NICTERプロジェクトの10年を振り返る

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

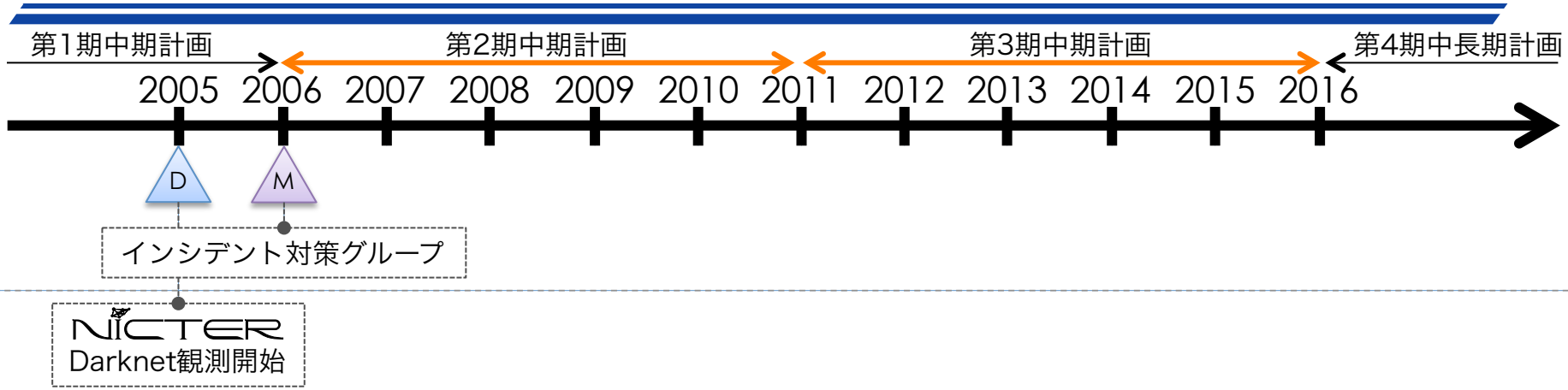
本講演のあらまし

NICTERプロジェクトの約10年の歴史を、
プロジェクトを支え・育て・叱咤激励してくださった

「7つの言葉」

とともに振り返ります。

NICTERプロジェクト 10年線表



Darknet

Livenet

CTF

NICTERプロジェクト加入

2006年4月 インシデント対策グループ

松島 祐一 理事
現 早稲田大学教授

中尾 康二 グループリーダー
現 KDDI顧問 / NICT主管研究員

井上 大介 研究員
現 NICT サイバーセキュリティ研究室
室長

衛藤 将史 研究員
現 NICT セキュリティ人材育成研究センター
研究マネージャー

吉岡 克成 研究員
現 横浜国立大学
准教授

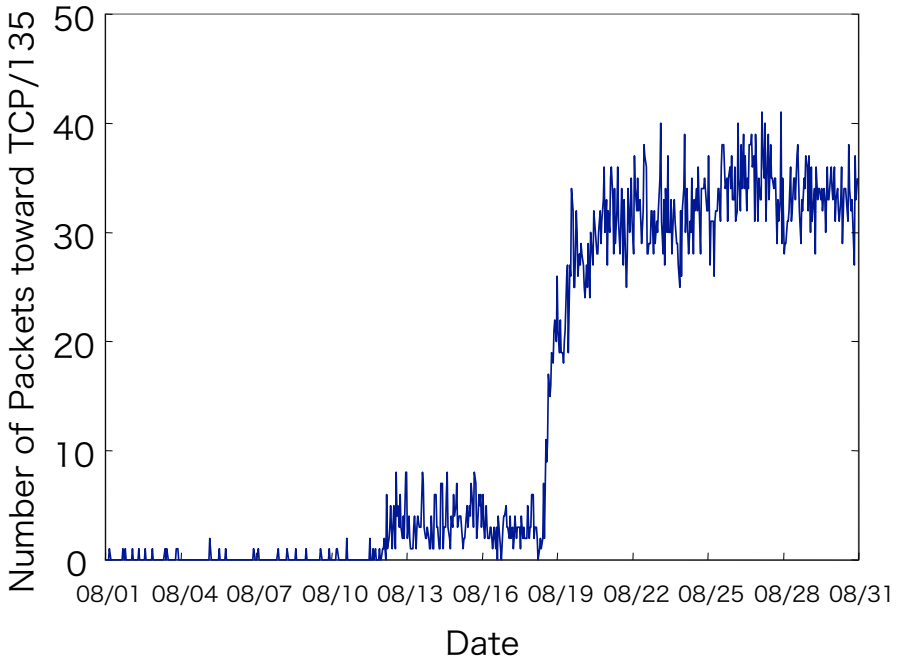
NICTERプロジェクトを育てた言葉 ①

親はなくとも子は育つ。

2003年 Blasterショック

- **2003年8月 MSBlasterのパンデミック**
  - ✓ Windowsのリモート・プロシージャ・コール（RPC）の脆弱性を攻撃
  - ✓ 過去最大規模の感染（後のMicrosoftの発表では最低でも800万台）

- **大規模感染を把握する仕組みが必要！**
  - ✓ Network Telescope（米 CAIDA）
  - ✓ Internet Motion Sensor（米 ミシガン大）
  - ✓ ISDAS、TSUBAME（JPCERT/CC）
  - ✓ インターネット定点観測（@Police）
  - ✓ TALOT2、MUSTAN（IPA）
  - ✓ WCLSCAN（鈴木裕信さん+MRI）
  - ✓ 京大ハニーポット（高倉先生）
  - ✓ NICTER（NICT） etc...

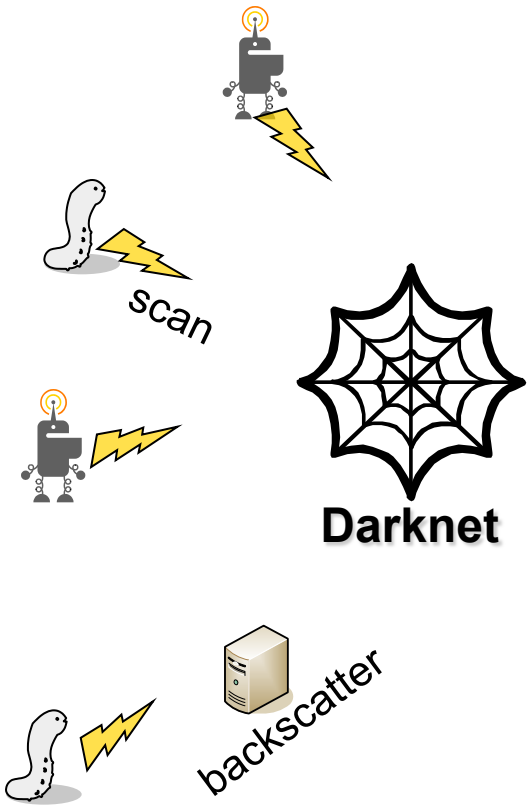


National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

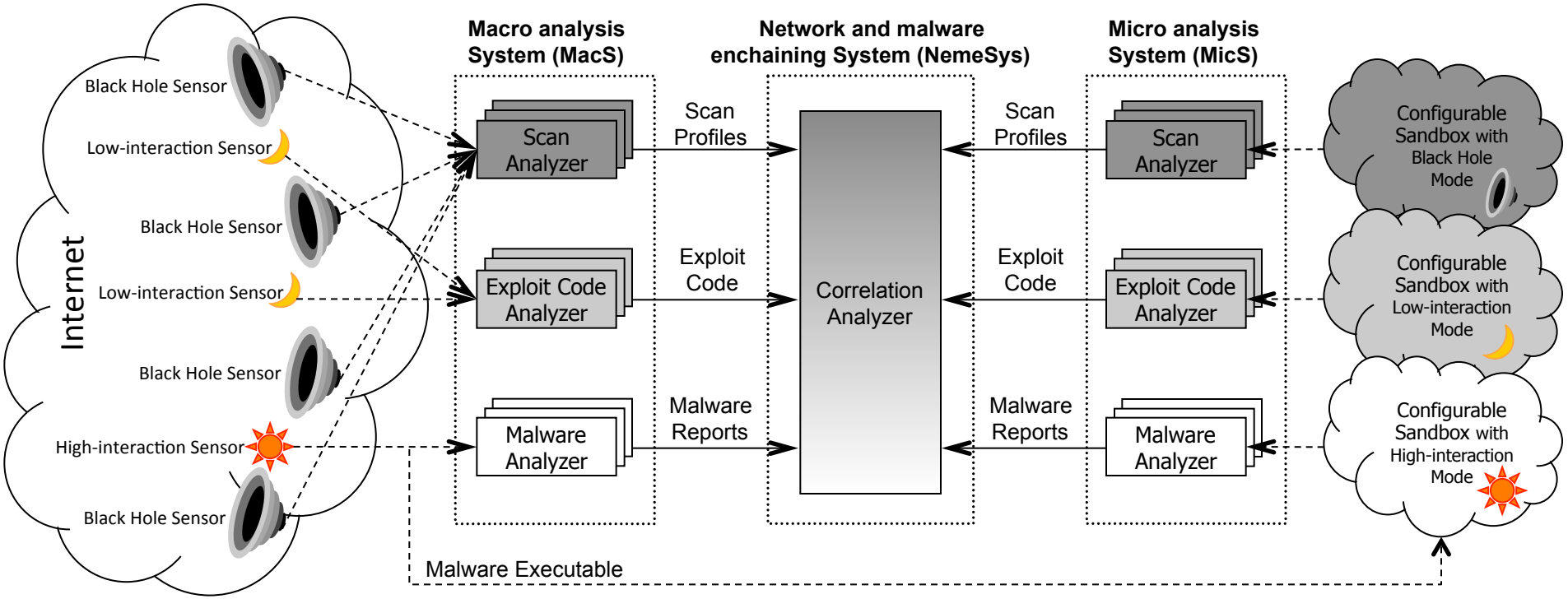
ダークネットで見えるもの（2005年頃）

- **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
- **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
- **設定ミス**



NICTERのコンセプト[1] (2007)

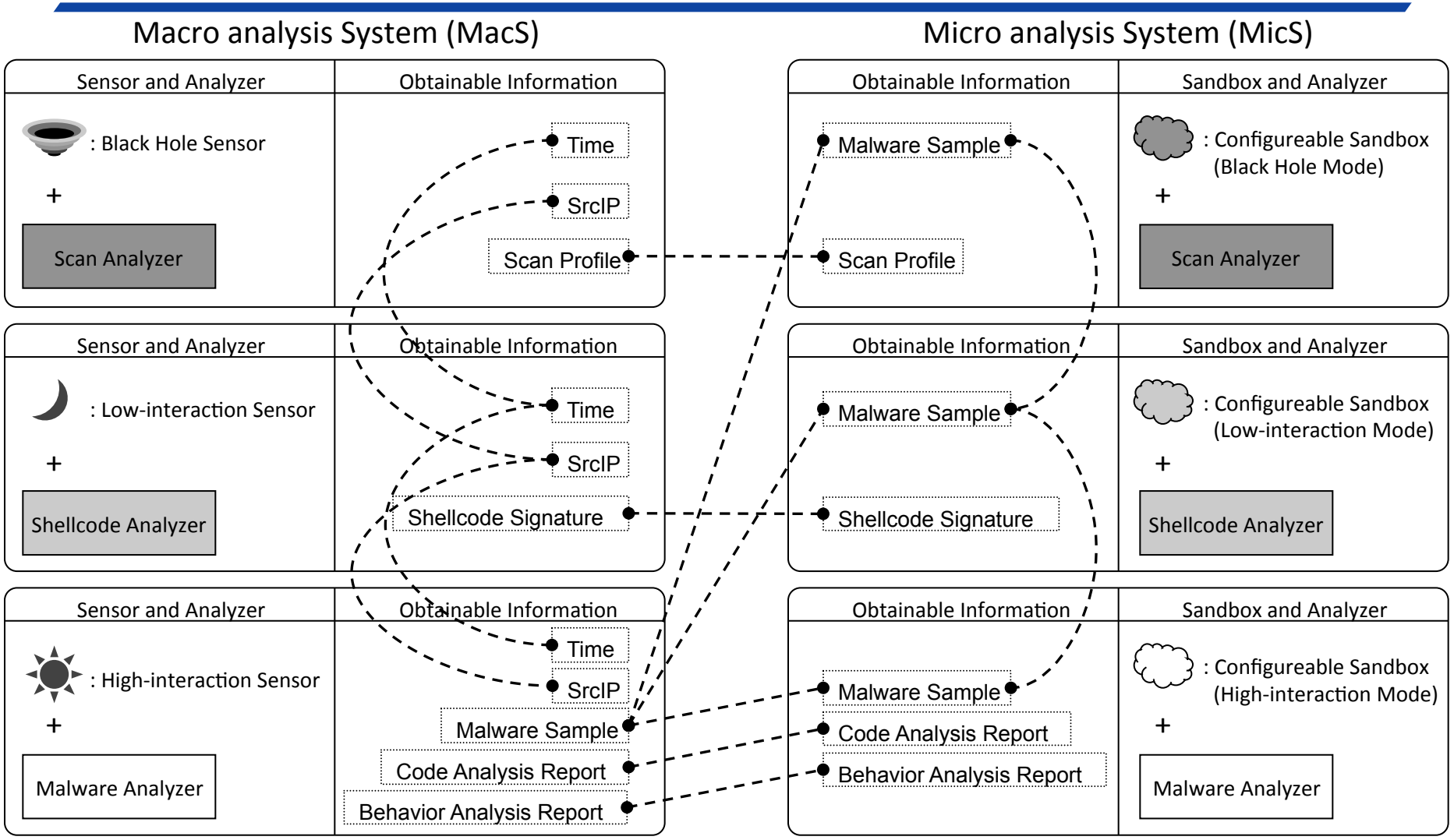
～ マクロとミクロの融合 ～



[1] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, "A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities," Proc. of the 2nd Joint Workshop on Information Security (JWIS2007), 2007.

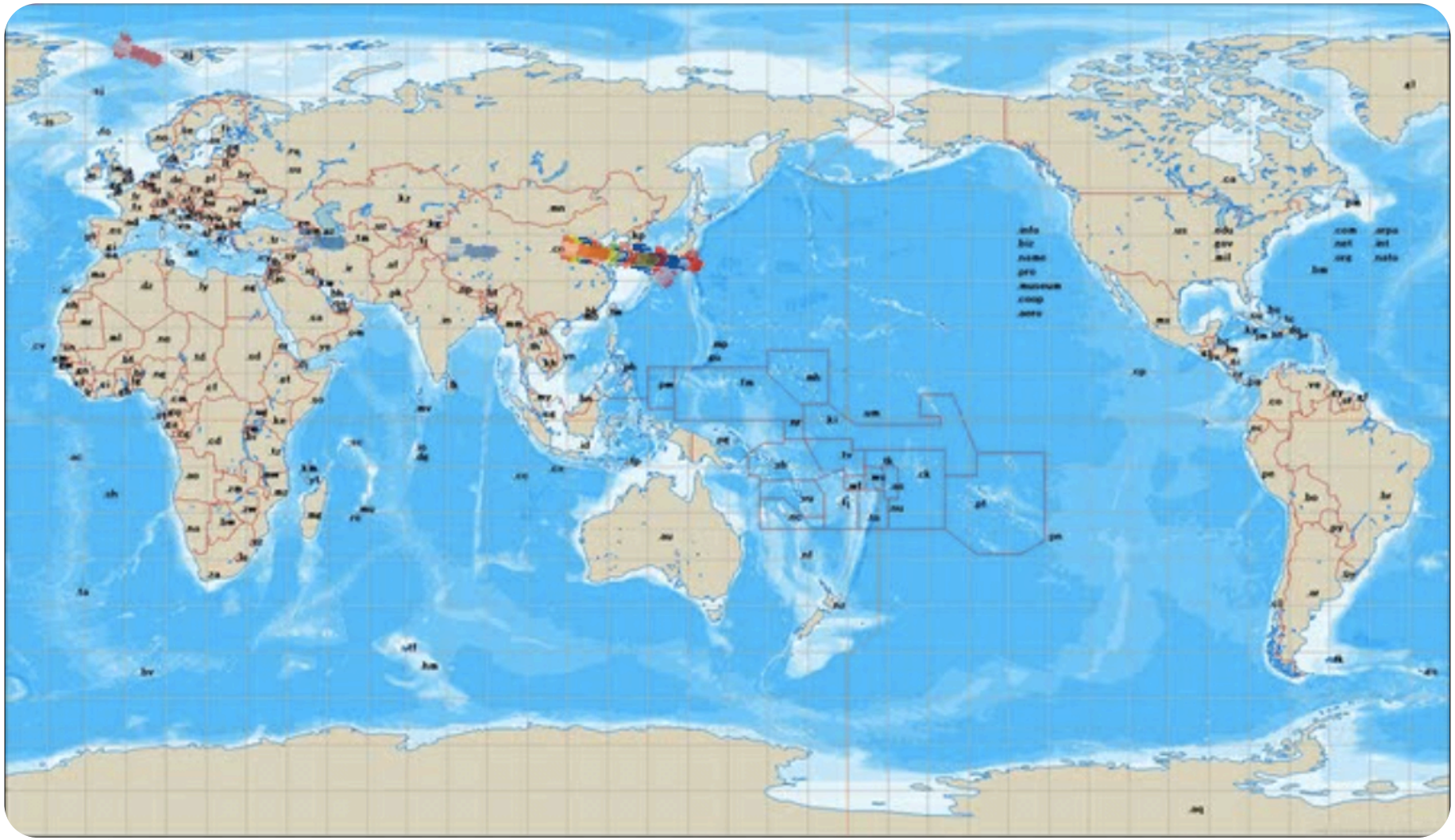
NICTERのコンセプト[1] (2007)

～ マクロとミクロの相関分析 ～



K. Nakao, K. Yoshioka, D. Inoue, M. Eto, "A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities," Proc. of the 2nd Joint Workshop on Information Security (JWIS2007), 2007.

