2017年5月31日 サイバーセキュリティタスクフォース

資料５－２

NICTにおける サイバーセキュリティ研究開発の 取組について

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
井上 大介

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

サイバーセキュリティ分野の研究開発体制

NICT 第4期中長期計画

1-4. サイバーセキュリティ分野

(1) サイバーセキュリティ技術

(ア) アドバンスト・サイバーセキュリティ技術
(イ) サイバーセキュリティ・ユニバーサル・リポジトリ技術

(2) セキュリティ検証プラットフォーム構築活用技術

(ア) 模擬環境・模擬情報構築活用技術
(イ) セキュリティ・テストベッド技術

(3) 暗号技術

(ア) 機能性暗号技術
(イ) 暗号技術の安全性評価
(ウ) プライバシー保護技術

NICT 組織体制

サイバーセキュリティ研究所
宮崎 哲弥 所長
中尾 康二 主管研究員

サイバーセキュリティ研究室
（小金井＋北陸）

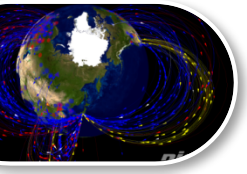
井上 大介 室長

セキュリティ基盤研究室
（小金井）

盛合 志帆 室長

サイバーセキュリティ研究室 研究マップ

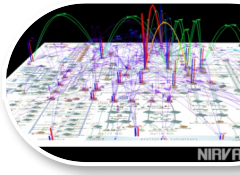
