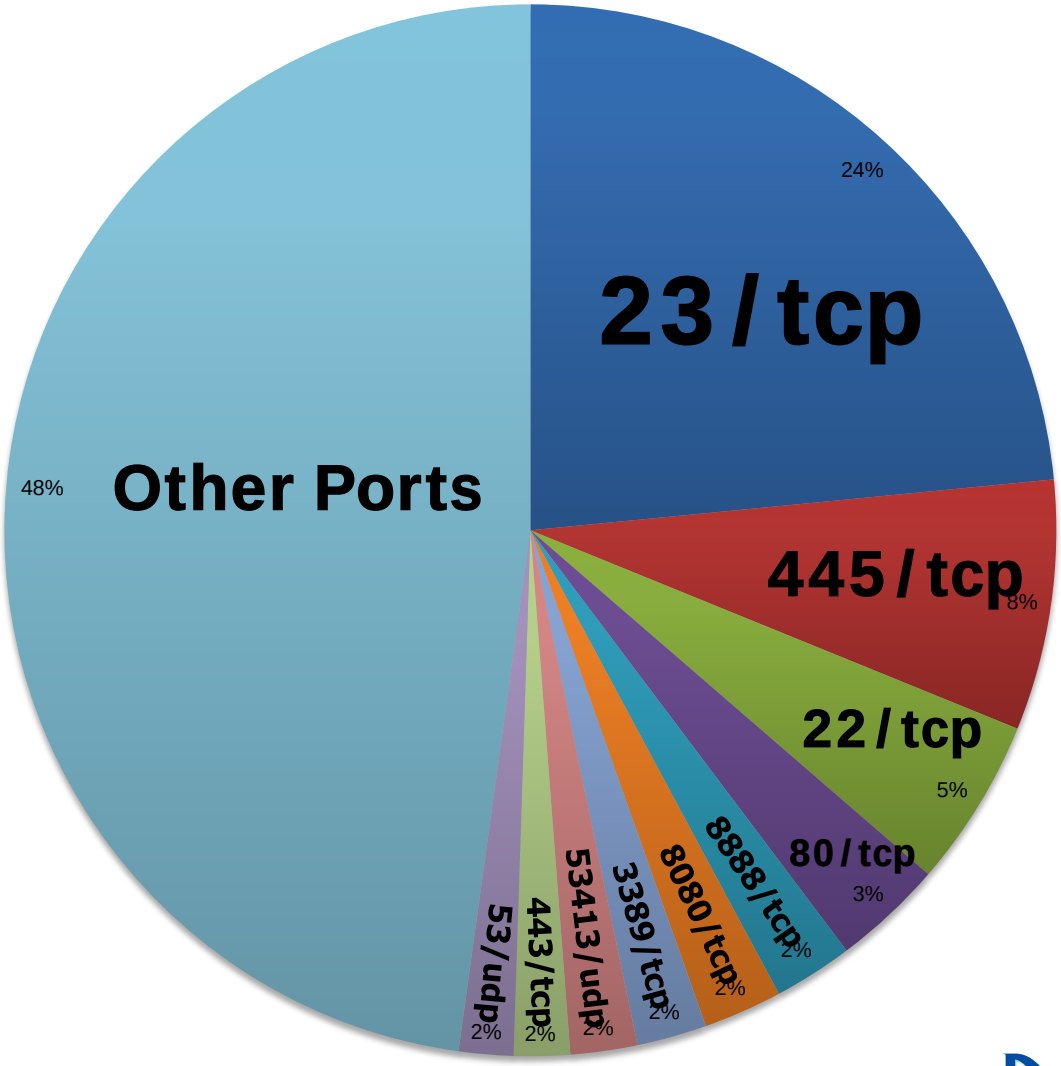
年	年間 総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの 年間総観測パケット数
2005	約3.1億	約1.6万	19,066
2006	約8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	**213,523**