2005年当時のダークネット観測結果

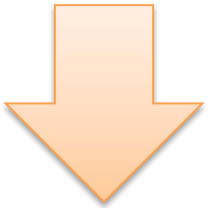


NICTERプロジェクトを育てた言葉 ②

Blasterのような
パンデミックは
もう起こらない

ポストBlaster：ボットネット

- **2004年頃～ ボットネットの台頭**
  - ✓ 2004年頃からマルウェアに感染しているPC群の同期した活動を観測
  - ✓ 感染後は特定のIRCサーバに接続して指令者からの制御命令を待ち受け
  - ✓ ボットネットを使ったマネタイズ（愉快犯→経済目的）



大規模感染はもう起こらないって！

（≒ ダークネット観測は無駄無駄無駄ァ）

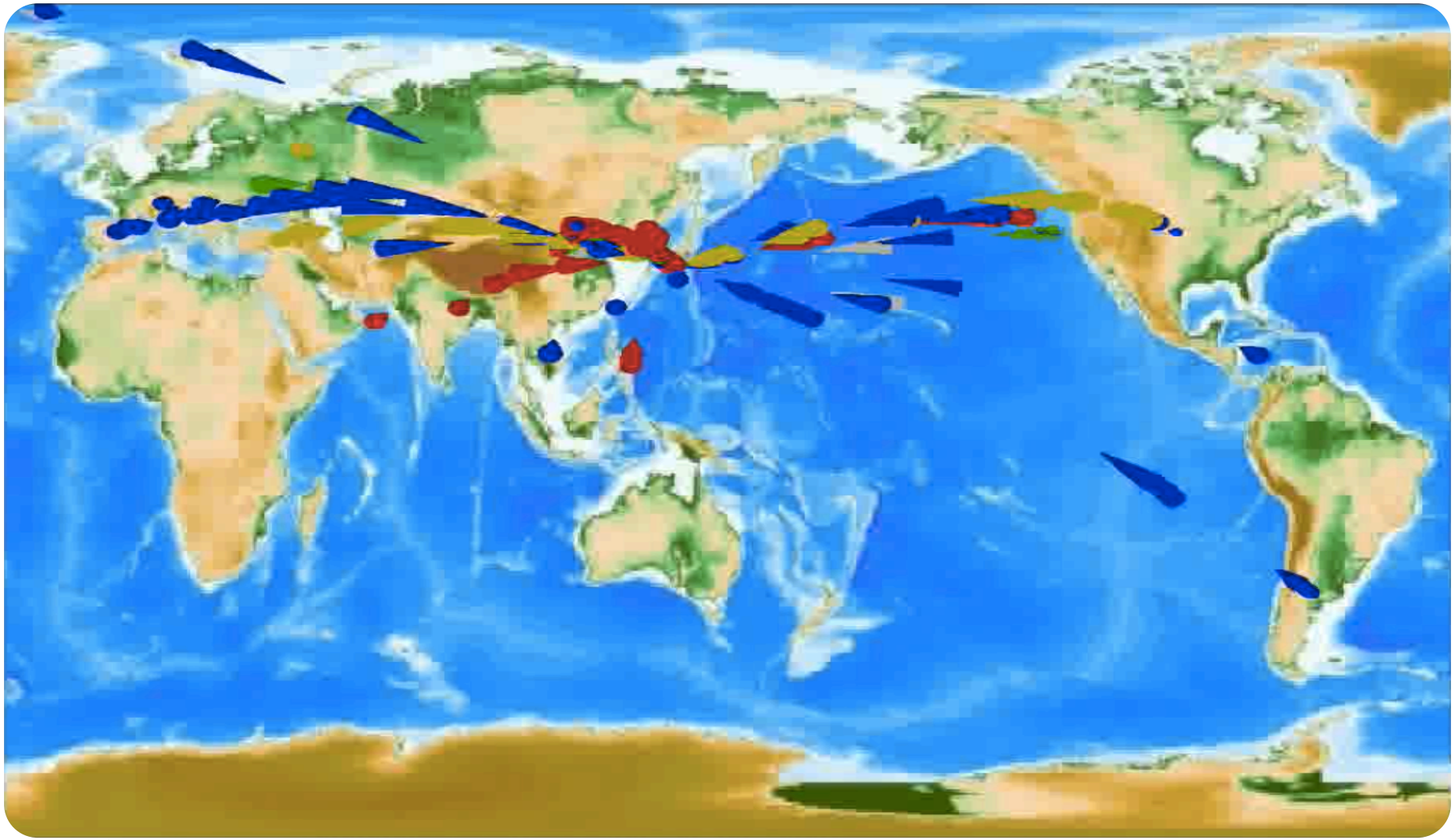
ちょっと待って下さい…

その説
根拠なくないですか？

↓

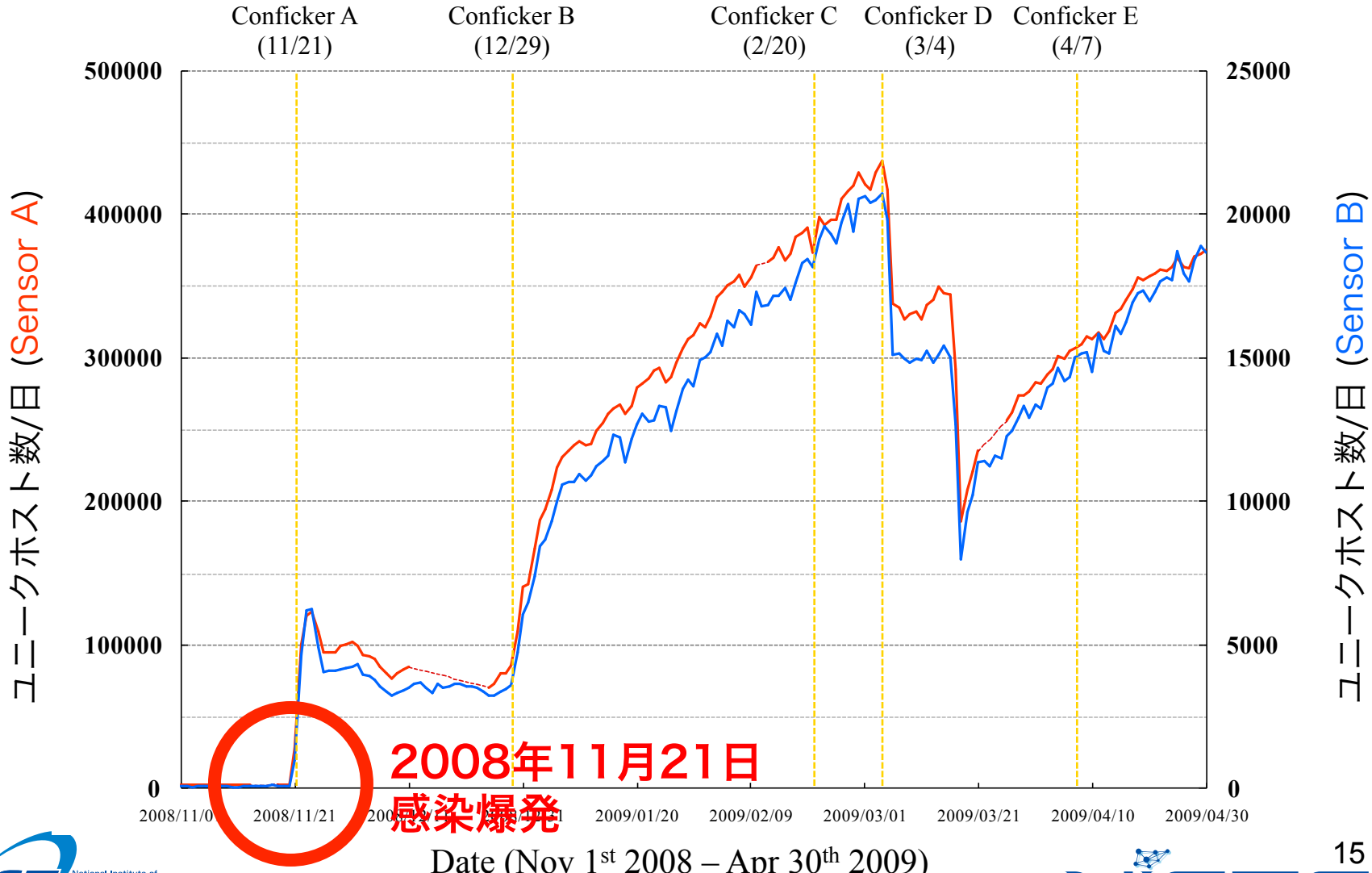
観測は続けますね！

2007年当時のダークネット観測結果



そして2008年… Conficker出現

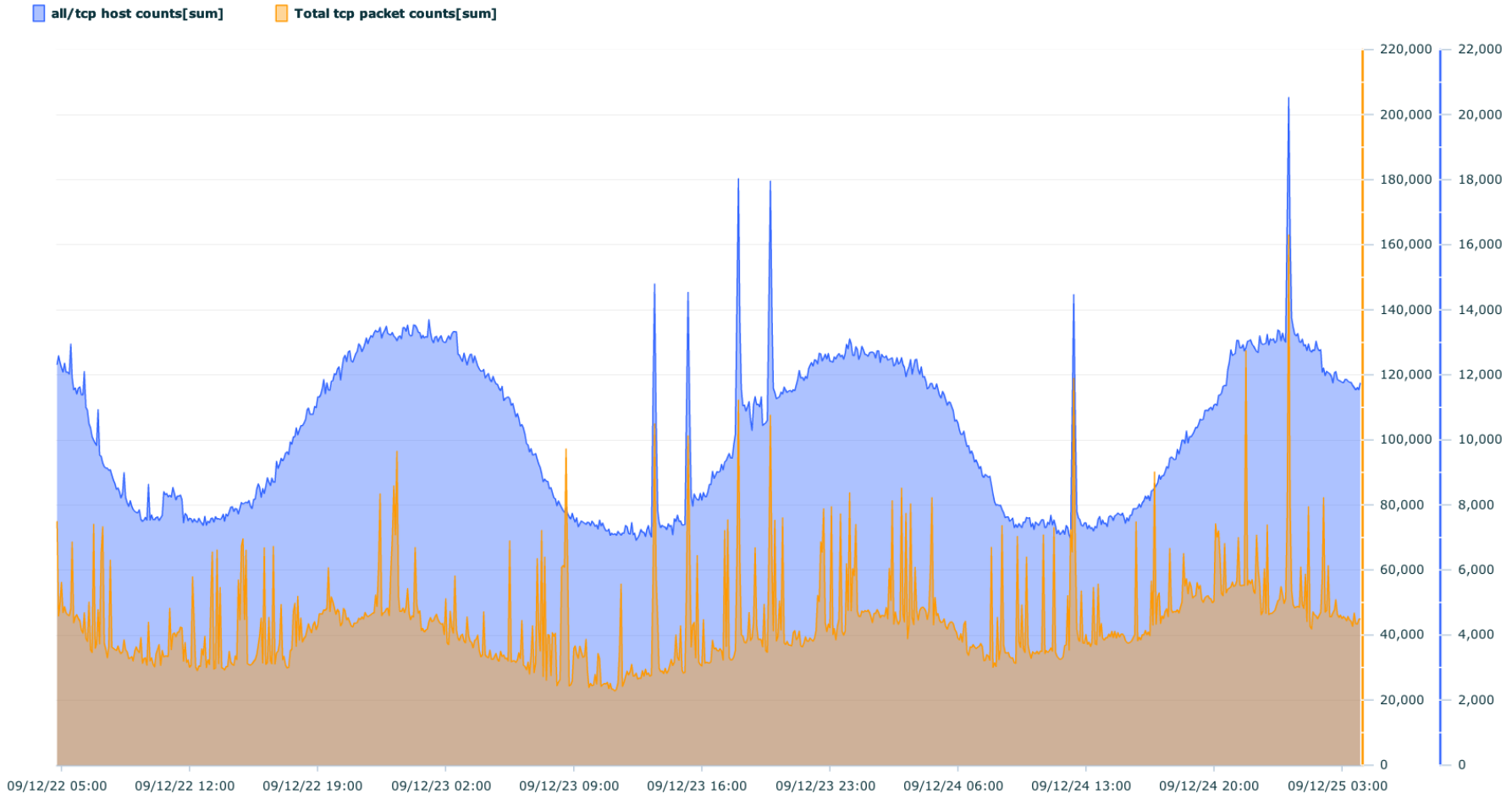
～ ユニークホスト数 on 445/tcp ～



National Institute of Information and Communications Technology

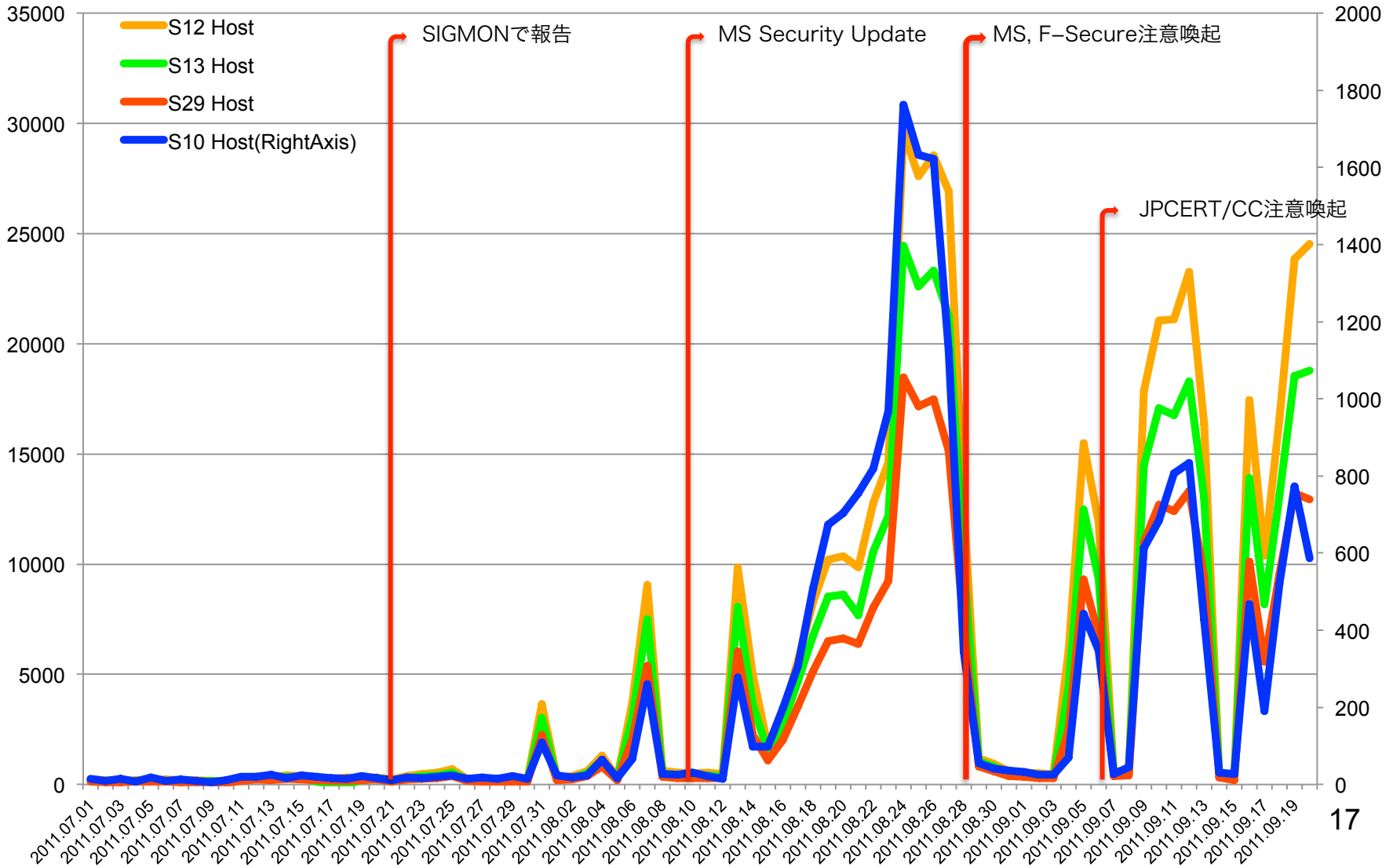
NICTER Network Incident analysis Center for Tactical Emergency Response