Passive



インシデント分析センタ
NICTER
（ニクター）

対サイバー攻撃アラートシステム
DAEDALUS
（ダイダロス）

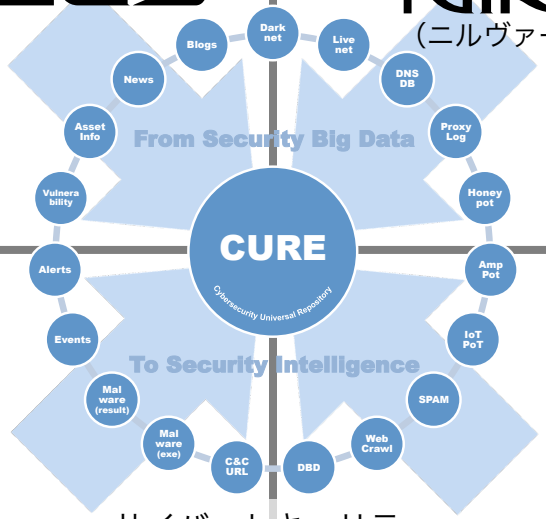
ネットワーク可視化システム
NIRVANA
（ニルヴァーナ）



サイバー攻撃統合分析プラットフォーム
NIRVANA改
（ニルヴァーナ・カイ）

Global

Local



リフレクション攻撃専用ハニーポット
AmpPOT※

IoTマルウェア専用ハニーポット
IoTPOT※

サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

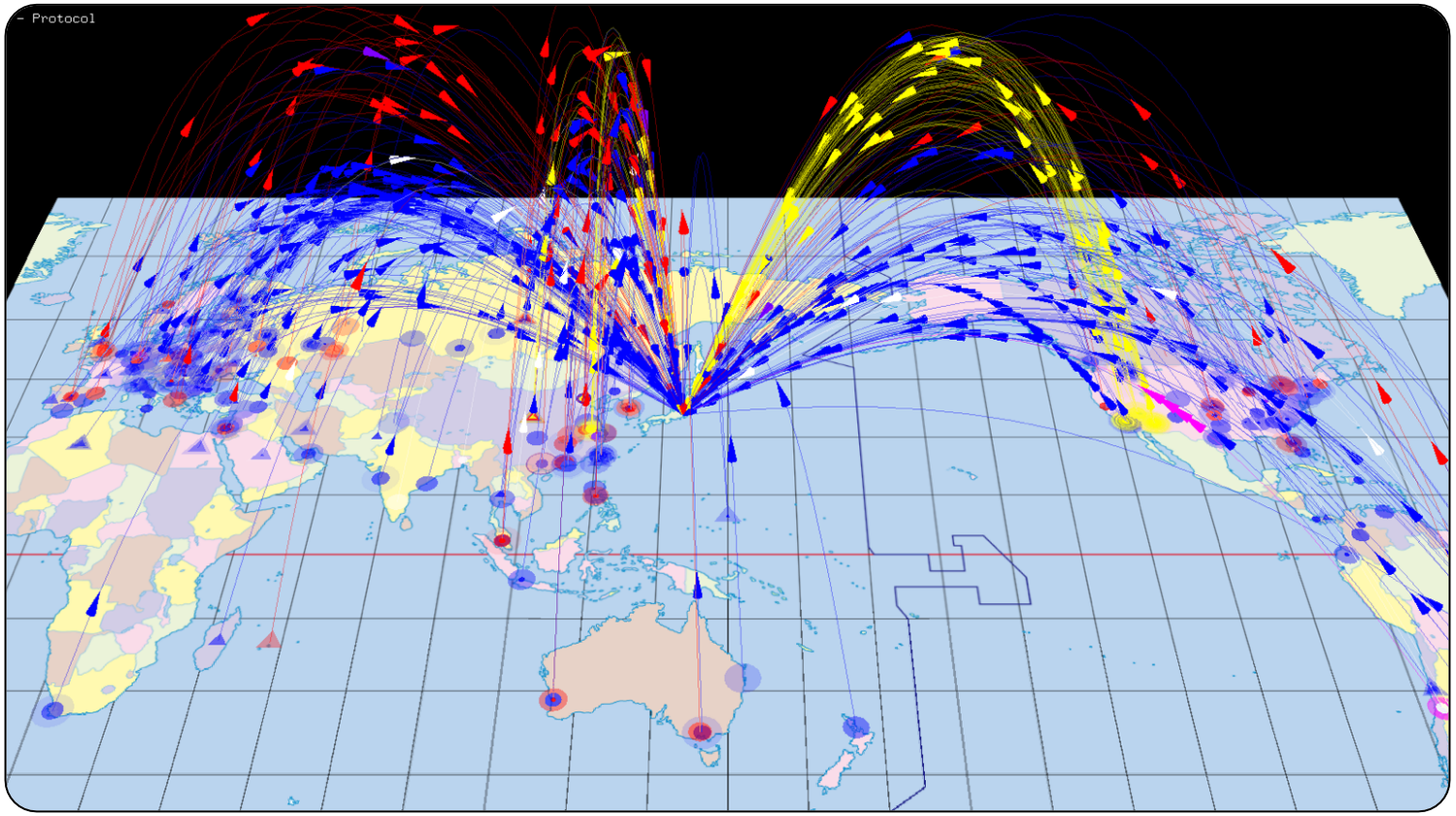
Active

※横浜国立大学/独Saarland大との共同研究

インシデント分析センタ（ニクター）

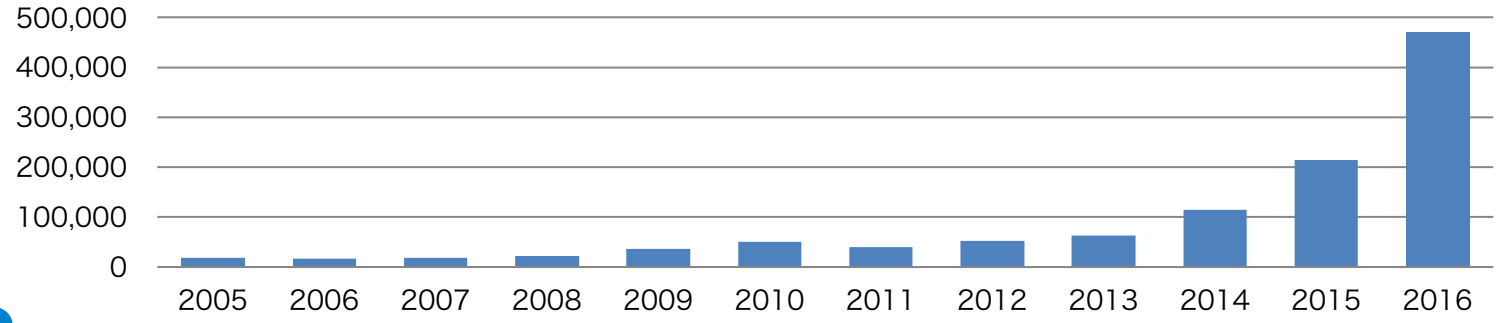
NICTER

- 大規模サイバー攻撃観測・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
- 無差別型攻撃の大局的な傾向把握に有効



NICTER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
2016	**約1,281億**	約30万	**469,104**