1 IPアドレス当たりの年間総観測パケット数

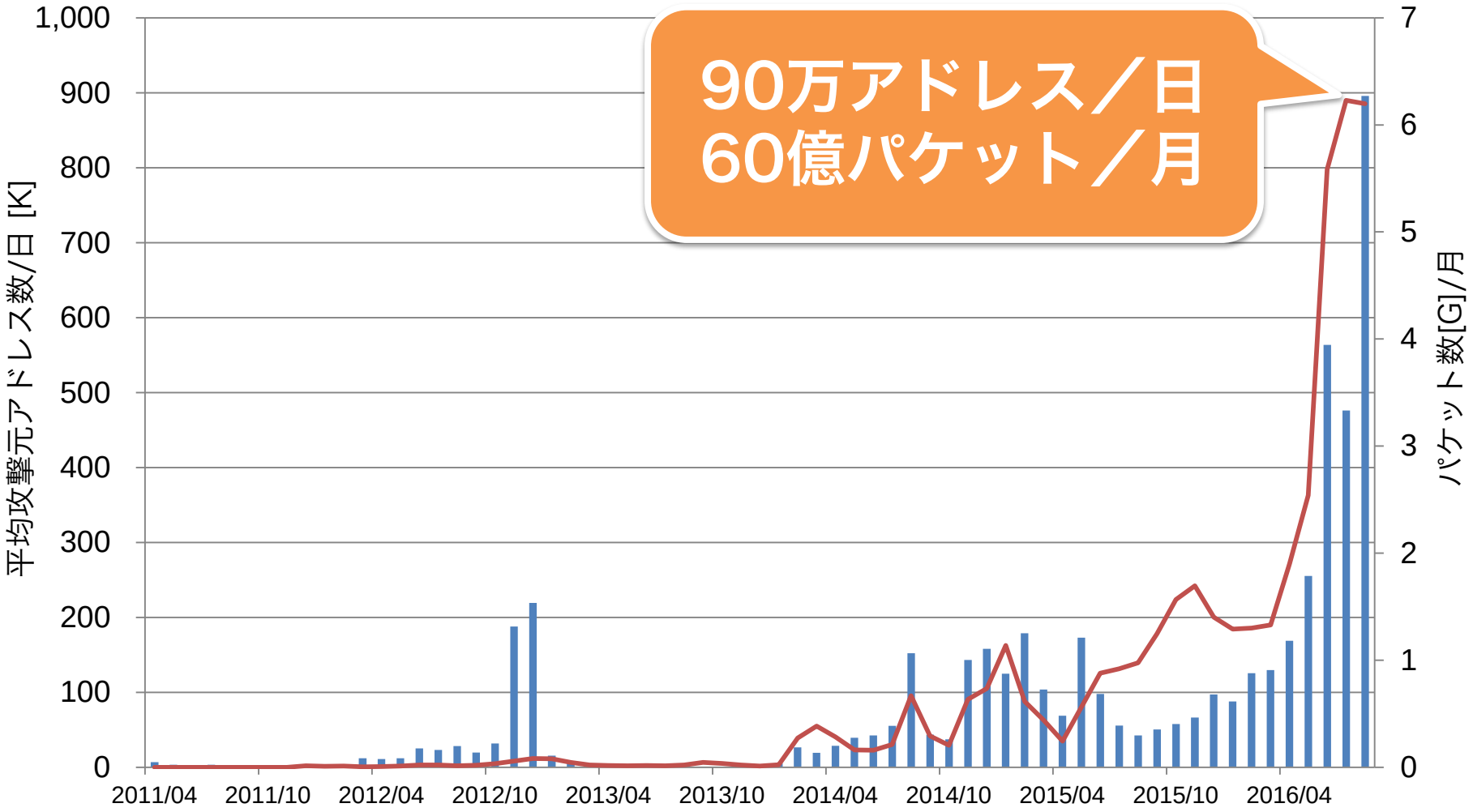
NICT National Institute of Information and Communications Technology
NICTER Network Incident analysis Center for Tactical Emergency Response

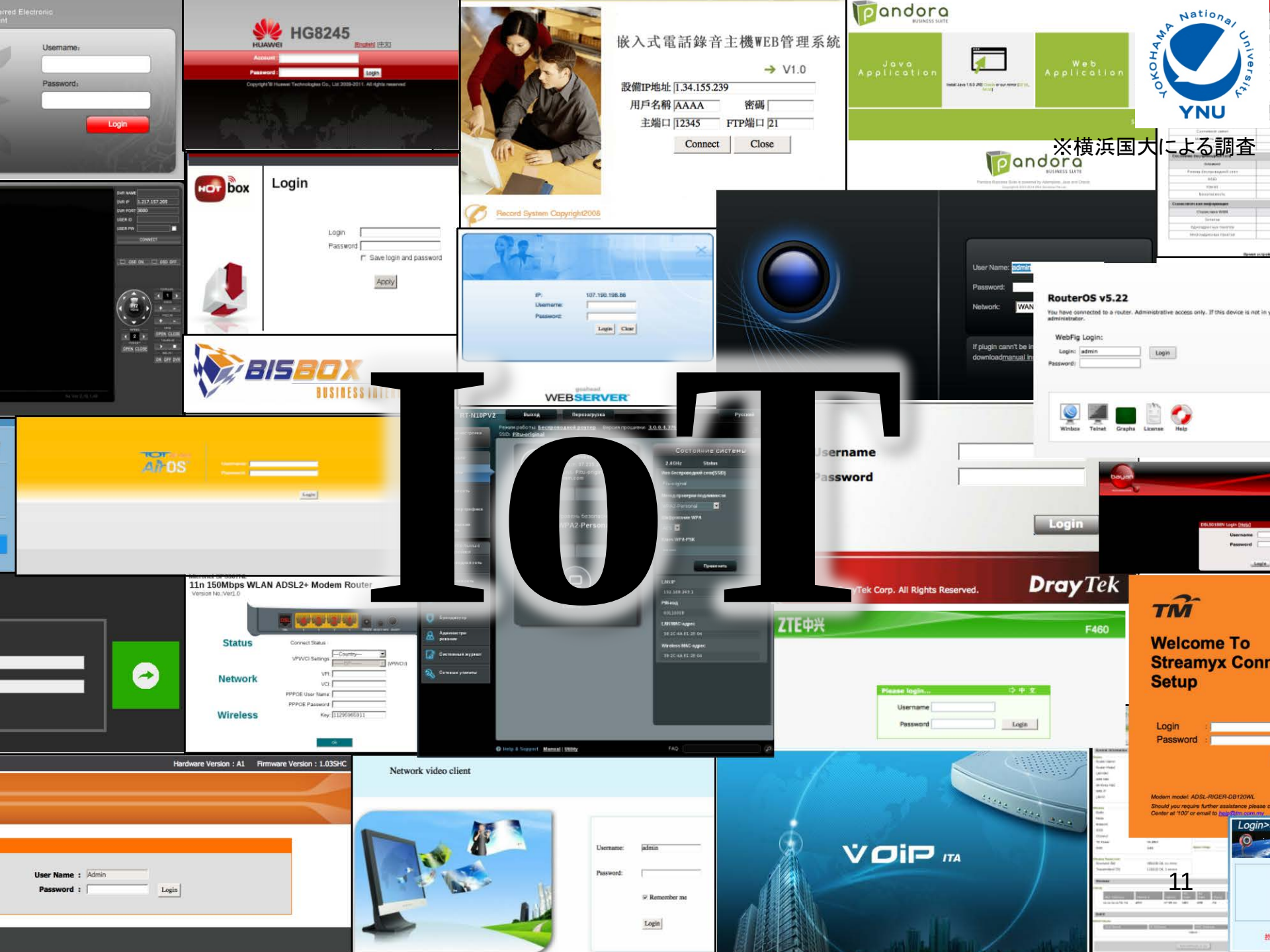
宛先ポート番号別パケット数 (2015年)