Conficker の影響：ダークネットの周期性

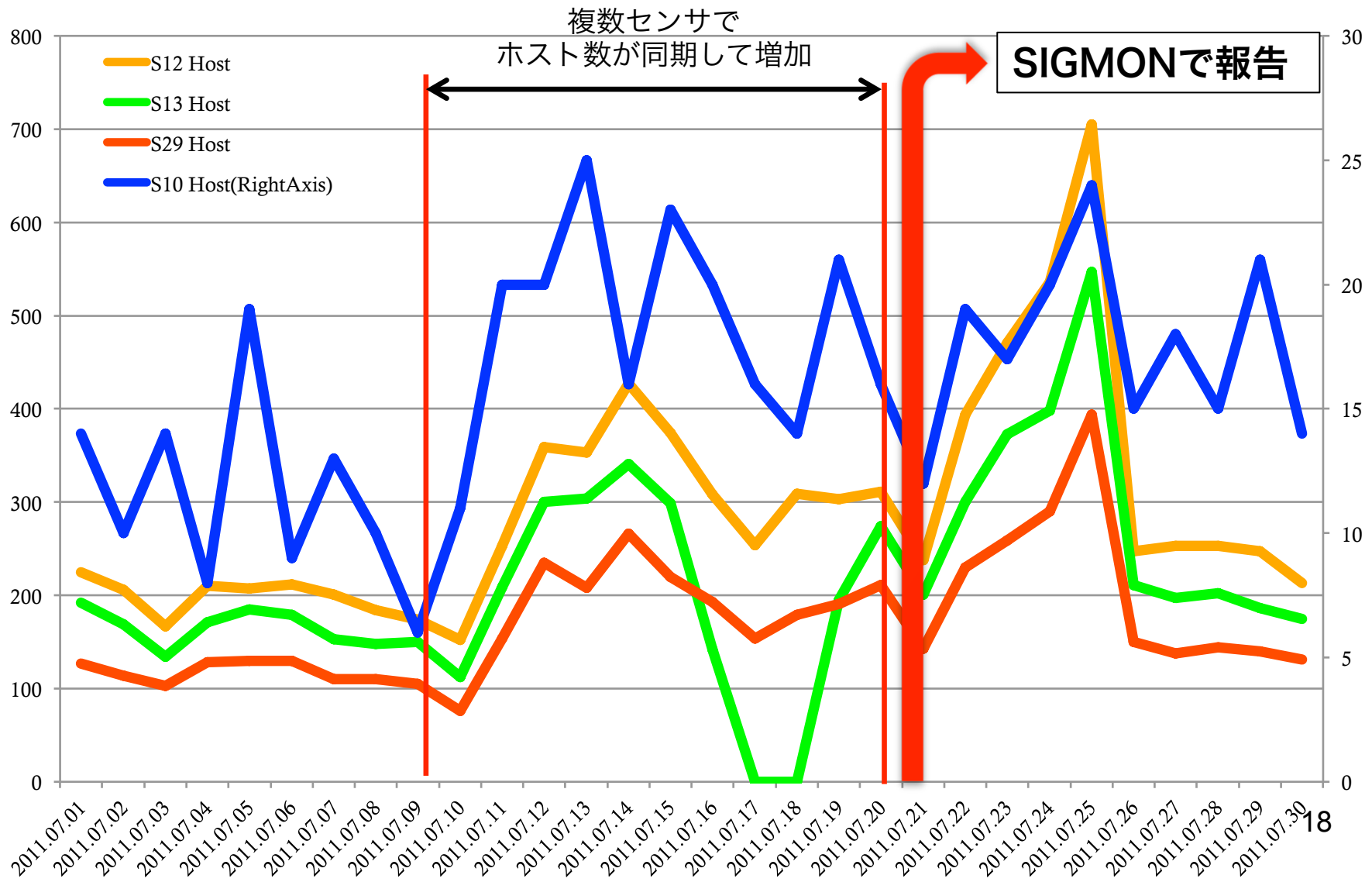


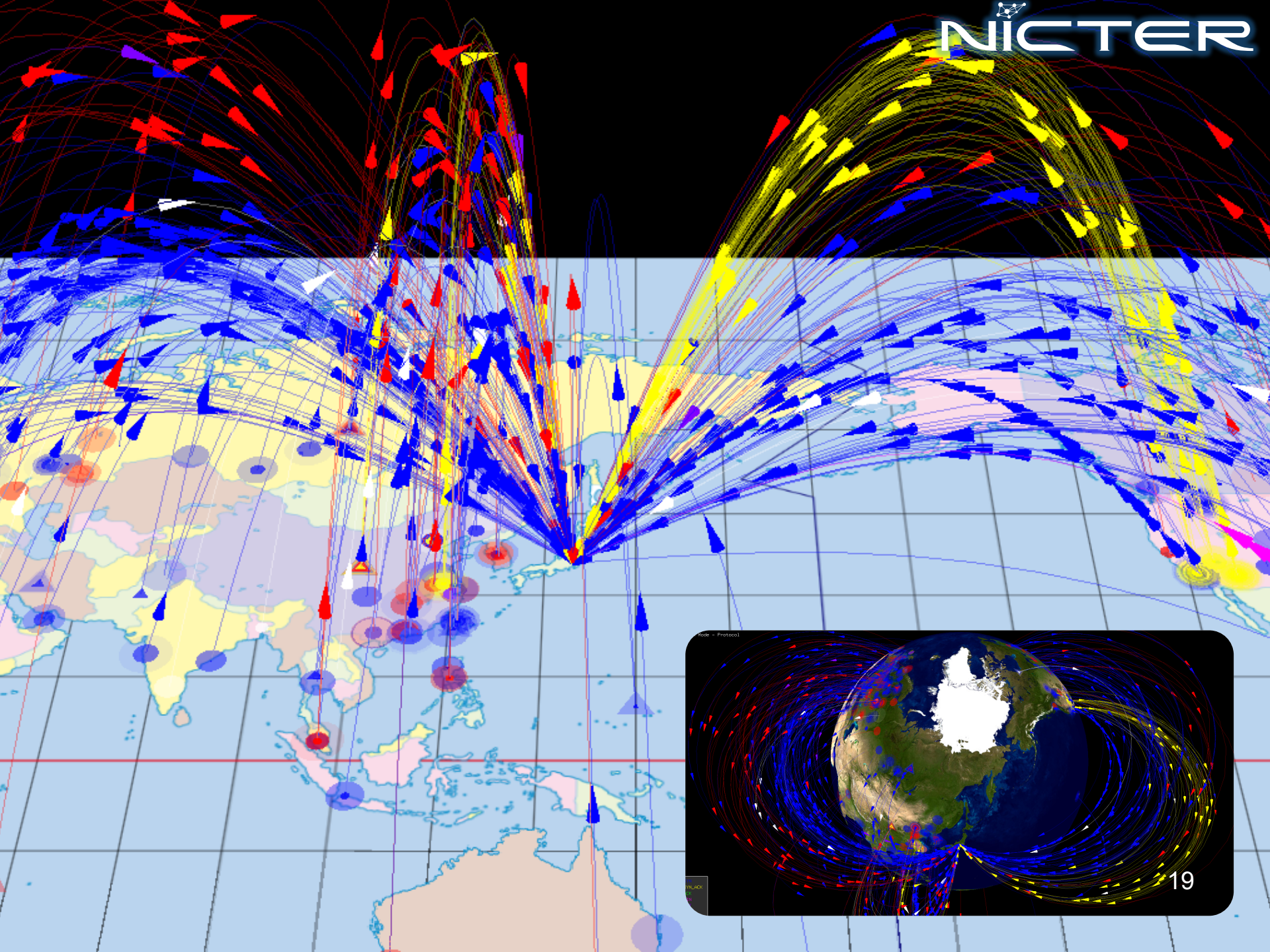
2011年 Mortoワーム出現

～ ユニークホスト数 on 3389/tcp ～

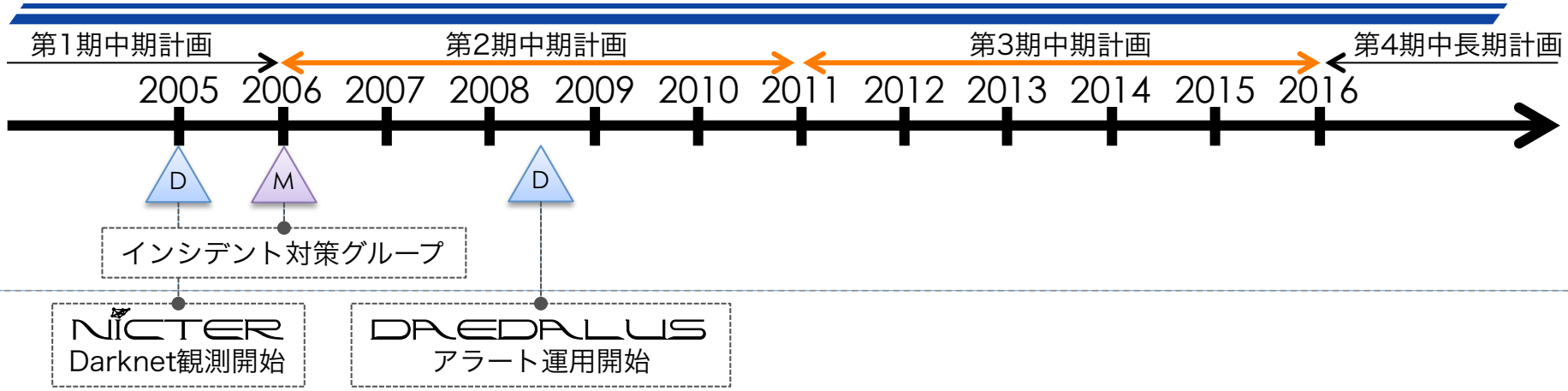


3389/tcp ダークネット観測結果（拡大）




NICTER
19

NICTERプロジェクト 10年線表



Darknet

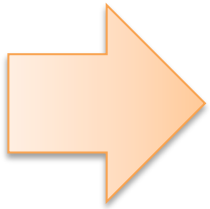
Livenet

CTF

DAEDALUS[2]の出発点 (2008)

- ダークネット観測でワーム系マルウェアの全体傾向は見えるようになってきた。

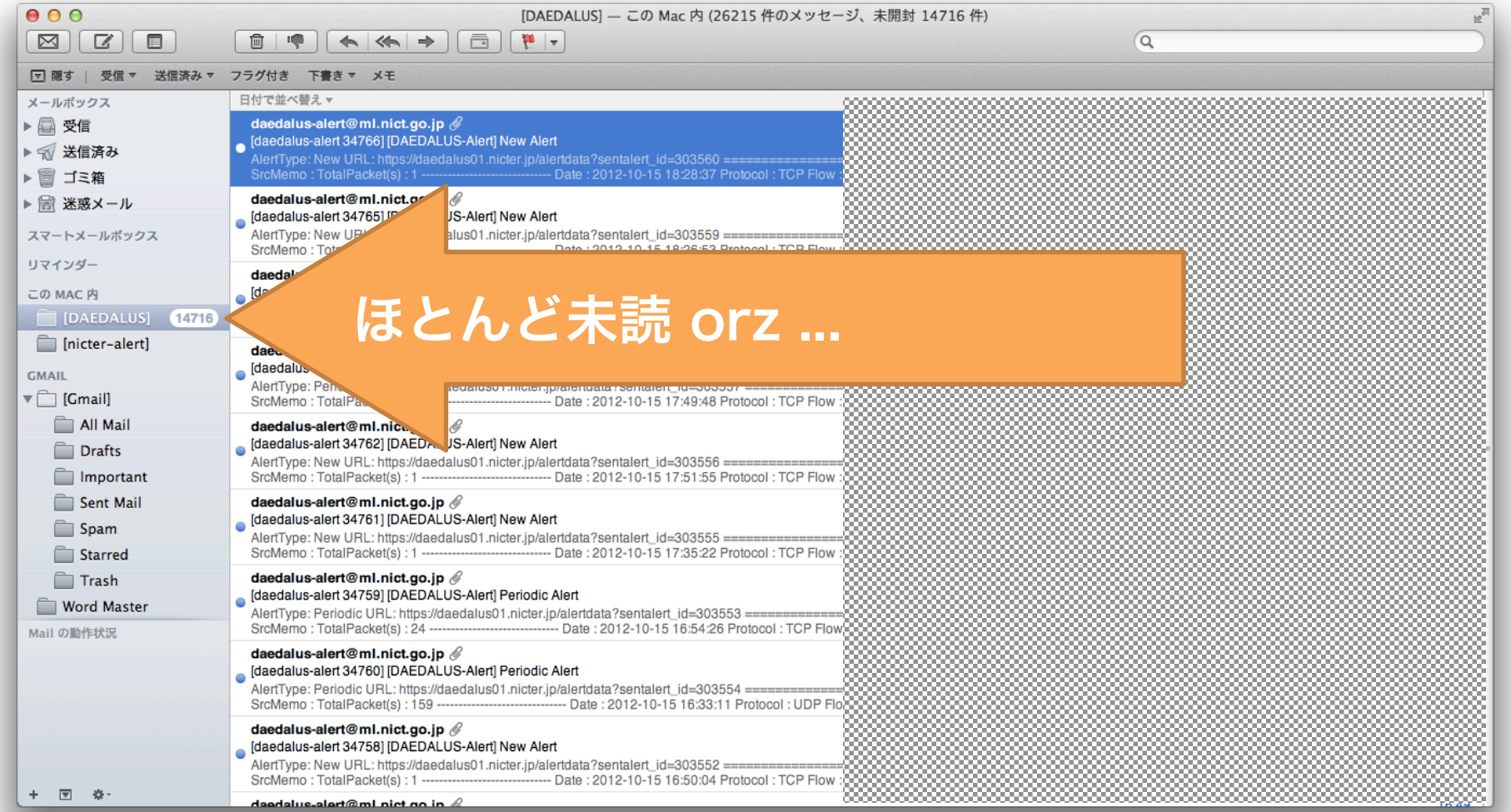
- センサ設置してもらっている組織から結構スキャン飛んでくるよね…



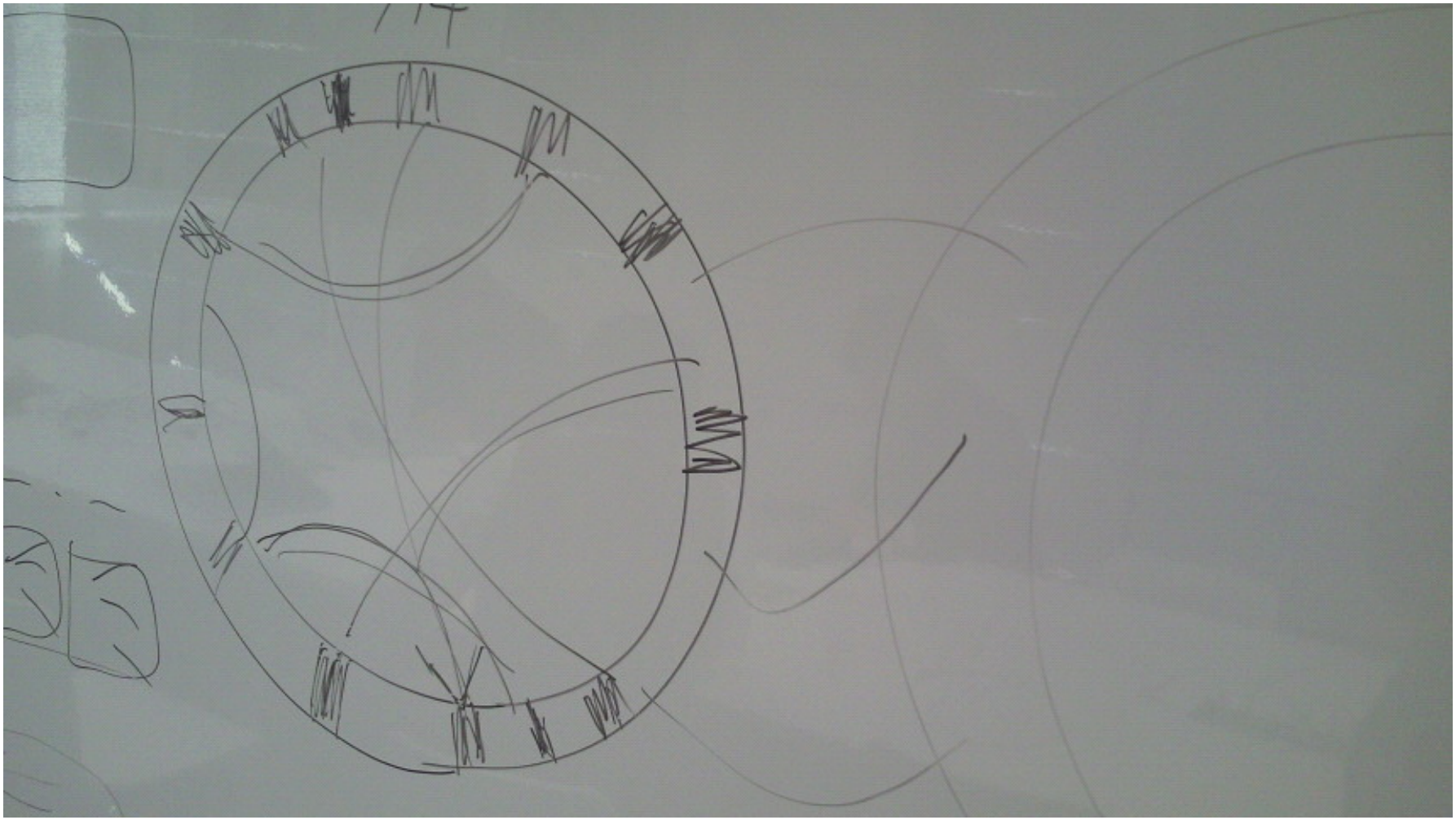
アラート送ってみよう！

[2] D. Inoue, M. Suzuki, M. Eto, K. Yoshioka, K. Nakao, “DAEDALUS: Novel Application of Large-scale Darknet Monitoring for Practical Protection of Live Networks,” 12th International Symposium on Recent Advances in Intrusion Detection (RAID 2009), pp. 381–382, 2009.