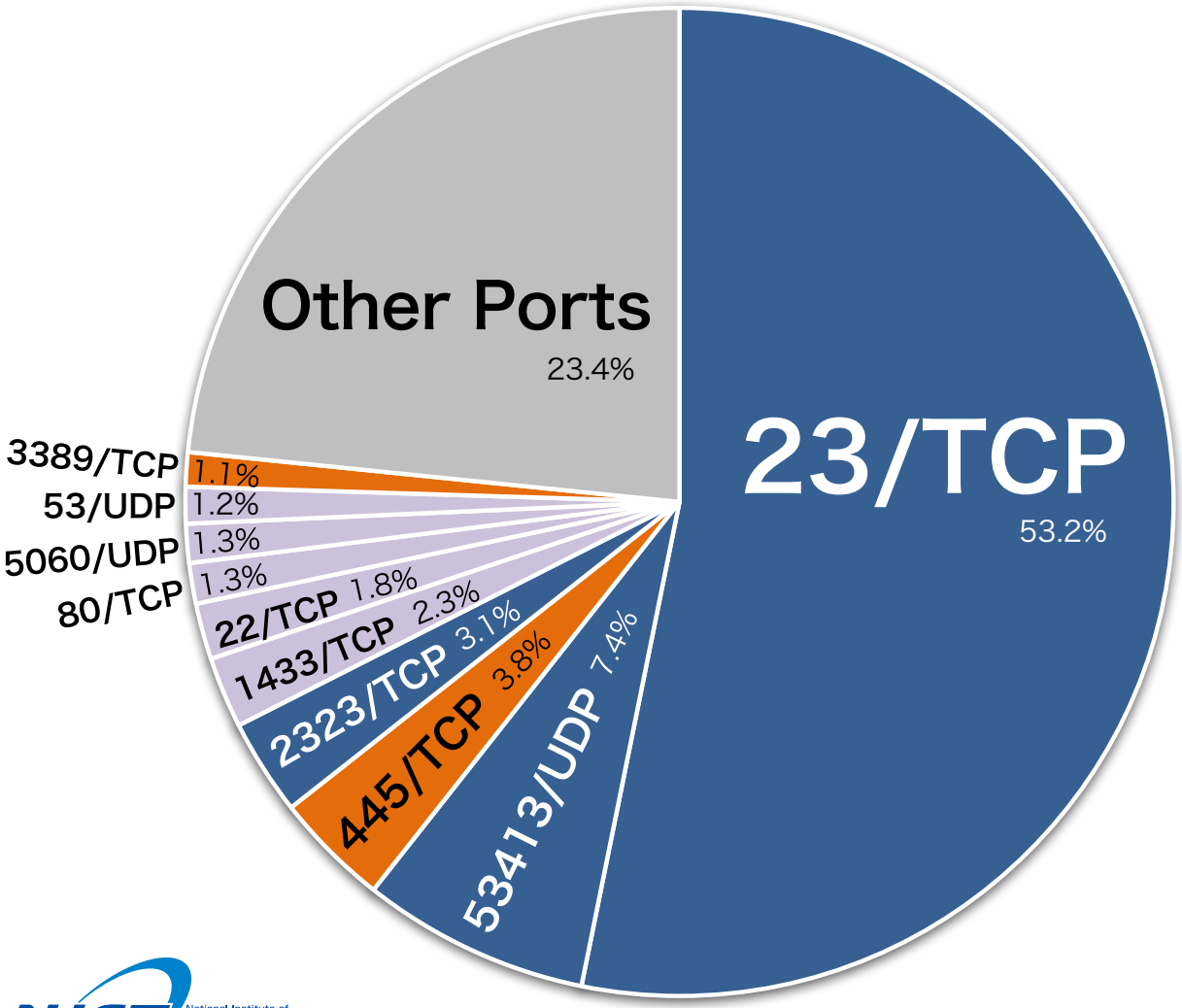
1 IPアドレス当たりの年間総観測パケット数

National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

感染機器の分布（2016年）

- 宛先ポート番号別パケット数分布 -



ポート番号	攻撃対象
23/TCP	IoT機器 （Webカメラ等）
53413/UDP	IoT機器（中国製ルータ）
445/TCP	Windows（サーバサービス）
2323/TCP	IoT機器 （Webカメラ等）
1433/TCP	データベースサーバ（SQL）
22/TCP	リモート認証サーバ（SSH）
80/TCP	Webサーバ（HTTP）
5060/UDP	IP電話サーバ（SIP）
53/UDP	名前解決サーバ（DNS）