National Institute of Information and Communications Technology
NICTER
Network Incident analysis Center for Tactical Emergency Response

NICTER 観測結果(23/TCP)




IoT
※横浜国大による調査

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

IoT機器を悪用した大規模DDoS攻撃

10月21日に米DNS事業者であるDynに対して
大規模なDDoS攻撃が発生
AmazonやTwitterなど多数のサイトに影響

攻撃者はマルウェア“Mirai” を感染させた
Webカメラ等のIoT機器を悪用して攻撃を行った

Dyn confirms Mirai botnet involved in distributed denial of service attack

The attack, which knocked out popular sites last week, came in two waves. Dyn outlined its initial analysis.

National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

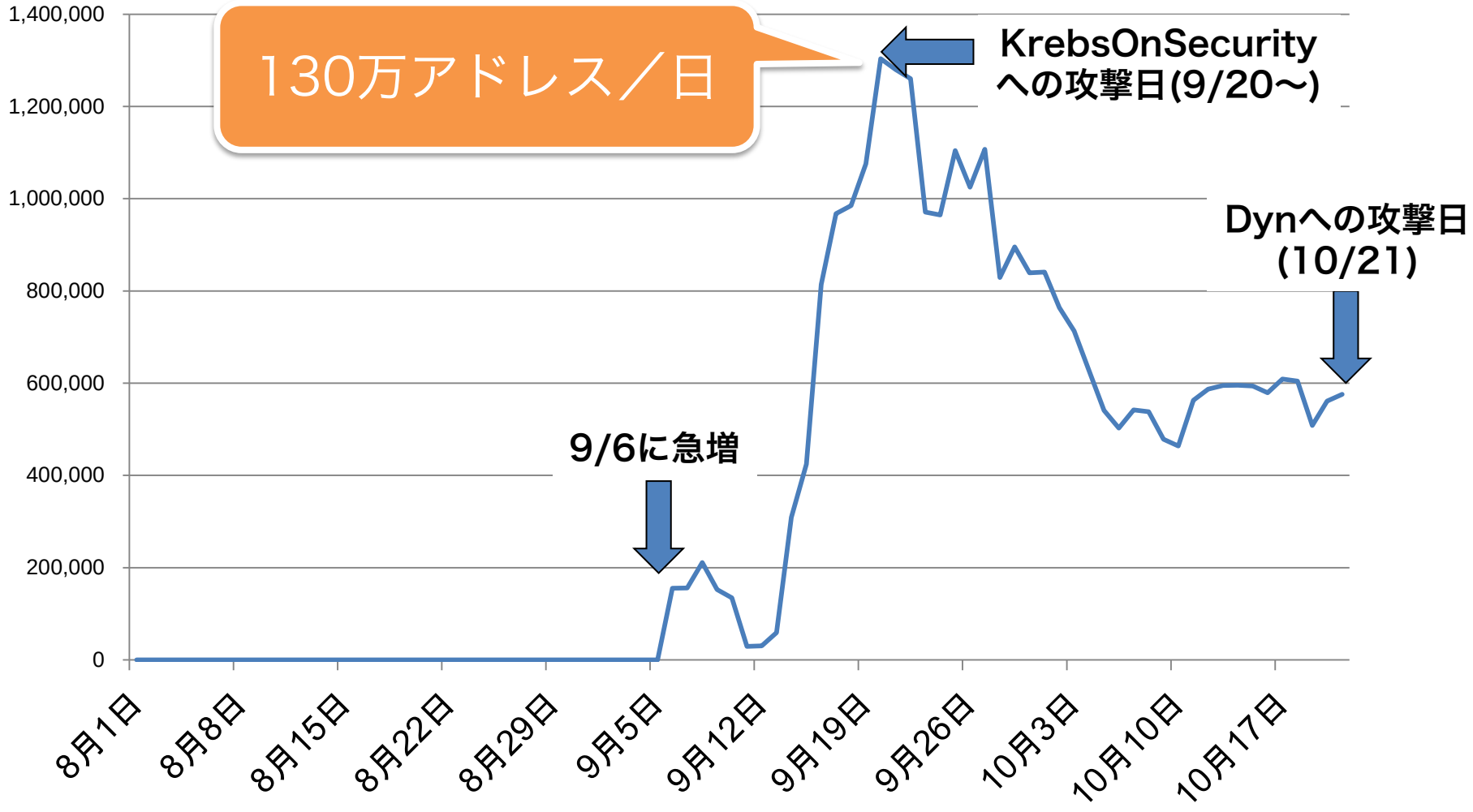
Mirai

- Telnet（23/TCP, **2323/TCP**）でアクセス
- よくあるIDとパスワードの組み合わせで侵入
- KrebsOnSecurityへのDDoSに利用（620 Gbps!!）
- 作者がソースコードを公開

```
123     // Set up passwords
124     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
125     add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
126     add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
127     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
128     add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
129     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root     xmhdipc
130     add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root     default
131     add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root     juantech
132     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
133     add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
134     add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
135     add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
```


NICT National Institute of Information and Communications Technology
NICTER Network Incident analysis Center for Tactical Emergency Response

NICTER 観測結果(2323/TCP)