膨大なアラートが・・・

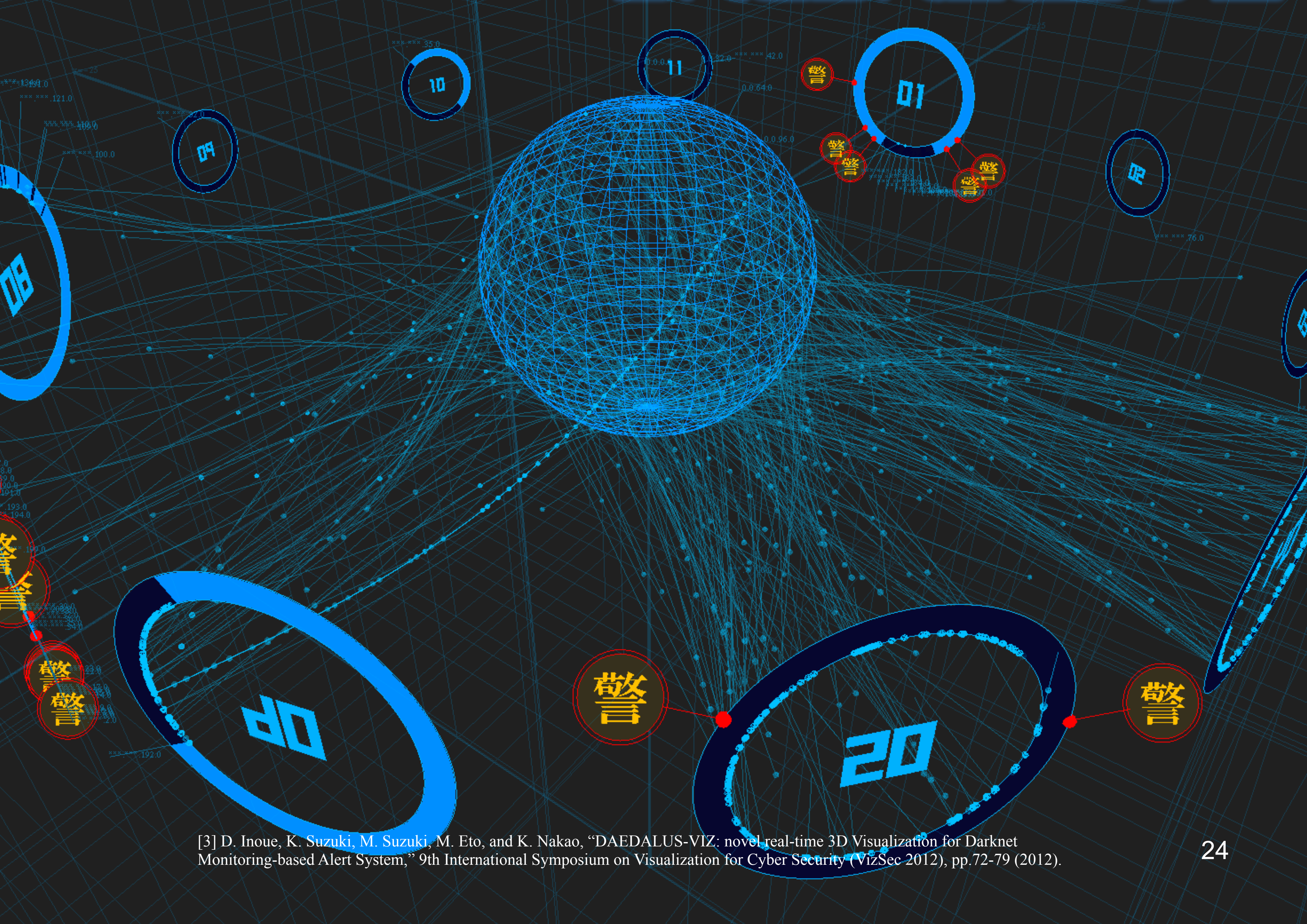

[DAEDALUS] — この Mac 内 (26215 件のメッセージ、未開封 14716 件)
隠す
受信
送信済み
フラグ付き
下書き
メモ
メールボックス
受信
送信済み
ゴミ箱
迷惑メール
スマートメールボックス
リマインダー
この MAC 内
[DAEDALUS] 14716
[nicter-alert]
GMAIL
[Gmail]
All Mail
Drafts
Important
Sent Mail
Spam
Starred
Trash
Word Master
Mail の動作状況
日付で並べ替え
daedalus-alert@ml.nict.go.jp
[daedalus-alert 34766] [DAEDALUS-Alert] New Alert
AlertType: New URL: https://daedalus01.nicter.jp/alertdata?sentalert_id=303560
SrcMemo : TotalPacket(s) : 1 Date : 2012-10-15 18:28:37 Protocol : TCP Flow
daedalus-alert@ml.nict.go.jp
[daedalus-alert 34765] [DAEDALUS-Alert] New Alert
AlertType: New URL: https://daedalus01.nicter.jp/alertdata?sentalert_id=303559
SrcMemo : TotalPacket(s) : 1 Date : 2012-10-15 18:26:52 Protocol : TCP Flow
daedalus-alert@ml.nict.go.jp
[daedalus-alert 34762] [DAEDALUS-Alert] New Alert
AlertType: New URL: https://daedalus01.nicter.jp/alertdata?sentalert_id=303556
SrcMemo : TotalPacket(s) : 1 Date : 2012-10-15 17:51:55 Protocol : TCP Flow
daedalus-alert@ml.nict.go.jp
[daedalus-alert 34761] [DAEDALUS-Alert] New Alert
AlertType: New URL: https://daedalus01.nicter.jp/alertdata?sentalert_id=303555
SrcMemo : TotalPacket(s) : 1 Date : 2012-10-15 17:35:22 Protocol : TCP Flow
daedalus-alert@ml.nict.go.jp
[daedalus-alert 34759] [DAEDALUS-Alert] Periodic Alert
AlertType: Periodic URL: https://daedalus01.nicter.jp/alertdata?sentalert_id=303553
SrcMemo : TotalPacket(s) : 24 Date : 2012-10-15 16:54:26 Protocol : TCP Flow
daedalus-alert@ml.nict.go.jp
[daedalus-alert 34760] [DAEDALUS-Alert] Periodic Alert
AlertType: Periodic URL: https://daedalus01.nicter.jp/alertdata?sentalert_id=303554
SrcMemo : TotalPacket(s) : 159 Date : 2012-10-15 16:33:11 Protocol : UDP Flo
daedalus-alert@ml.nict.go.jp
[daedalus-alert 34758] [DAEDALUS-Alert] New Alert
AlertType: New URL: https://daedalus01.nicter.jp/alertdata?sentalert_id=303552
SrcMemo : TotalPacket(s) : 1 Date : 2012-10-15 16:50:04 Protocol : TCP Flow
ほとんど未読 orz ...

アラートの可視化エンジンを作ろう！



2012年2月13日 DAEDALUS-VIZ 1stスケッチ

DAEDALUS-VIZ[3]



[3] D. Inoue, K. Suzuki, M. Suzuki, M. Eto, and K. Nakao, "DAEDALUS-VIZ: novel real-time 3D Visualization for Darknet Monitoring-based Alert System," 9th International Symposium on Visualization for Cyber Security (VizSec 2012), pp.72-79 (2012).

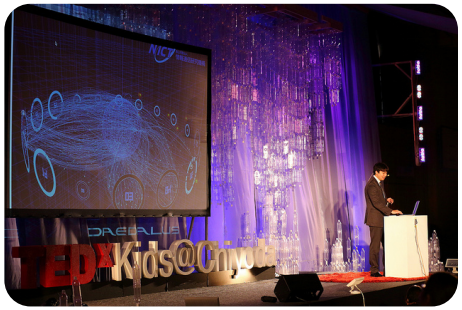
NICTERプロジェクトを育てた言葉 ③

俺たちの知ってる
日本が帰って来た！

DAEDALUS現象

Youtube

JP: over 600,000 access
EN: over 200,000 access



TEDx

TEDxKids@Chiyoda 2013

Web News

COMPUTERWORLD, etc.

Exhibition

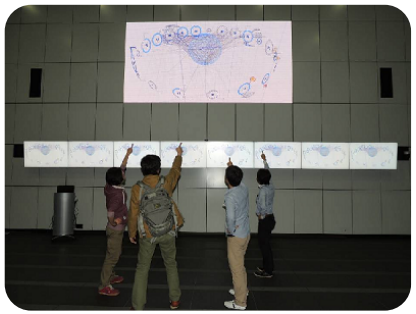
THE SEKAI-ICHI:
Unique Inspirations
“Made in Japan”

TV

TBS “NEWS23X”, etc.

Ghost in the Shell

Interview by GITS ARISE



Museum

Miraikan
National Museum of Emerging
Science and Innovation

National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

NICTERプロジェクトを育てた言葉 ⑤

ハニーポットは
もう死んでいる

2010年頃から…

- ハニーポットで捕獲されるマルウェアがAllapleやConfikerばかり…

- 「マルウェア等サイバー攻撃情報収集分析手法の技術評価に関する調査研究」（2014）

ハニーポットは無駄無駄無駄ァ

ちょっと待って下さい…

＊＊＊の脆弱性ハンドラって
更新されてるんですか？

↓

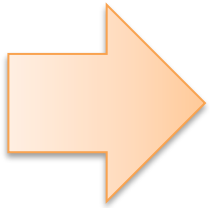
2008年で開発止めてますよ。

↓

お…おう…

新たなハニーポット技術

- ハニーポットという観測手法が死んだわけではない。
- ハニーポットが最新の攻撃に追いついていないだけ。

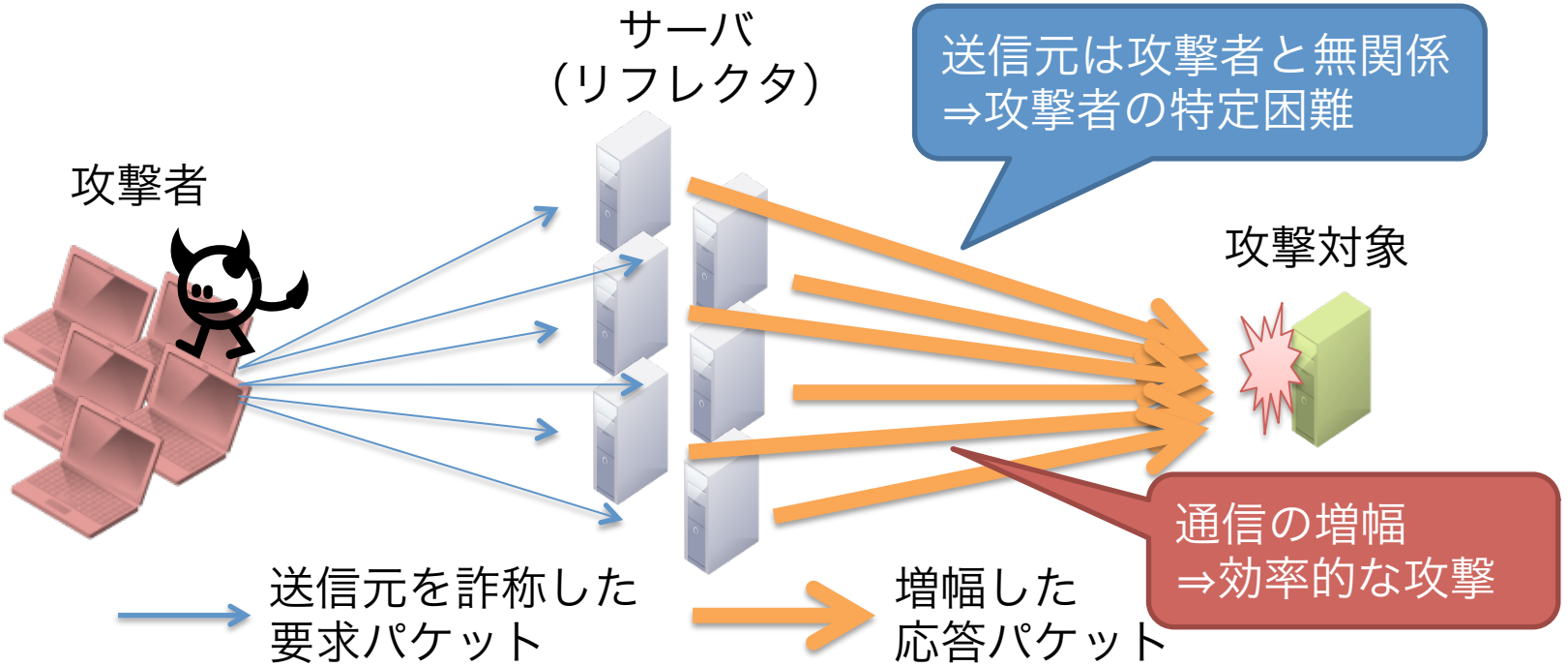


新たなハニーポット技術が必要

- AmpPot（横浜国大＋NICT）
- IoTPot（横浜国大）

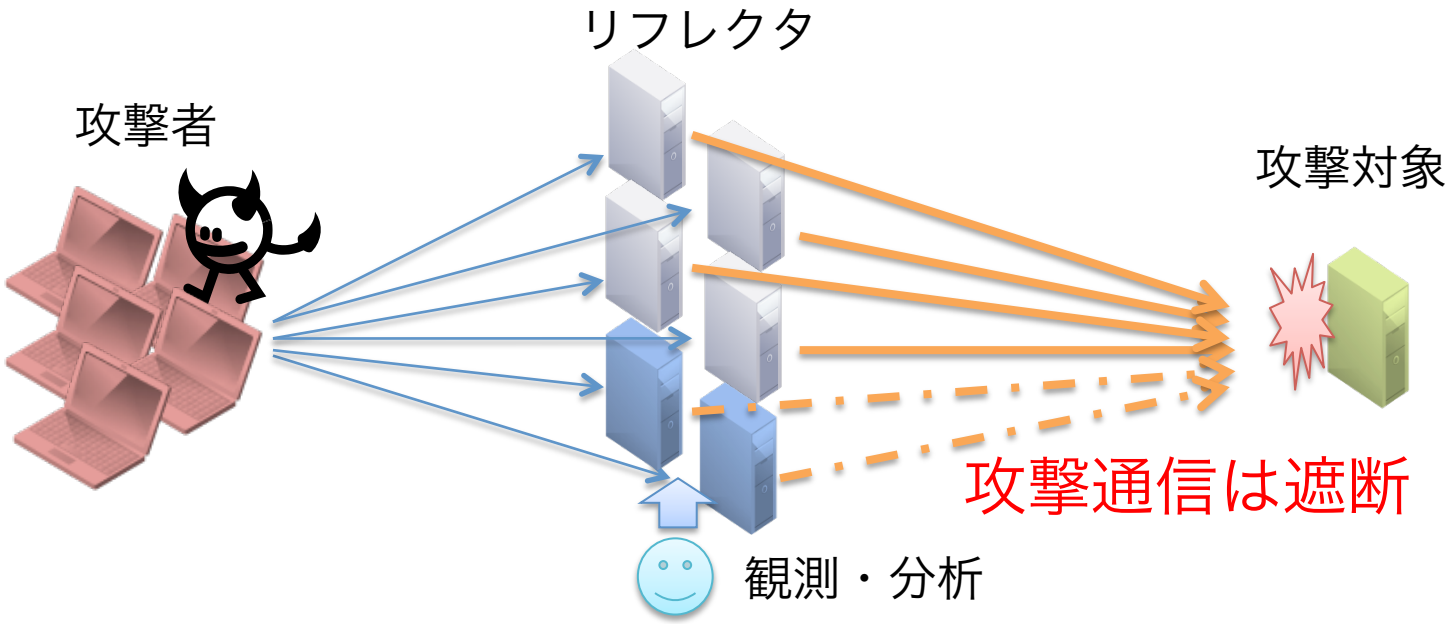
DRDoS攻撃

- **DRDoS攻撃（分散反射型サービス妨害攻撃）**
  - ✓ Distributed Reflection Denial of Service
  - ✓ サーバを経由して攻撃対象の資源を圧迫



DRDoSハニーポット[4]（AmpPot）

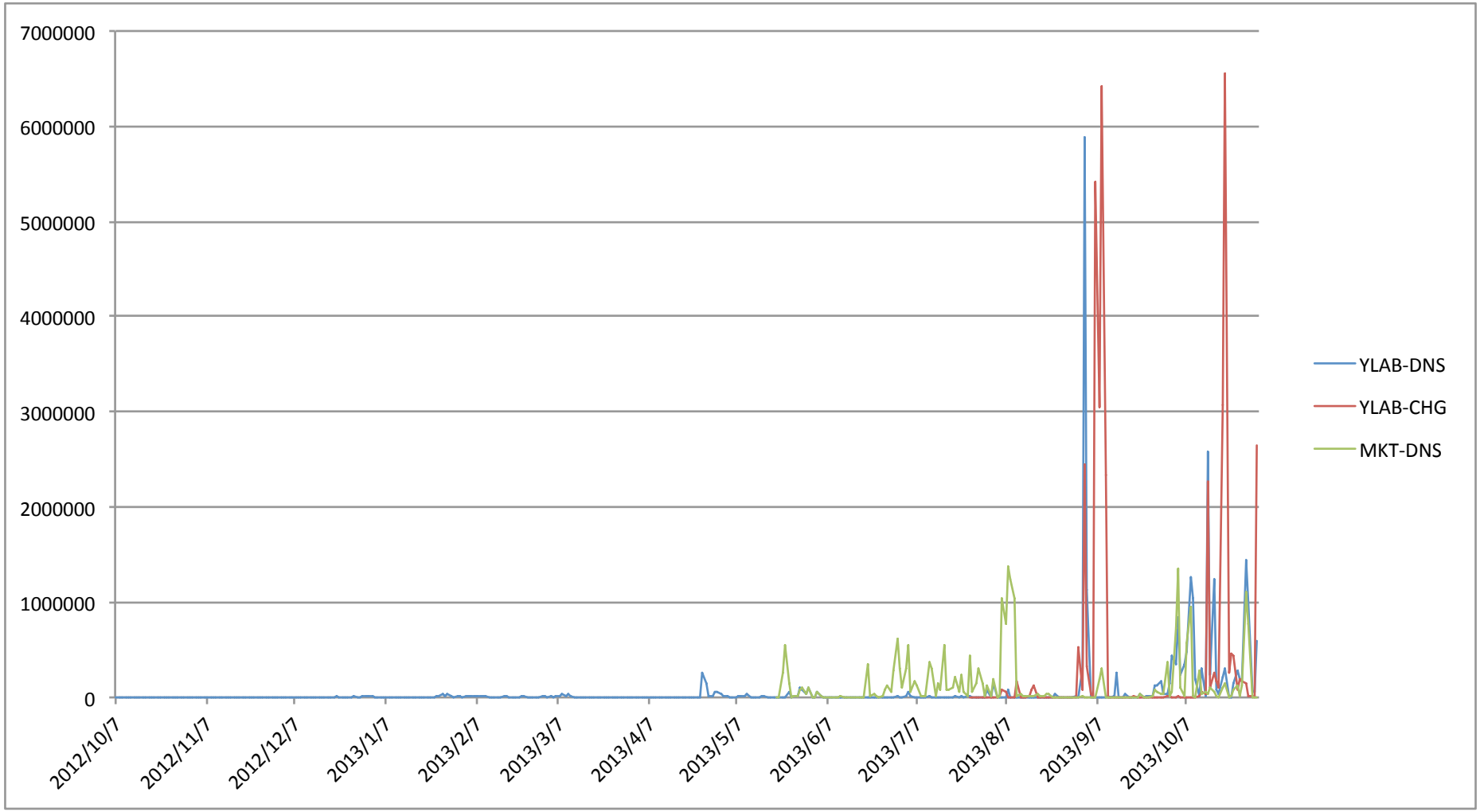
- DNS、NTP等を模擬したハニーポット
- リフレクタの視点でDRDoS攻撃を観測