3389/TCP	Windows画面共有（RDP）

NICTER観測情報の利活用

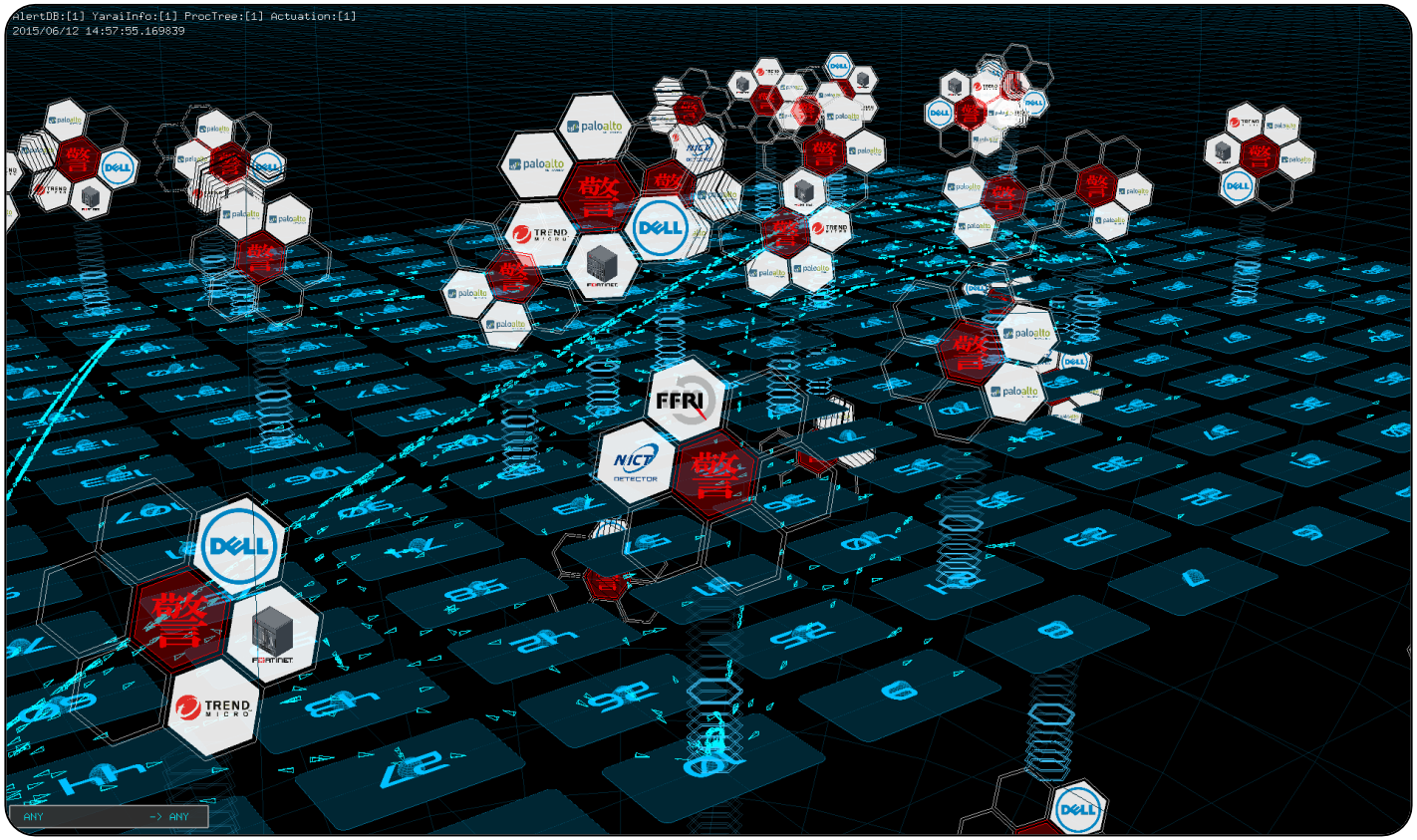
- **セキュリティ関連組織への観測情報提供**
  - ✓ **SIGMON**（定点観測友の会）
    - JPCERT/CC、IPA、@Police等との観測結果共有（2004年～）
  - ✓ **ICT-ISAC Japan**（DoS攻撃即応-WG）
    - DoS攻撃関連情報共有（2011年～）
  - ✓ **ACTIVEプロジェクト**（総務省）
    - ISPに感染端末情報提供→ユーザへの注意喚起（2014年～）
  - ✓ **オリパラ体制検討会**（NISC、オリパラ組織委員会、関連組織、他）
    - DoS攻撃関連情報共有（2015年～）