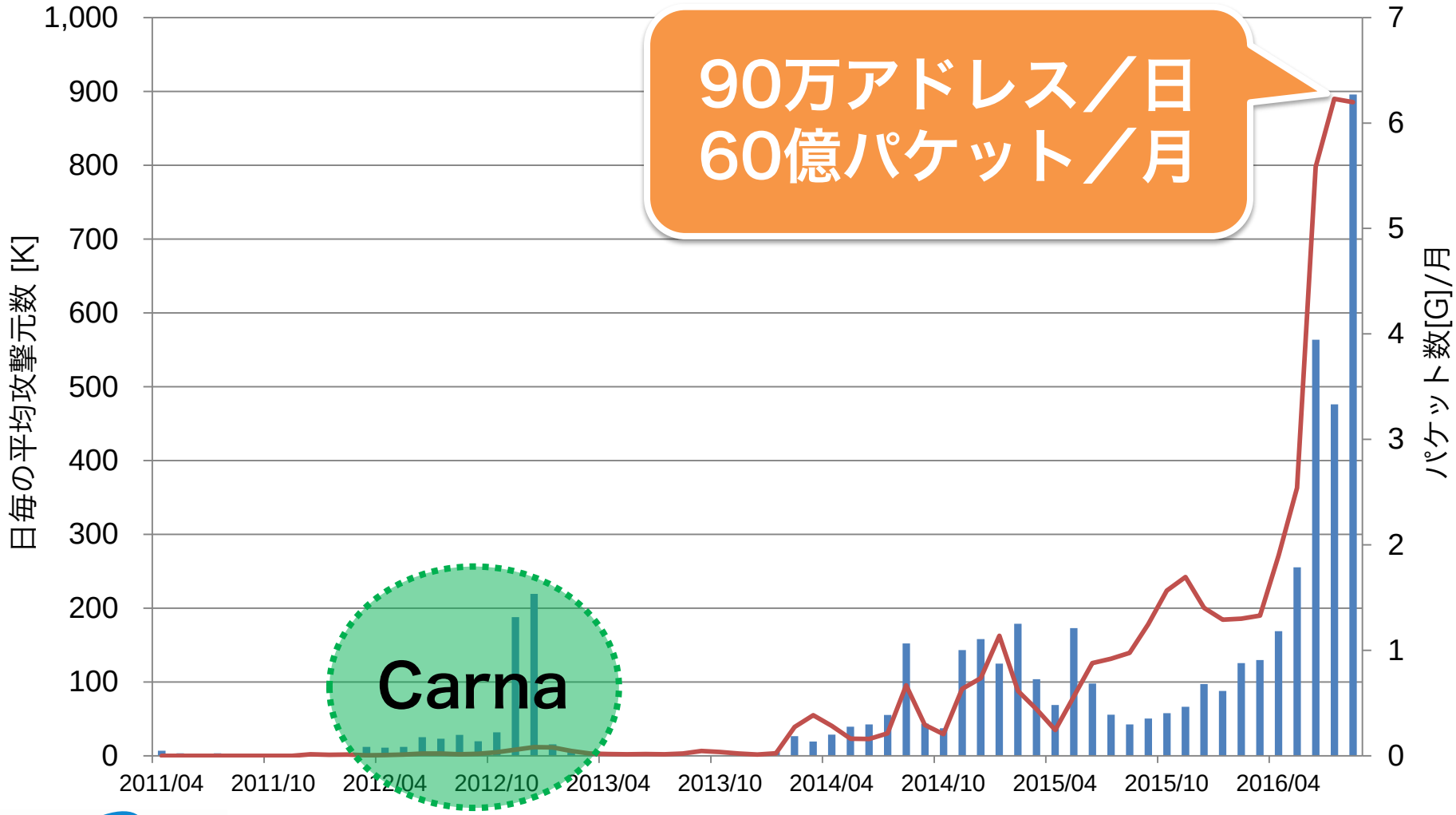


NICT National Institute of Information and Communications Technology
NICTER Network Incident analysis Center for Tactical Emergency Response

2012年には既にIoT機器の大量感染が

- **Carnaボットネット**
  - Telnet経由で**42万台以上**のIoT機器に侵入
  - 侵入したIoT機器を使って**インターネット全域にスキャン**を実施
  - スキャン結果を2012年にWeb＋Bittorrentで公開
- **Linux.Moose**
  - Telnet経由で**世界中のIoT機器**に侵入 (主にルータを狙う)
  - **プロキシ，盗聴，DNS改ざん，SNS悪用**など多くの機能を持つ
  - ESETが2015年5月に解析レポートを公開
- **Linux.Wifatch**
  - Telnet経由で感染拡大．**P2P**によって攻撃者からの指令を受信
  - 侵入した機器の**Telnetを停止**し，**他のマルウェアの削除**を行う
  - 2015年10月にSymantecが報告．作者がgithubでソース公開

NICTER 観測結果(23/TCP)



NICT National Institute of Information and Communications Technology
NICTER Network Incident analysis Center for Tactical Emergency Response

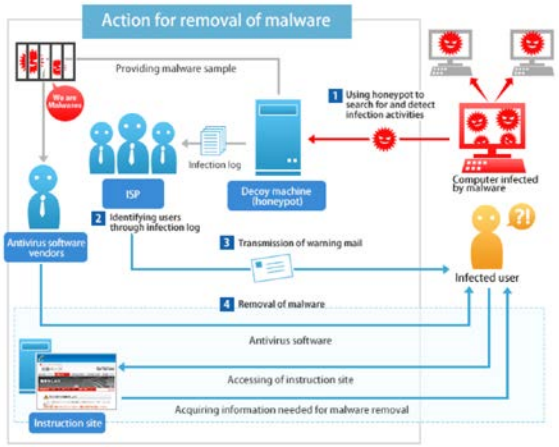
ダークネット観測結果の共有・提供

- **SIGMON**（定点観測友の会）
  - ✓ 参画組織：JPCERT/CC、IPA、@Police、NICT、国内大学等
  - ✓ ダークネット観測結果を情報共有（2004年～）