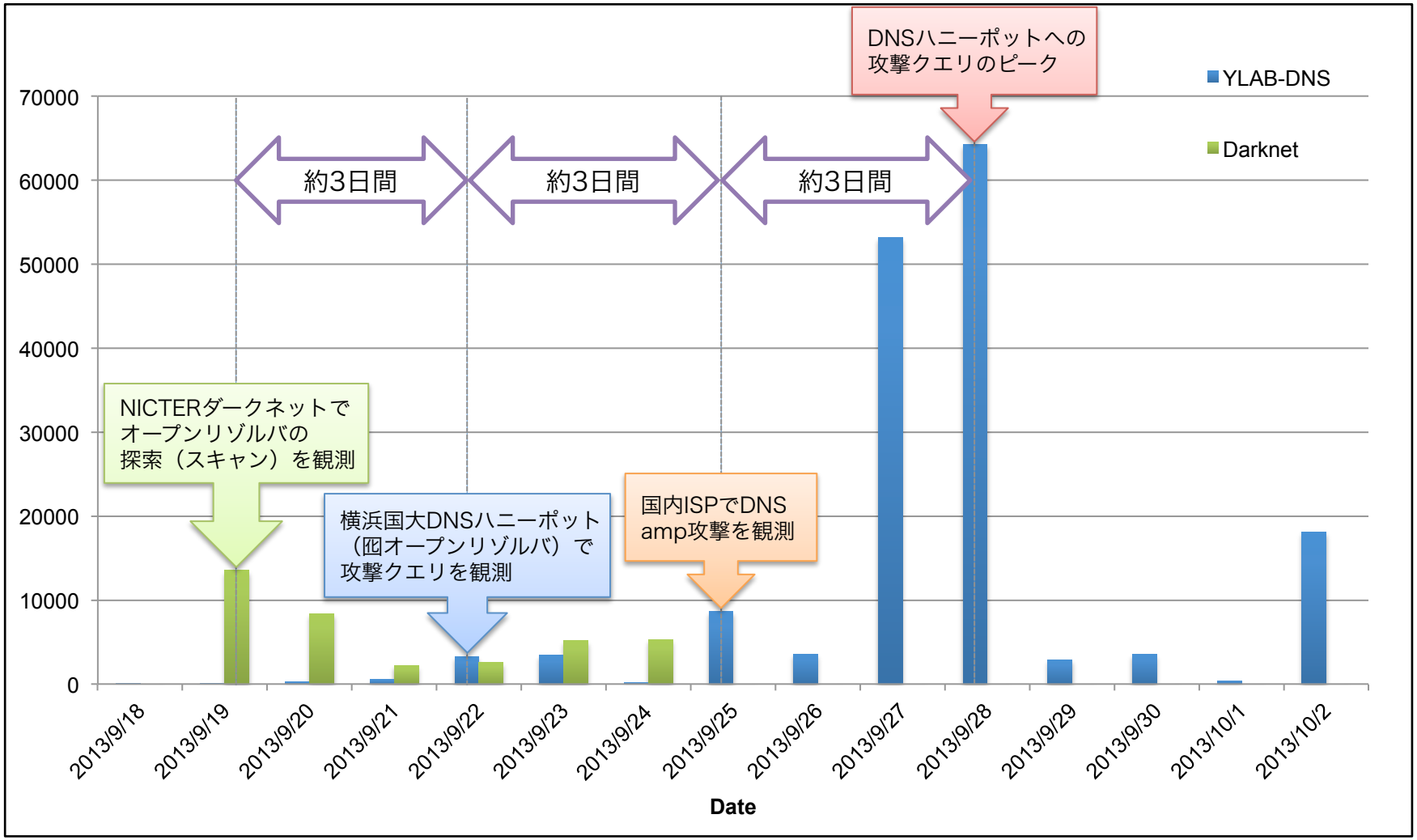
※横浜国立大学とNICTの共同開発・共同運用

[4] Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks," Proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'15).

DNSハニーポット 受信パケット数
– 2012年10月～2013年10月 –

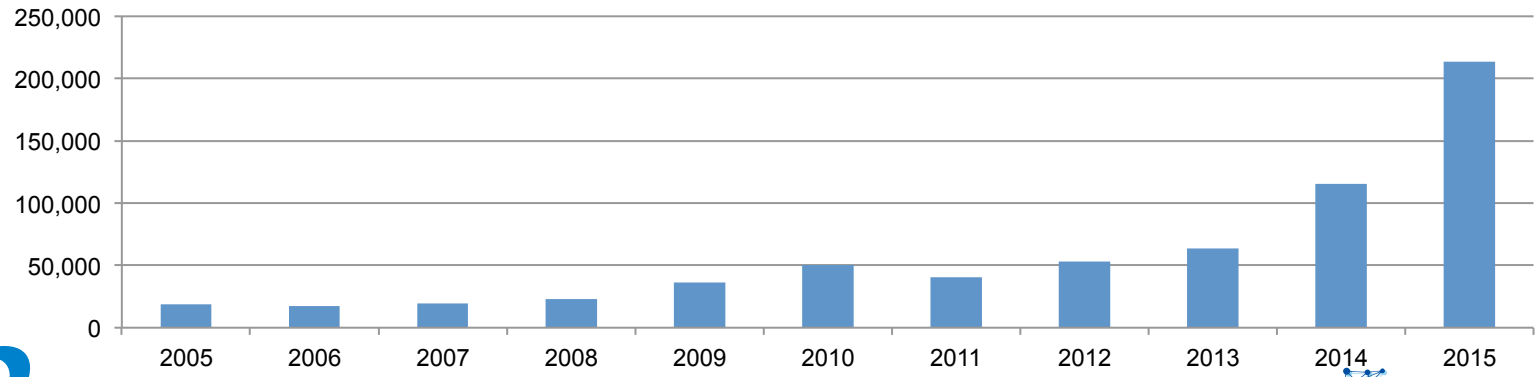


DNS amp攻撃観測事例（bitstress.com）



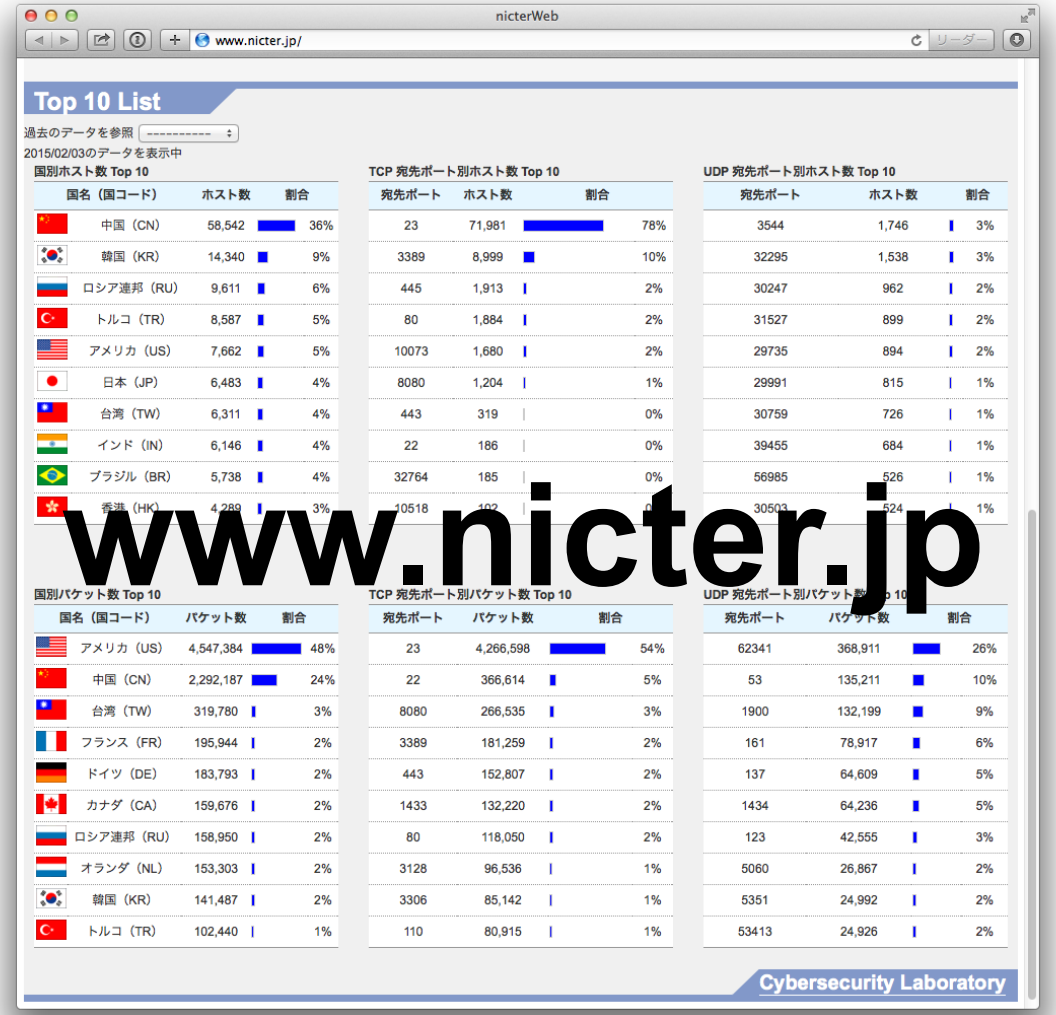
NICTERダークネット観測統計

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**

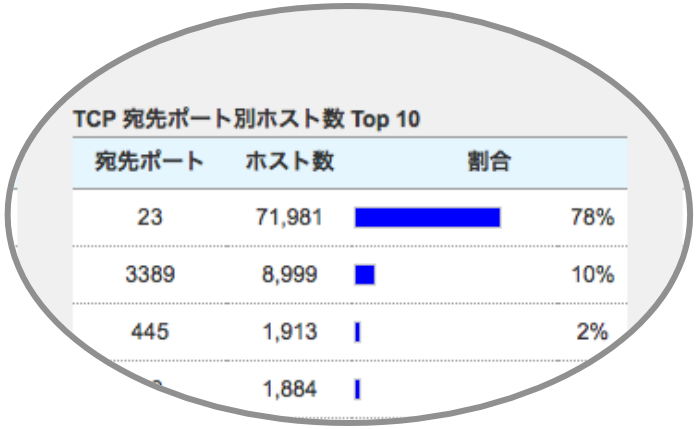


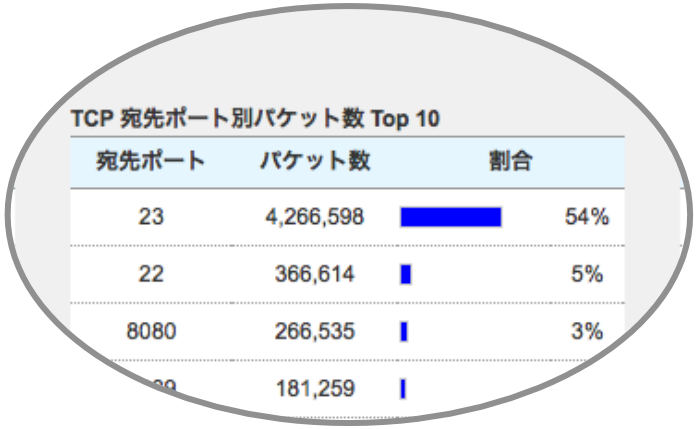
1 IPアドレス当たりの年間総観測パケット数

ダークネットトラフィック急増の原因



www.nicter.jp

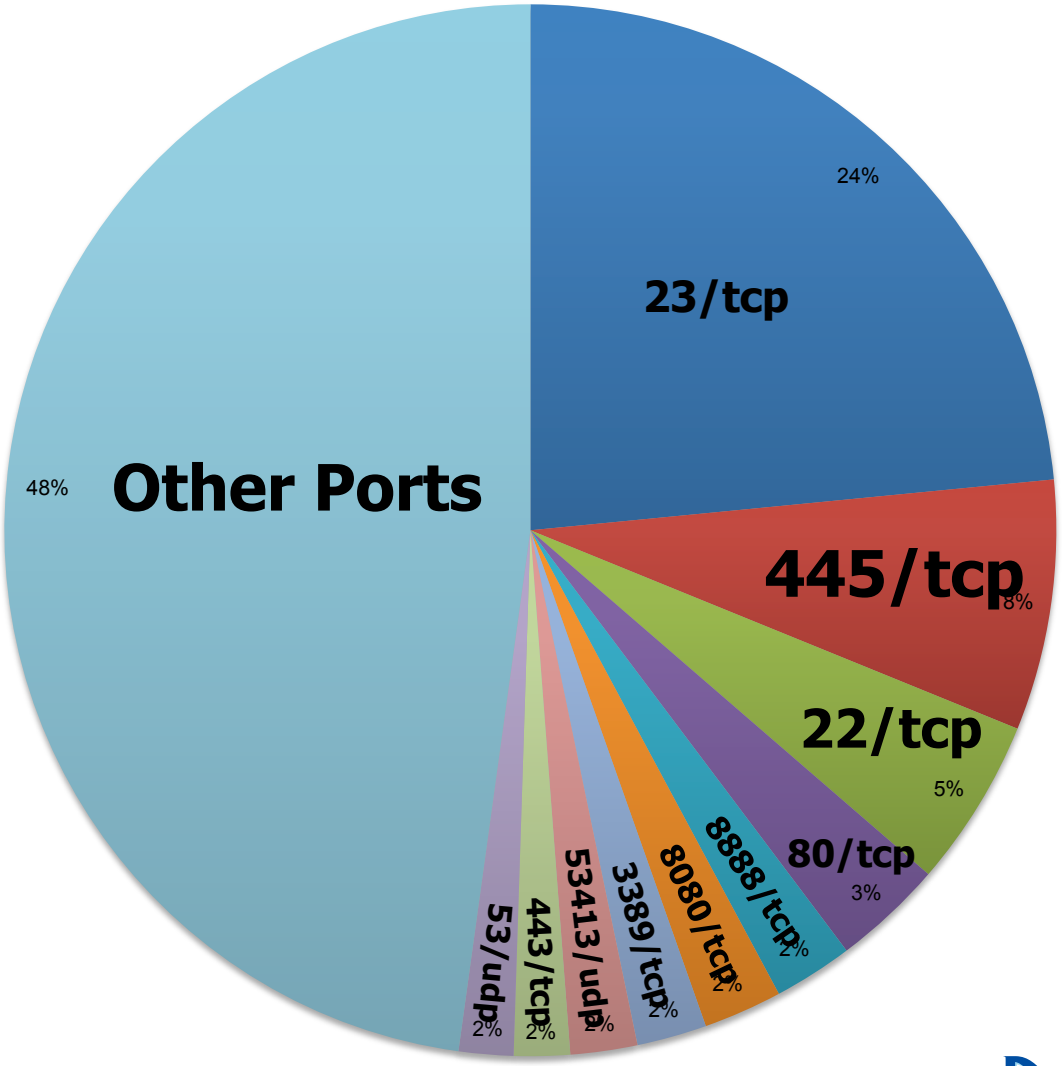




National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

宛先ポート番号別パケット数（2015年）




HG8245
HUAWEI
Account :
Password :
Login
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
Record System Copyright2008
pandora
BUSINESS SUITE
Java Application
Web Application
YOKOHAMA National University
YNU
※横浜国大による調査
Login
Password
Save login and password
Apply
BISBOX
BUSINESS
WEBSERVER
RouterOS v5.22
WebFig Login:
Winbox
Telnet
Graphs
License
Help
DrayTek
11n 150Mbps WLAN ADSL2+ Modem Router
Status
Network
Wireless
F460
Please login...
Welcome To Streamyx Conn Setup
Login
Password
Hardware Version : A1
Firmware Version : 1.03SHC
User Name :
Admin
Network video client
Remember me
VoIP ITA
38

攻撃元IoTデバイス

- 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

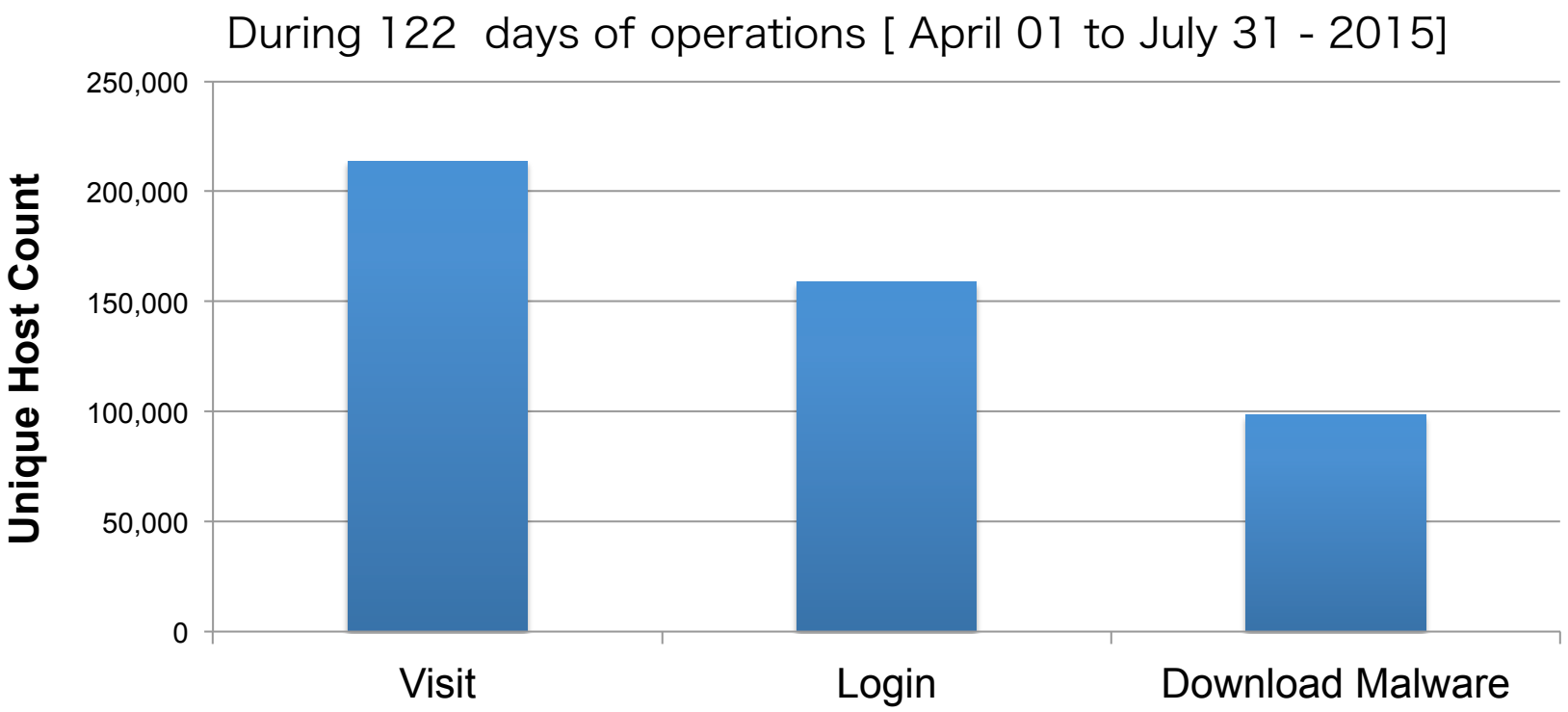
- **放送関連機器**
  - 映像配信システム
  - デジタル音声レコーダ
  - ビデオエンコーダ/デコーダ
  - セットトップボックス・アンテナ

- **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

IoTPot[5]で捕獲したマルウェア

横浜国大による実験結果

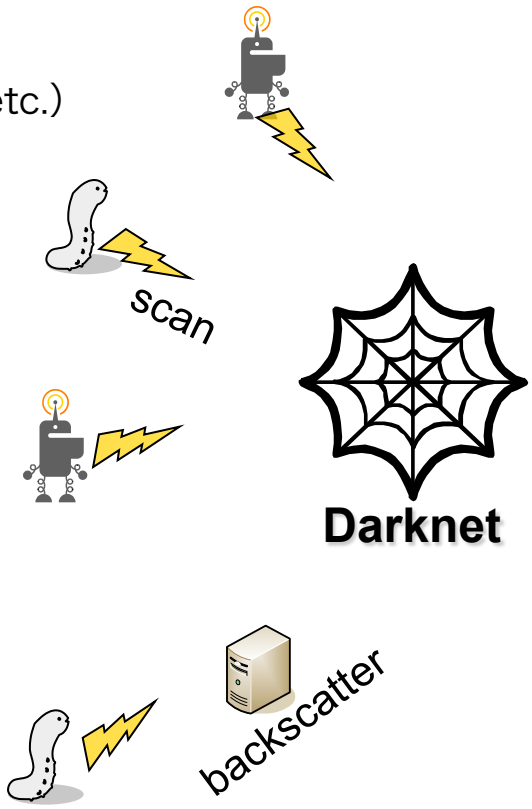


- 900,394 Malware Download Attempts
- Malware of 11 different CPU architectures
- 93% of downloaded binaries are new to Virus Total (2015/09)

[5] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, Proc. The 9th USENIX Workshop on Offensive Technologies (WOOT'15) (2015).

ダークネットで見えるもの（2016年版）

- **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.）
  - ✓ **IoT機器からのスキャン**
  - ✓ **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**



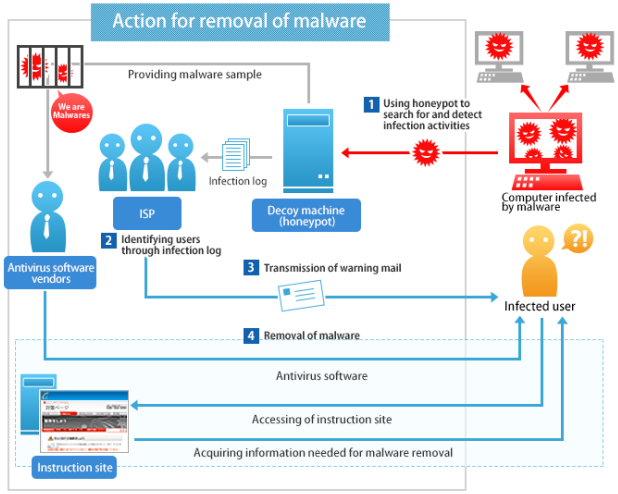
ダークネット観測結果等の共有

- **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～）

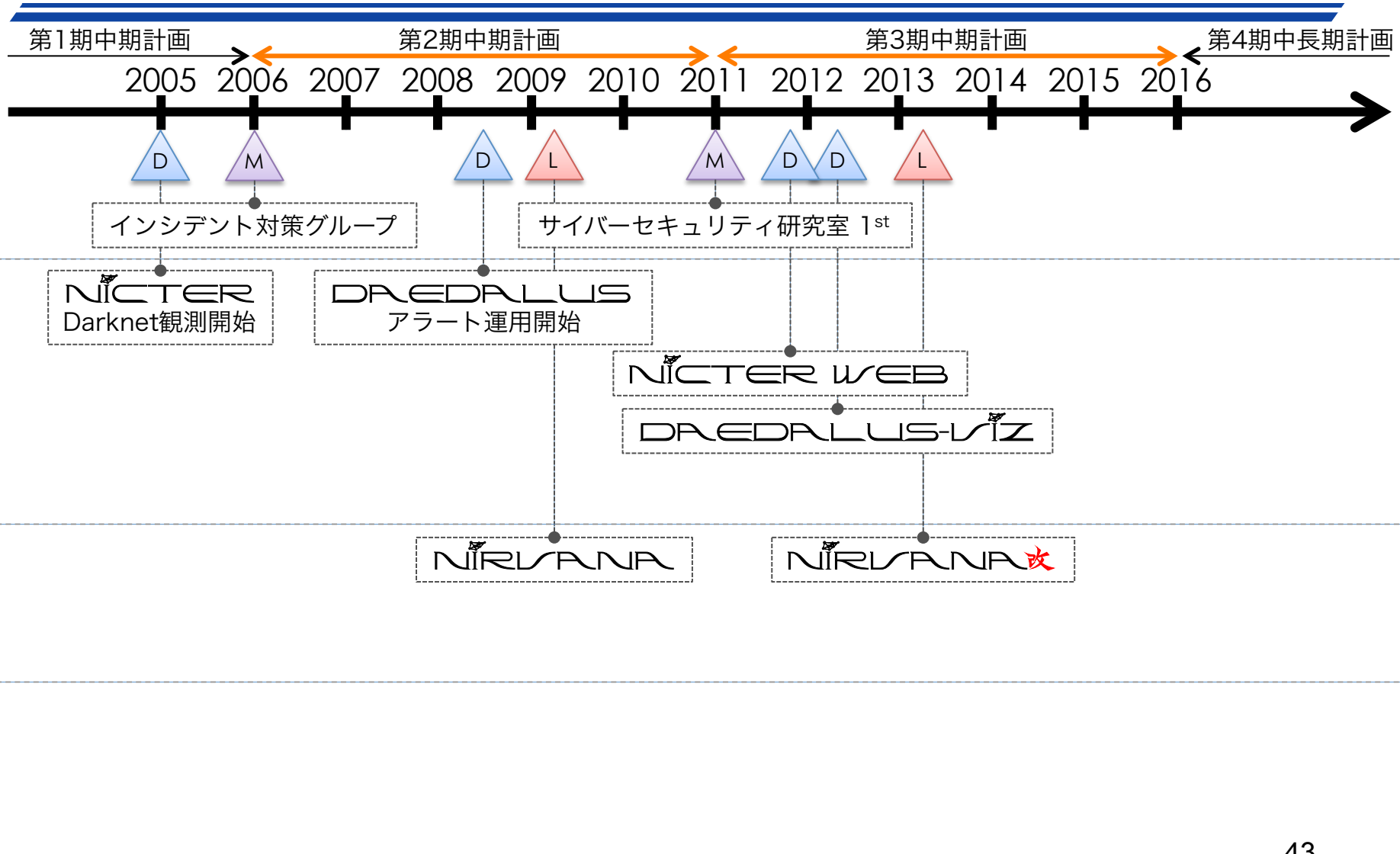
- **ACTIVE**（総務省）
  - ✓ 『国民のマルウェア対策支援プロジェクト』
  - ✓ 感染ユーザのIPアドレスを提供（2014年～）

- **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)

NICTERプロジェクト 10年線表

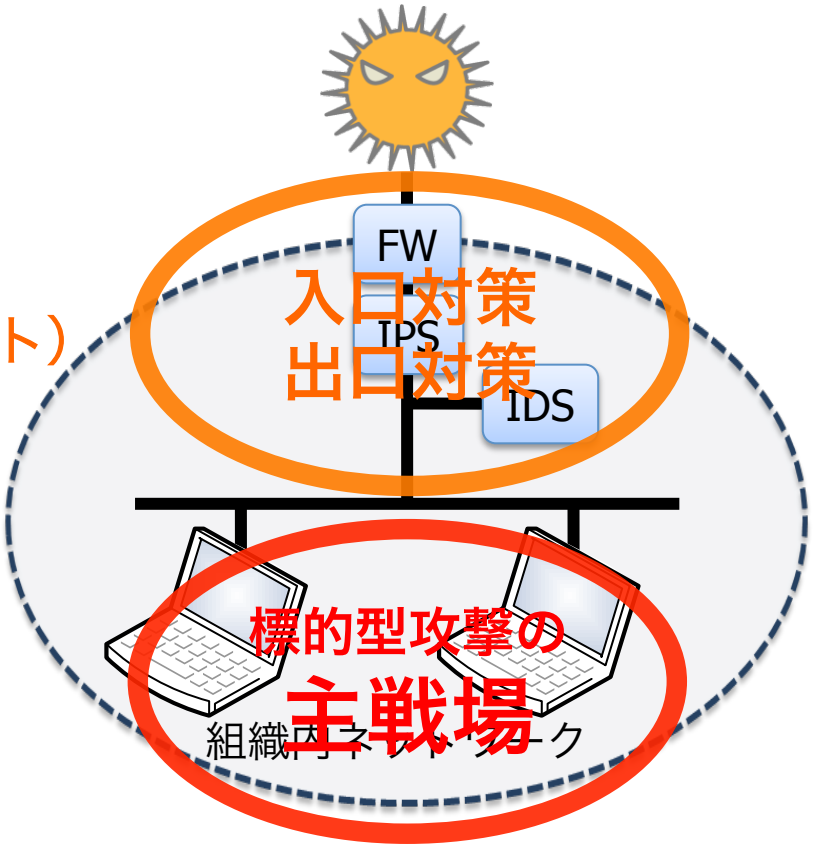


NICTERプロジェクトを育てた言葉 ④

標的型攻撃は出口対策

入口対策/出口対策 = 境界防御

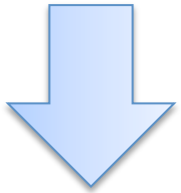
- **FW**（ファイアウォール）
  - ✓ Network層/Transport層/Application層で<u>パケット通過の可否</u>を判定
  - ✓ インライン
- **IDS**（侵入検知システム）
  - ✓ シグネチャで攻撃を<u>検知(アラート)</u>
  - ✓ ポートミラーリング or TAP
- **IPS**（侵入防止システム）
  - ✓ シグネチャで攻撃を<u>防止（遮断）</u>
  - ✓ インライン



標的型攻撃研究の難しさ（2011年当時）

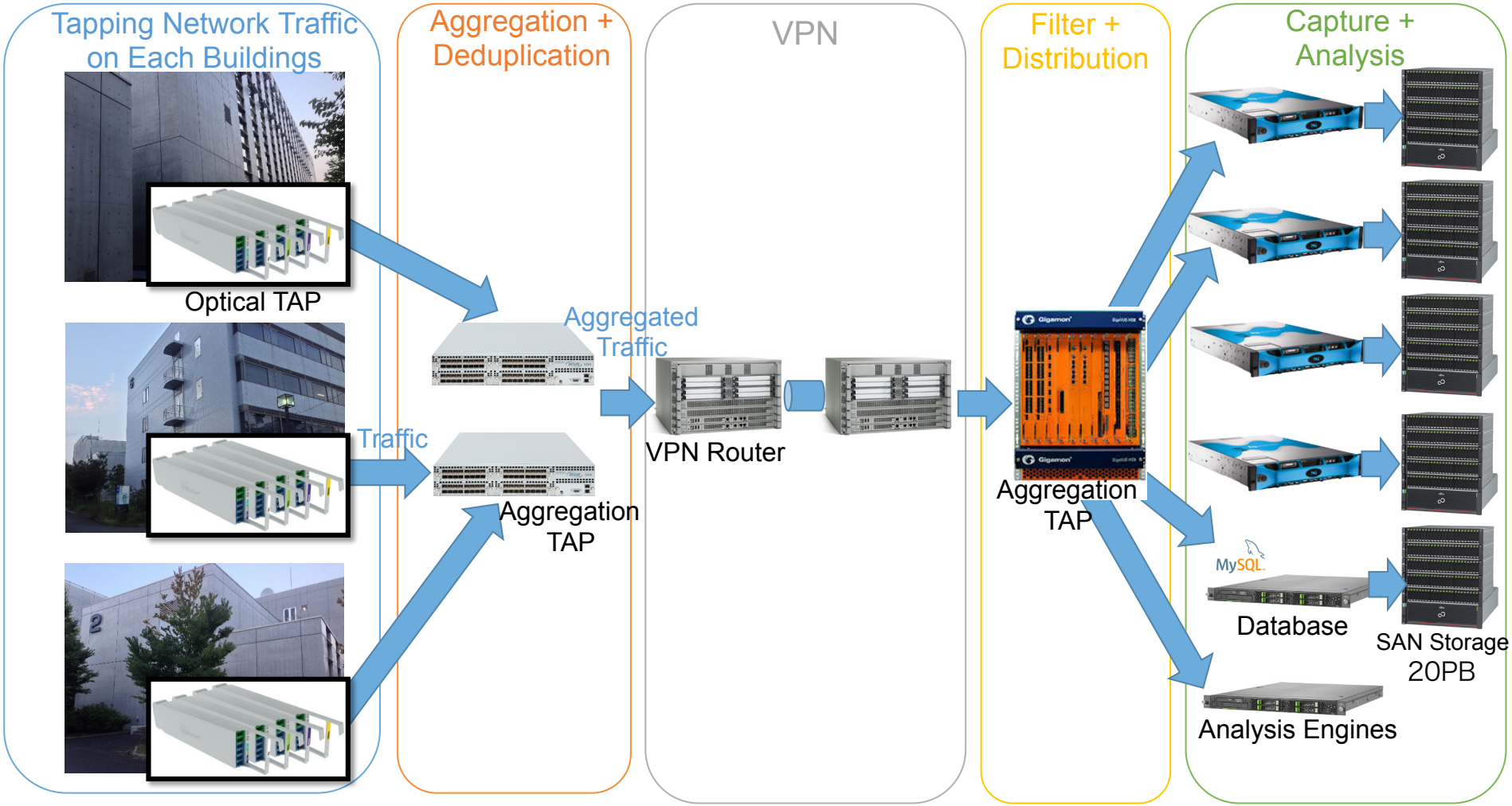
- **対策研究に必要なデータ取得が困難**
  - ✓大規模観測の網にかからない
  - ✓攻撃を受けた組織からデータが出てこない
    - 侵入の痕跡は消されている
    - トラフィックログを長期間保存している組織は稀
    - 組織の秘密情報が含まれるため組織外提供が不可