- **DOS攻撃即応-WG**（Telecom-ISAC Japan）
  - ✓ 国内ISPによるDoS攻撃への迅速な対応と協調対処
  - ✓ Backscatter＋DRDoS攻撃情報を共有（2011年～）

- **ACTIVE**（総務省）
  - ✓ 『国民のマルウェア対策支援プロジェクト』
  - ✓ 感染ユーザのIPアドレスを提供（2014年～）

- **オリパラCSIRT**（NISC 他）
  - ✓ オリパラ関連組織との情報共有体制構築（2015年～）



ACTIVE（www.active.go.jp）

NICT National Institute of Information and Communications Technology
NICTER Network Incident analysis Center for Tactical Emergency Response

GOOD DESIGN AWARD 2013

対サイバー攻撃アラートシステム

DAEDALUS

Direct **A**lert **E**nvironment for

Darknet **A**nd **L**ivenet **U**nified **S**ecurity

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

基本アイデア

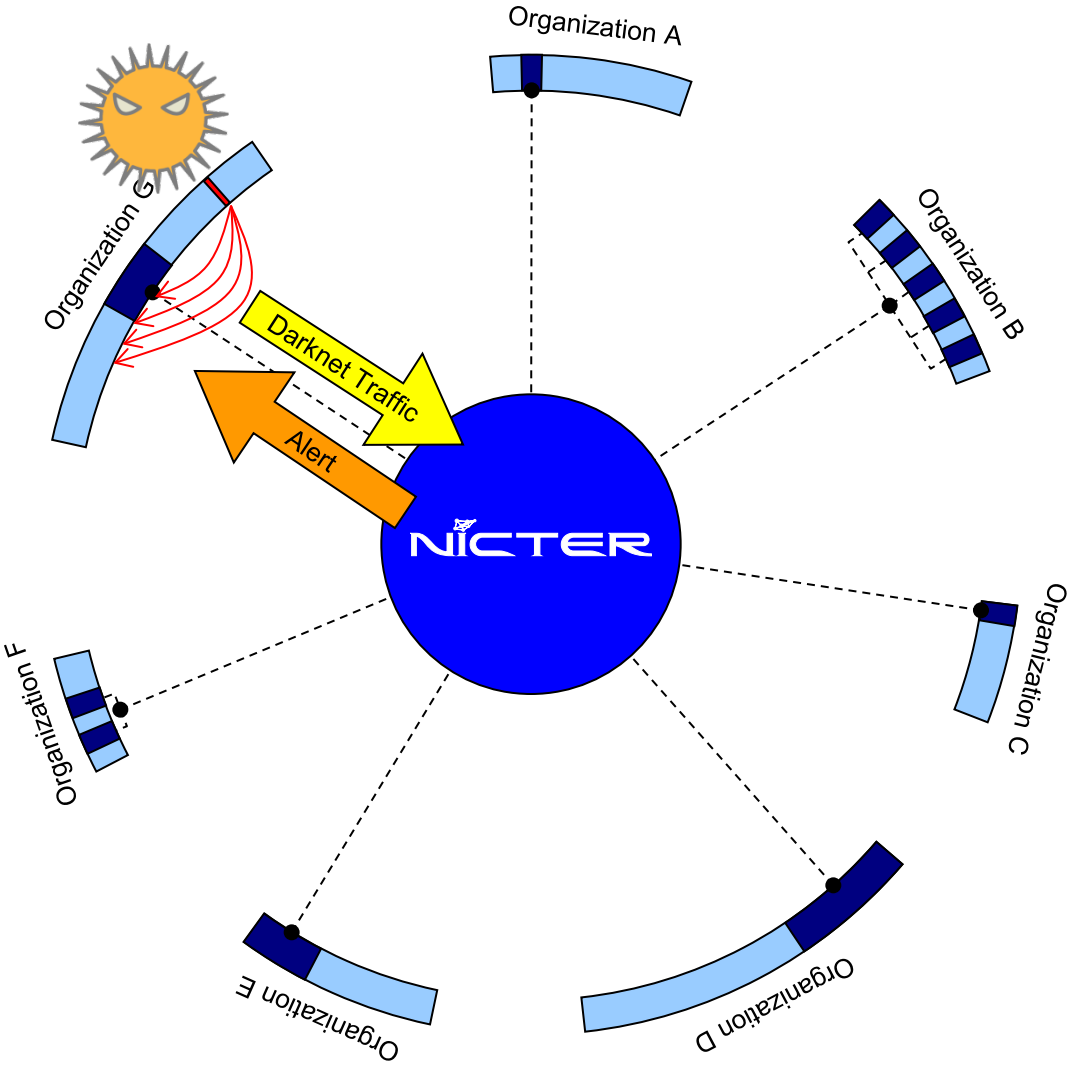