- **対策検証環境の未整備**
  - ✓攻撃を再現できる検証環境がない
  - ✓攻撃に対抗するための多層防御の検証環境がない



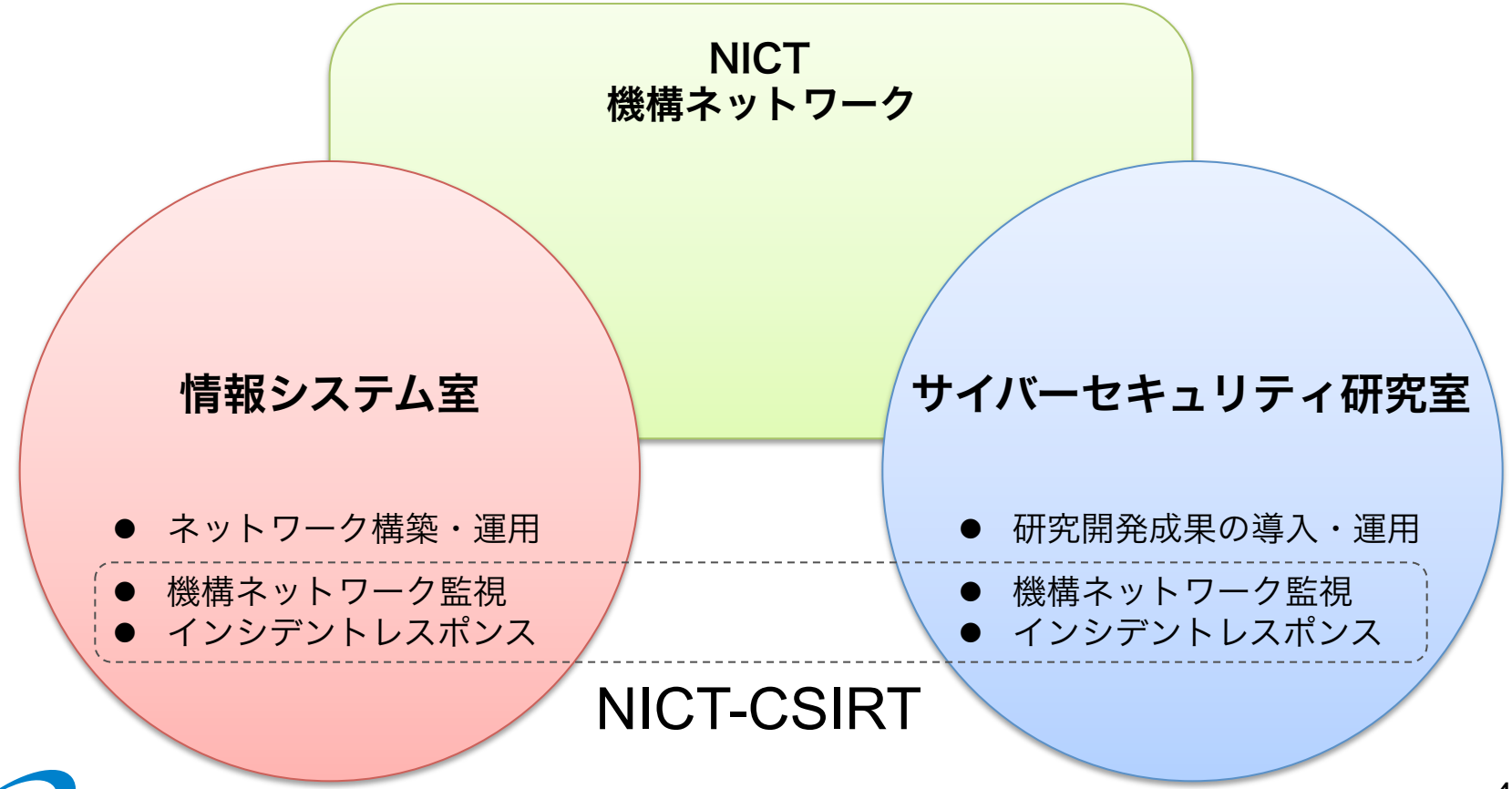
作るしかない！

ライブネット観測・分析機構 構築

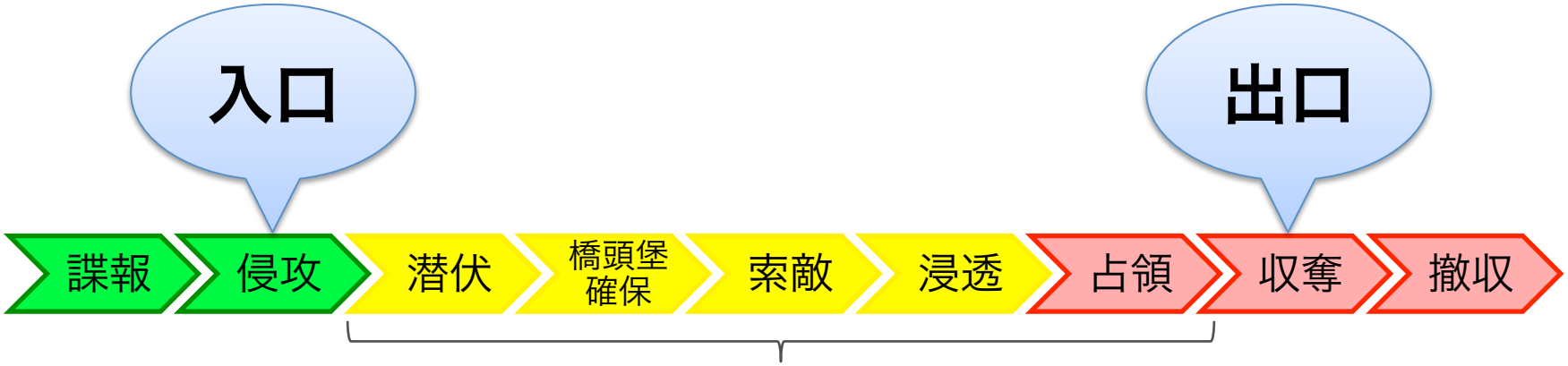


NICT-CSIRT 構築

- NICT内ネットワークを研究開発成果の実践の場に
- 情報システム室と連携しインシデントレスポンス



入口対策/出口対策 ＋ 内部対策



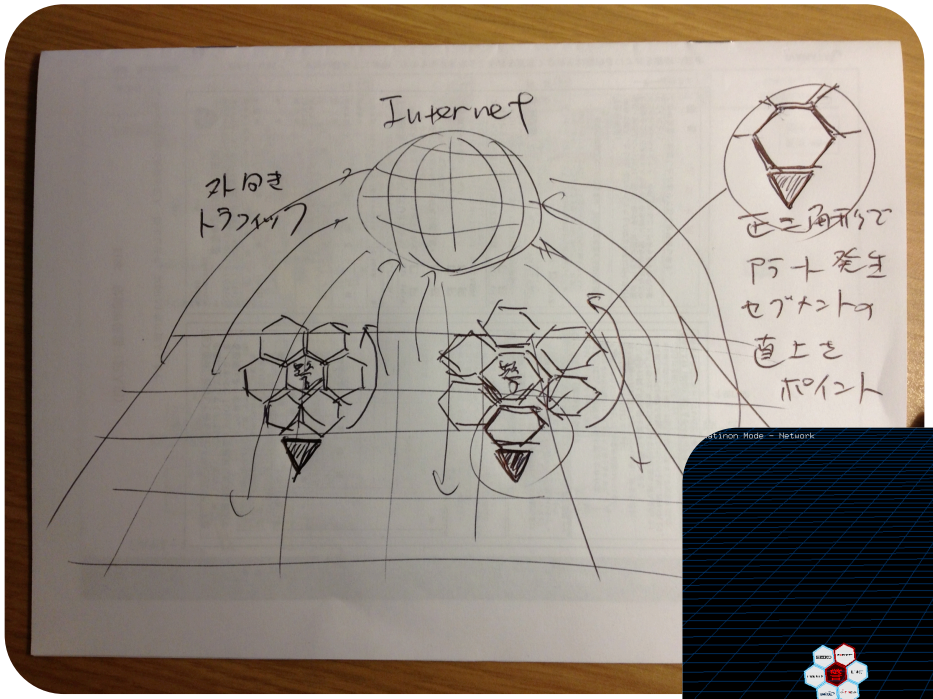
ネットワークの内側でも対策を！

（組織内ネットワークのリアルタイム観測・分析）

NIRVANA改

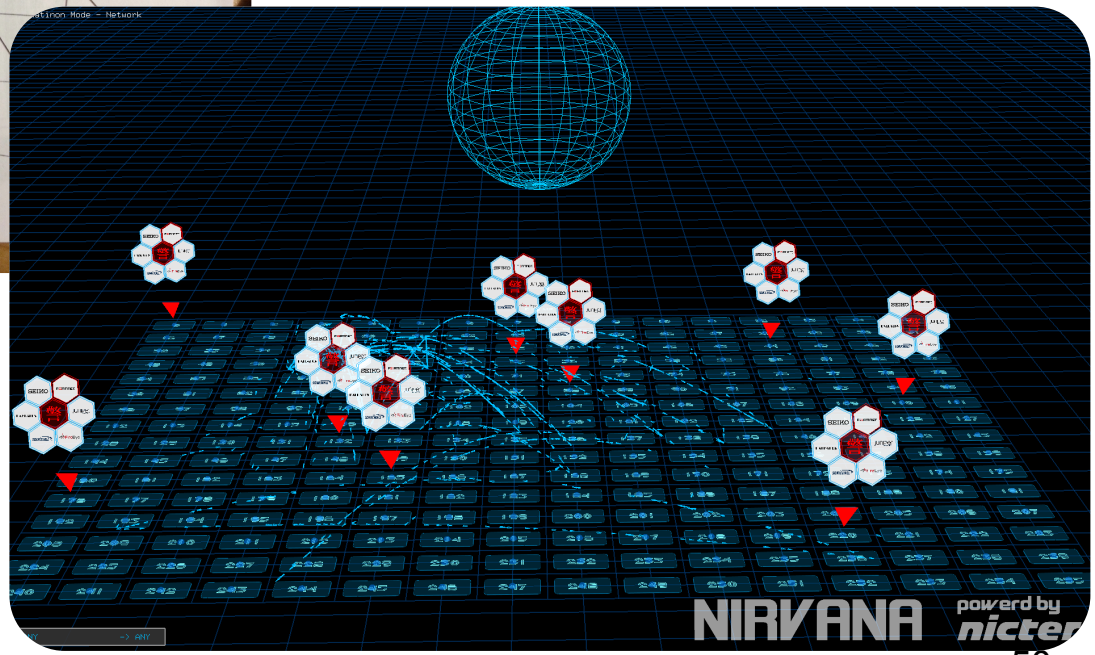
= NIRVANA ＋ セキュリティ分析機能

NIRVANA改 1st スケッチ



23:31:08 (JST)
April 26, 2013

14 Hours Later...

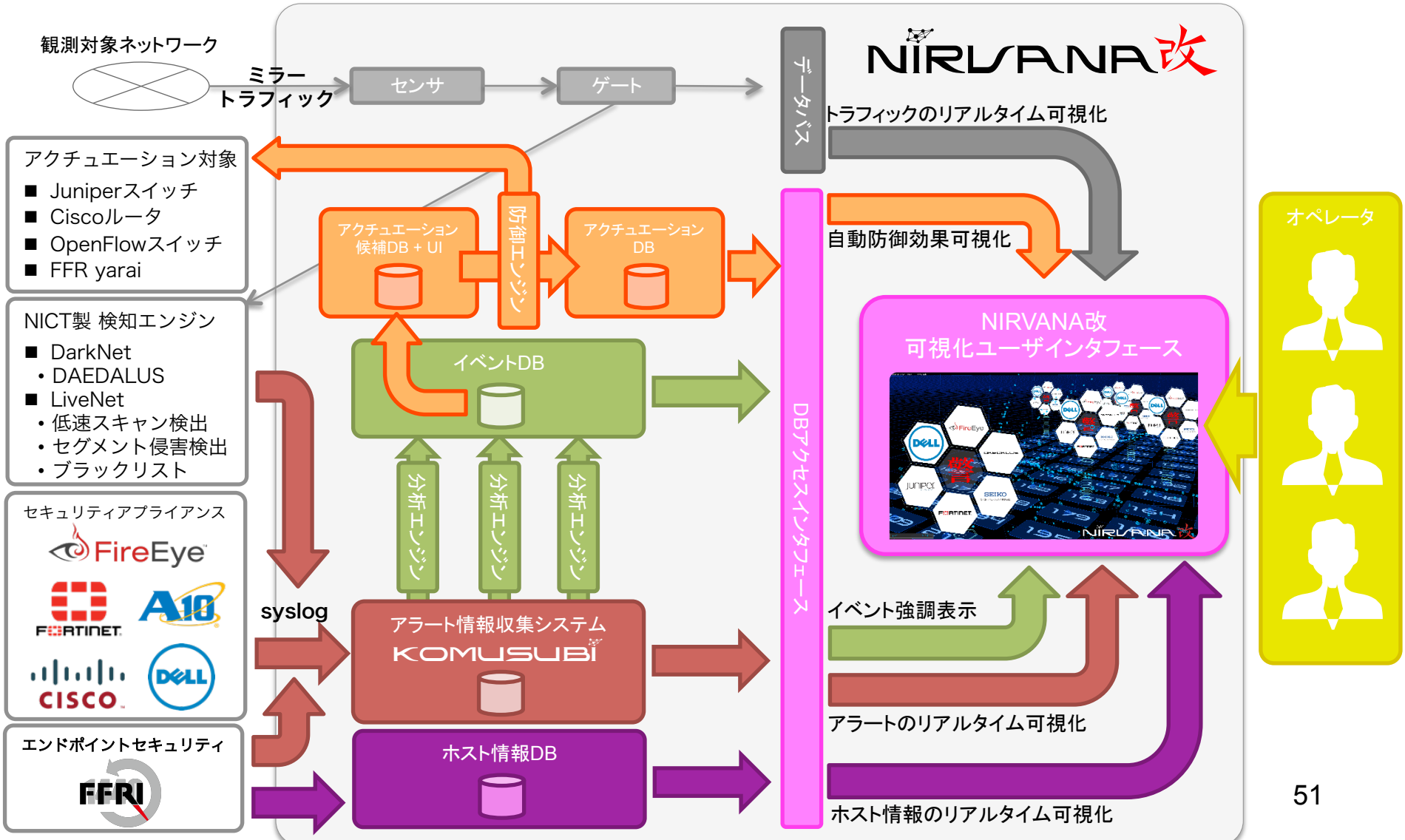


12:54:03 (JST)
April 27, 2013

National Institute of Information and Communications Technology

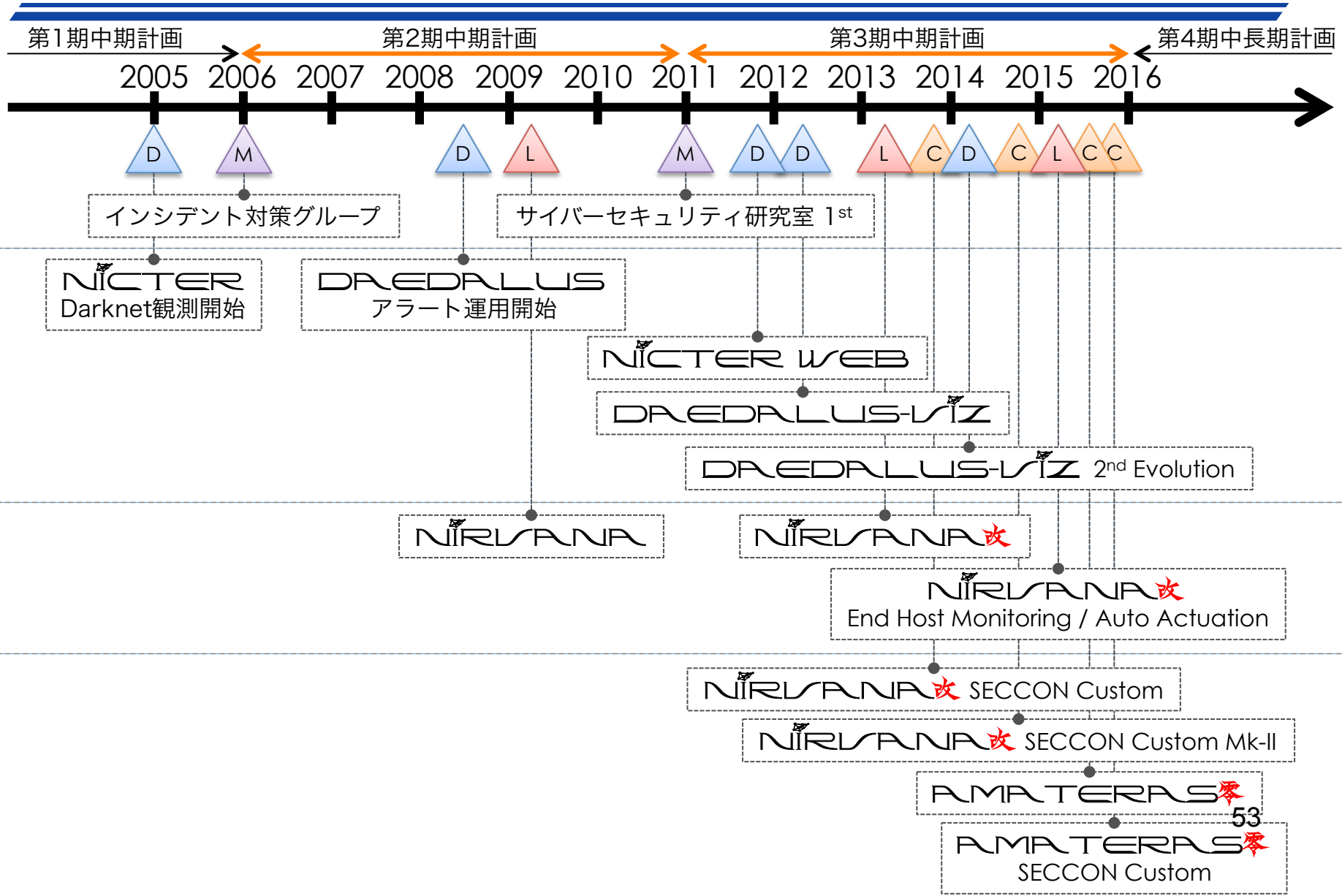
NICTER
Network Incident analysis Center for Tactical Emergency Response

NIRVANA改 システム詳細




[1] ProcTree:[1] Actuation:[1]
0839
NIRVANA 改
paloalto
DELL
TREND MICRO
FORTINET
FFRI
NICT
DETECTOR
警告
ANY
52