登録されたIPアドレスから

ダークネットにパケットが飛んできたら

アラート。

ケース1

組織内感染（内部アラート）

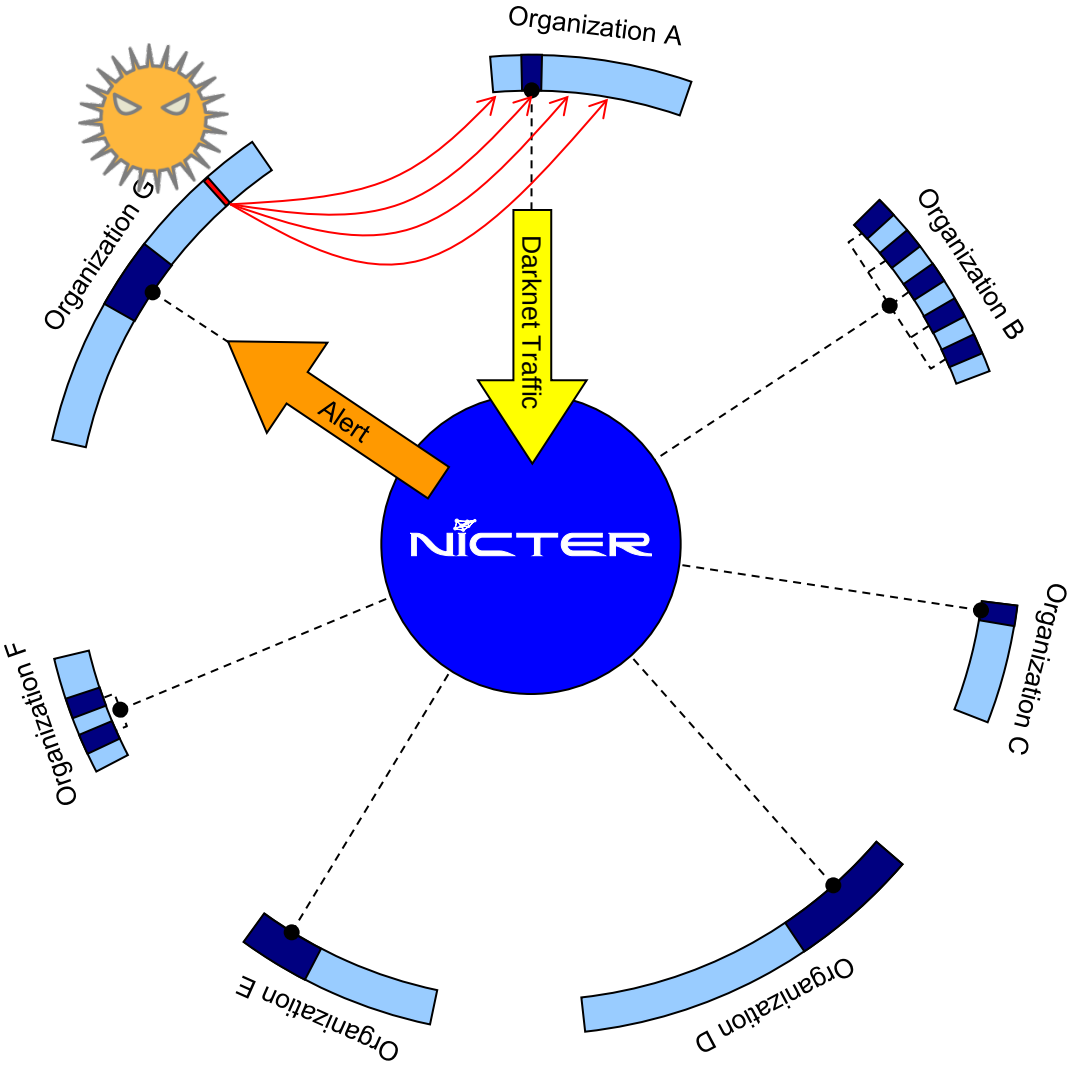


National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

ケース2

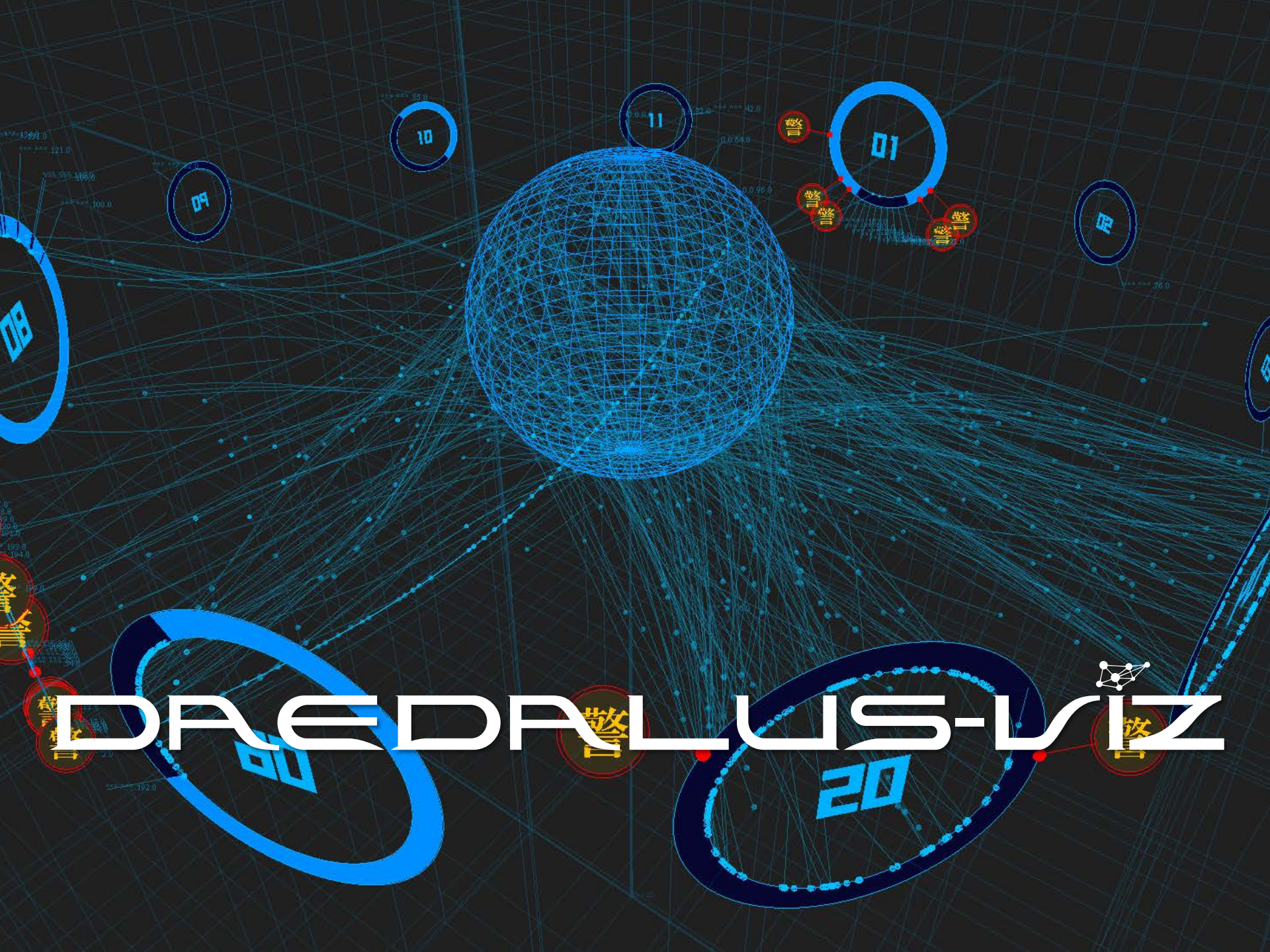
組織外への攻撃（外部アラート）



: Livenet
: Darknet
: Infected Host

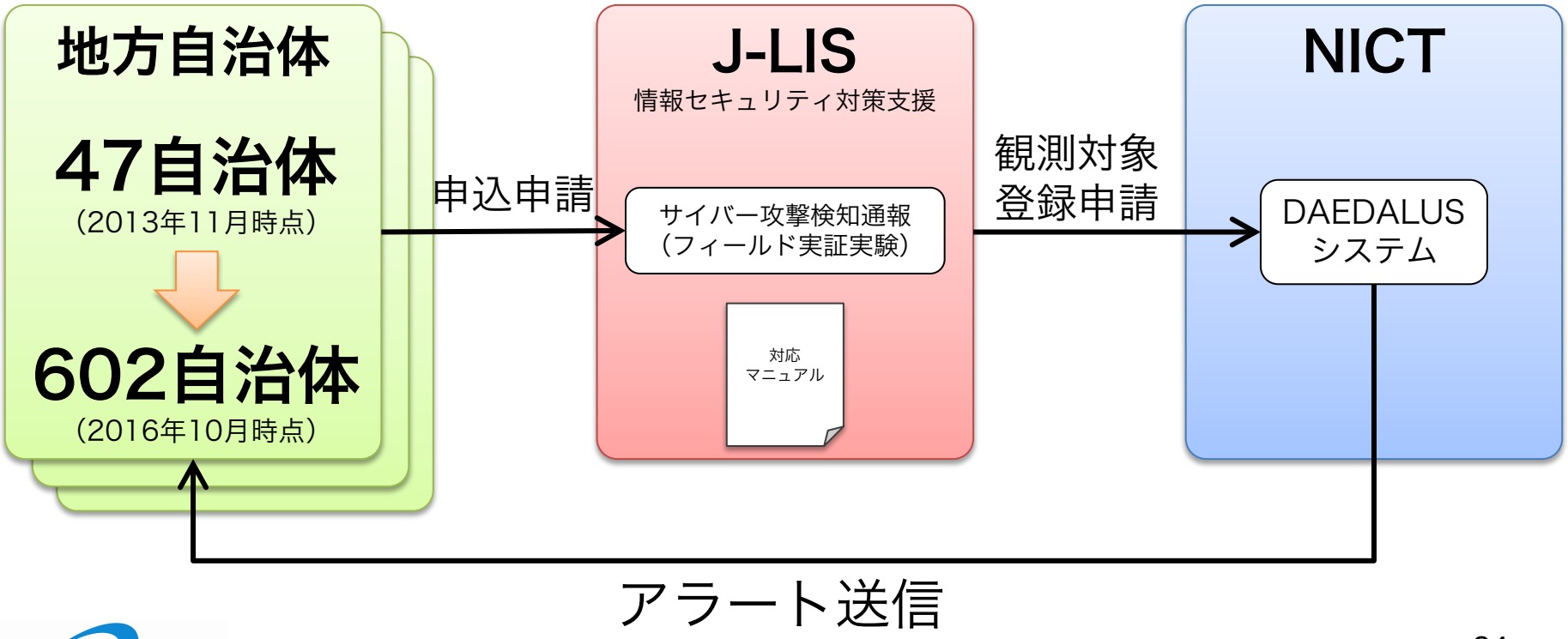
National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response


DAEDALUS-VIZ

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



セキュリティ人材育成への貢献

- **CYDER（実践的サイバー防御演習）**
  演習ネットワーク環境提供（北陸StarBED³）
- **MWS（マルウェア対策研究人材育成ワークショップ）**
  研究データセット提供（ダークネット観測情報）
- **セキュリティ競技大会SECCON**
  可視化技術提供（NIRVANA改 SECCONカスタム Mk-II）
- **攻殻CTF（女性限定サイバー模擬攻防戦）**
  可視化技術提供（AMATERAS零）
- **大学からの研修生受け入れ　etc.**

CYDER（実践的サイバー防御演習）

SECCON 全国大会カンファレンス

攻殻CTF（AMATERAS零）

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法の一部改正

第三章　業務等

（業務の範囲）

第十四条　機構は、第四条の目的を達成するため、次の業務を行う。

一　情報の電磁的流通及び電波の利用に関する技術の調査、研究及び開発を行うこと。

二　宇宙の開発に関する大規模な技術開発であって、情報の電磁的流通及び電波の利用に係るものを行うこと。

三　周波数標準値を設定し、標準電波を発射し、及び標準時を通報すること。

四　電波の伝わり方について、観測を行い、予報及び異常に関する警報を送信し、並びにその他の通報をすること。

五　無線設備（高周波利用設備を含む。）の機器の試験及び較正を行うこと。

六　前三号に掲げる業務に関連して必要な技術の調査、研究及び開発を行うこと。

七　第一号に掲げる業務に係る成果の普及としてサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条 に規定するサイバーセキュリティをいう。）に関する演習その他の訓練を行うこと。