NICTERプロジェクト 10年線表



NICTERプロジェクトを育てた言葉 ⑥

オレ、CTFをもっと
格好良くしたいんですよ！

月刊I/O 2014年5月号から抜粋

愛甲健二さん

tessyさん

園田道夫先生

ことの始まり

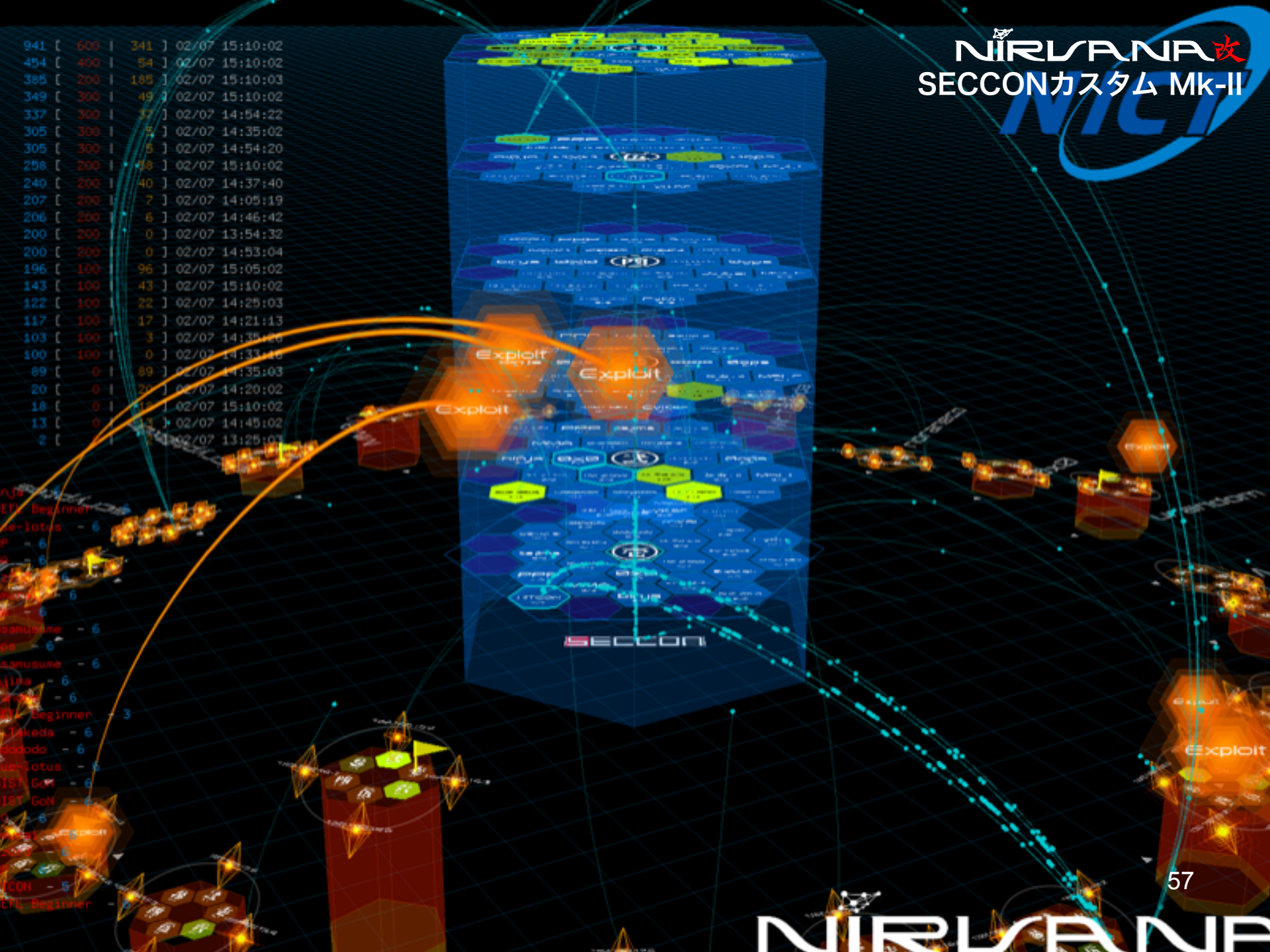
no drink, no hack

2013年夏。とあるキャンプ※の深夜の部で、情報セキュリティコンテストイベントSECCON実行委員の方々とCTF談義に花が咲きました。

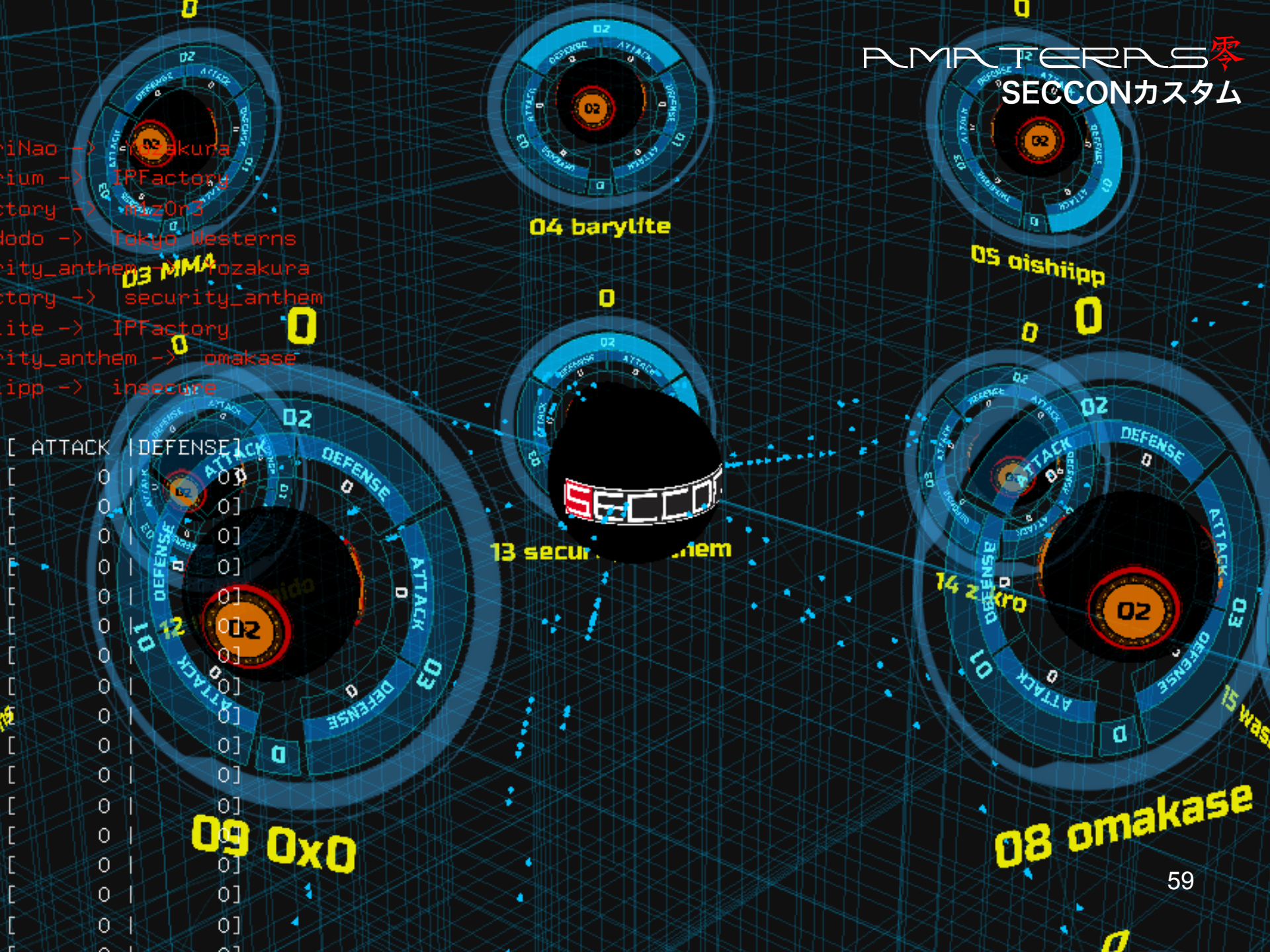
A氏「CTFをもっと格好良くしたいんですよ!」
井上「だったらガチで可視化しましょうか?」
T氏「お!SECCON全国大会可視化しようよ!」
S氏「…（寝落ち中）」
一同「いいねー!カンパーイ!」

※セキュリティ・キャンプ中央大会2013。

CTFの様子（可視化なし）


NIRVANA改
SECCONカスタム Mk-II
941 [600 | 341] 02/07 15:10:02
454 [400 | 54] 02/07 15:10:02
385 [200 | 185] 02/07 15:10:03
349 [300 | 49] 02/07 15:10:02
337 [300 | 37] 02/07 14:54:22
305 [300 | 5] 02/07 14:35:02
305 [300 | 5] 02/07 14:54:20
258 [200 | 58] 02/07 15:10:02
240 [200 | 40] 02/07 14:37:40
207 [200 | 7] 02/07 14:05:19
206 [200 | 6] 02/07 14:46:42
200 [200 | 0] 02/07 13:54:32
200 [200 | 0] 02/07 14:53:04
196 [100 | 96] 02/07 15:05:02
143 [100 | 43] 02/07 15:10:02
122 [100 | 22] 02/07 14:25:03
117 [100 | 17] 02/07 14:21:13
103 [100 | 3] 02/07 14:35:26
100 [100 | 0] 02/07 14:33:16
89 [0 | 89] 02/07 14:35:03
20 [0 | 20] 02/07 14:20:02
18 [0 | 18] 02/07 15:10:02
13 [0 | 13] 02/07 14:45:02
2 [0 | 2] 02/07 13:25:03
Exploit
Exploit
Exploit
SECCON
Exploit
Exploit
57
NIRVANA


Information and
Communications
Technology
idee - CRYPTO 100
mmmnmy - BINARY 200
m - [20]
ps - [30]
FORENSICS
300
NET
25 mmmnmy


AMATERAS 零
SECCONカスタム
04 barylite
05 oishiipp
03 MMA
09 0x0
08 omakase
13 secu hem
14 z kro
12
15 was
[ATTACK |DEFENSE]
ATTACK
DEFENSE

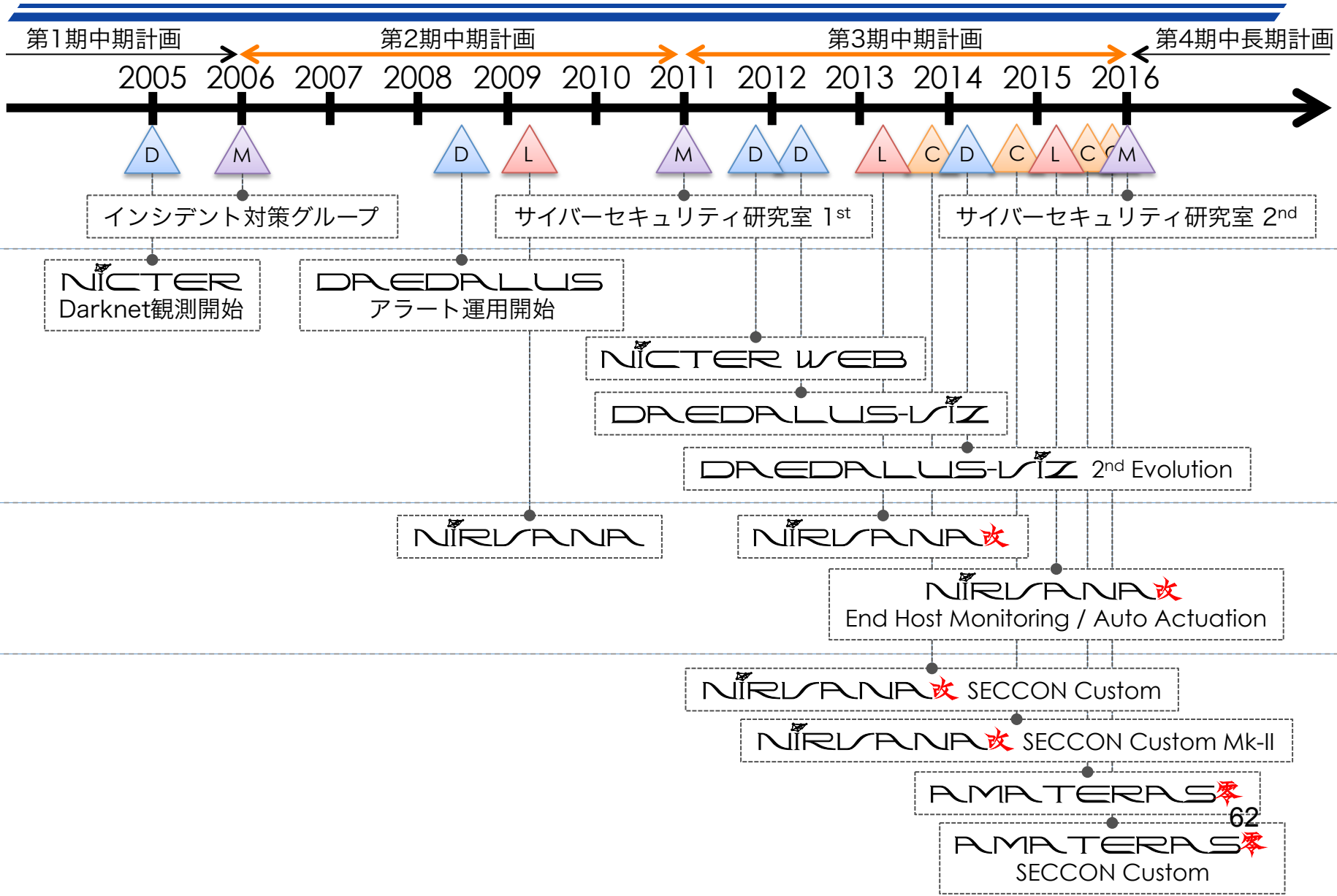
NICTERプロジェクトを育てた言葉 ⑦

日本の政府機関こそ
日本の最新技術で守る

まとめ

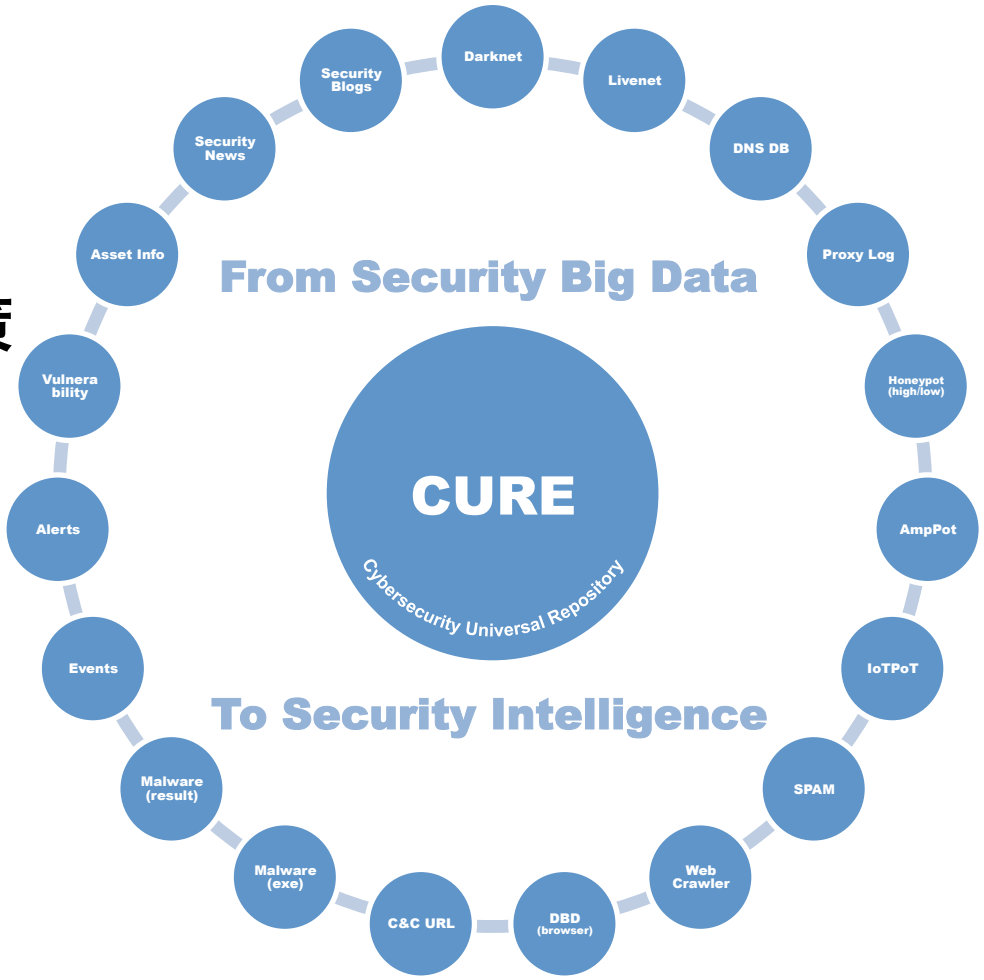
- セキュリティ業界に流れるそれらしい説は、結構外れることも多い
- 研究者はデータを見て検証すること！
- 日本の優位性・特異性を活かした研究開発
- サイバーセキュリティはデータが命

NICTERプロジェクト 10年線表



データを核としたセミ・オープン研究基盤

- **セキュリティ関連情報を大規模集約**
  - ✓ 各種観測情報
  - ✓ マルウェア検体/解析結果
  - ✓ セキュリティ機器のアラート情報
  - ✓ 脆弱性情報、資産情報
  - ✓ セキュリティNews/Blog etc...
- **マッシュアップと自動対策**
  - ✓ 複数情報源の紐付け
  - ✓ 攻撃キャンペーンの解明
  - ✓ 組織やユーザへの自動対策展開
- **セミ・オープン研究基盤**
  - ✓ CURE格納情報の外部研究利用
  - ✓ 機微情報への階層的アクセス制御
  - ✓ CUREを核にしたAll Japan体制のサイバーセキュリティ研究基盤創立



National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response