八　前号に掲げるもののほか、第一号、第二号及び第六号に掲げる業務に係る成果の普及を行うこと。

「サイバーセキュリティに関する演習その他の訓練を行うこと」がNICTの業務として規定

「セキュリティ人財育成研究センター」の立ち上げ

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

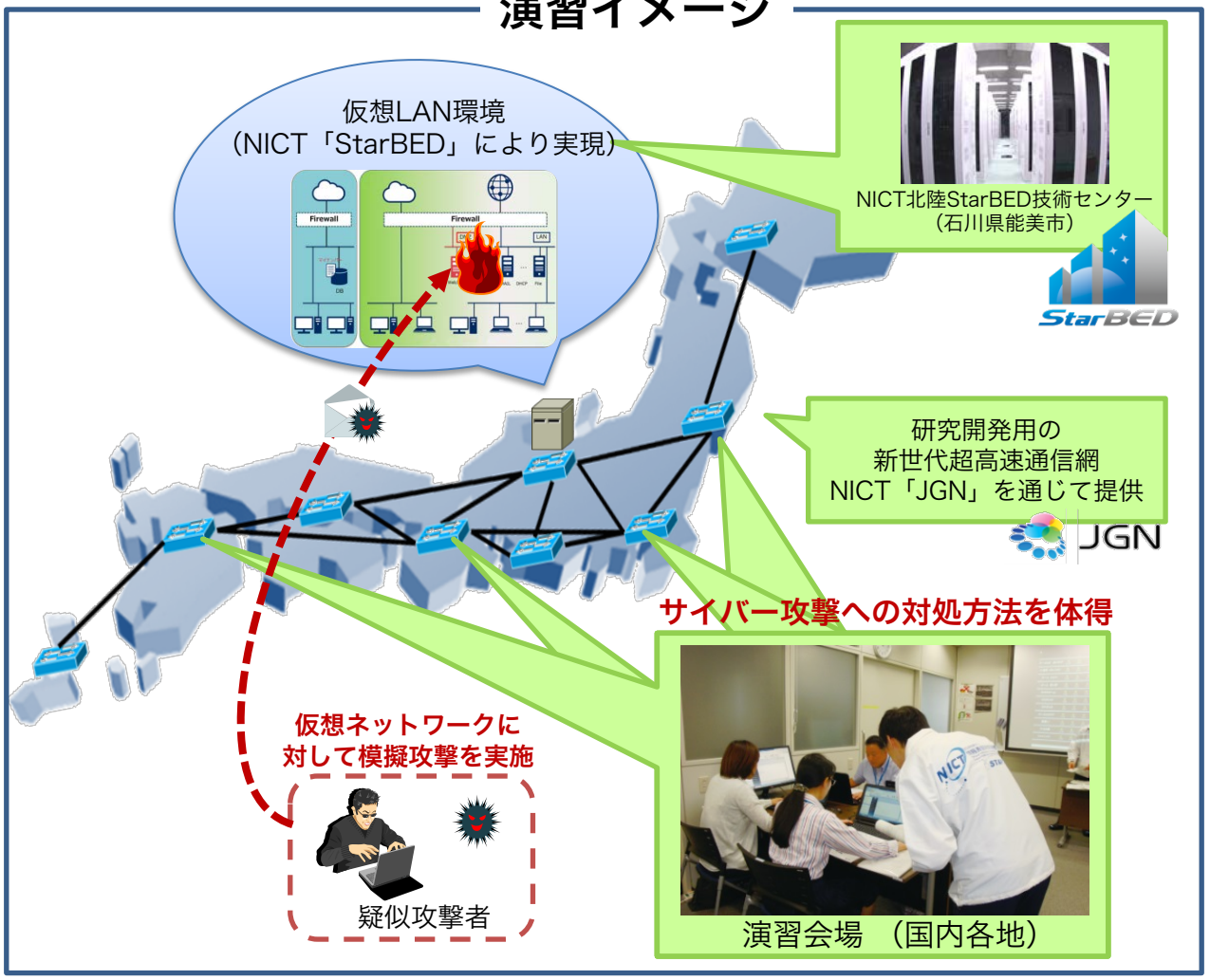
実践的サイバー防御演習（CYDER）

実践的サイバー防御演習（CYDER）の開発・実施

(CYDER：CYber Defense Exercise with Recurrence)

政府のサイバーセキュリティ戦略及び情報通信研究機構法改正に基づき、国の行政機関、地方公共団体等を対象として、NICTが有するサイバーセキュリティの技術的知見及び大規模計算機環境を最大限に活かしたサイバー防御演習を開発・実施

演習イメージ



演習の概要

- ✓ 受講者は組織の情報システム担当職員として演習に参加し、組織の LAN 環境を模擬した環境で標的型攻撃によるインシデントの検知から対応、回復まで一連の流れを体験しながら学ぶ。

演習の特徴

- ✓ NICT 北陸 StarBED 技術センターに設置された大規模高性能サーバ群を活用し、仮想ネットワーク環境として演習環境を構築
- ✓ NICT における長年にわたるサイバーセキュリティ研究で得られた技術的知見を活用
- ✓ 我が国固有のサイバー攻撃事例を徹底分析し、 最新の演習シナリオを用意

■対象組織
サイバーセキュリティ基本法に規定される国の行政機関、地方公共団体、独立行政法人、重要社会基盤事業者等

■参加人数
1,200 人以上に実施予定

■演習会場
全国の総合通信局・事務所が管轄する 11 地域