- **観測情報一般公開**
  - ✓ NICTERWEBでのリアルタイム公開（http://www.nicter.jp）
  - ✓ NICTER観測レポート（http://www.nict.go.jp/cyber/report.html）

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

- 標的型攻撃に対抗するための統合分析プラットフォーム
- 組織の末端までセンサを設置しトラフィック観測・分析
- セキュリティ機器からの膨大なアラートを管理を効率化



NIRVANA改 2016

- **セキュリティオーケストレーション**@Interop Tokyo 2016
- アラート連携：**19機種**、アクチュエーション連携：**8機種**

【アラート連携】

- FFRI yarai (FFRI)
- iNetSec Intra Wall (PFU)
- AX260A (AlaxalA Networks)
- Livenet Analyzer (NICT)
- DAEDALUS (NICT)
- DDI-4100 (Trend Micro)
- SRX1500 (Juniper Networks)
- FP 4120 (Cisco)
- PA 7050 (Palo Alto Networks)
- PA 5060 (Palo Alto Networks)
- FG-3815D (Fortinet)
- FG-3200D (Fortinet)
- FS-3000D (Fortinet)
- FA-3900E (Fortinet)
- Lastline Enterprise (Lastline)
- ThreatARMOR (Ixia)
- Damballa (Damballa)
- Thunder5435 (A10)
- SonicWALL SuperMassive 9800 (DELL)

【アクチュエーション連携】

- FFRI yarai (FFRI)
- iNetSec Intra Wall (PFU)
- AX3650S (AlaxalA Networks)
- SRX1500 (Juniper Networks)
- FortiGate 3200D (Fortinet)
- PA 7050 (Palo Alto Networks)
- ThreatArmor (Ixia)
- Flowspec Server (Interop NOC)

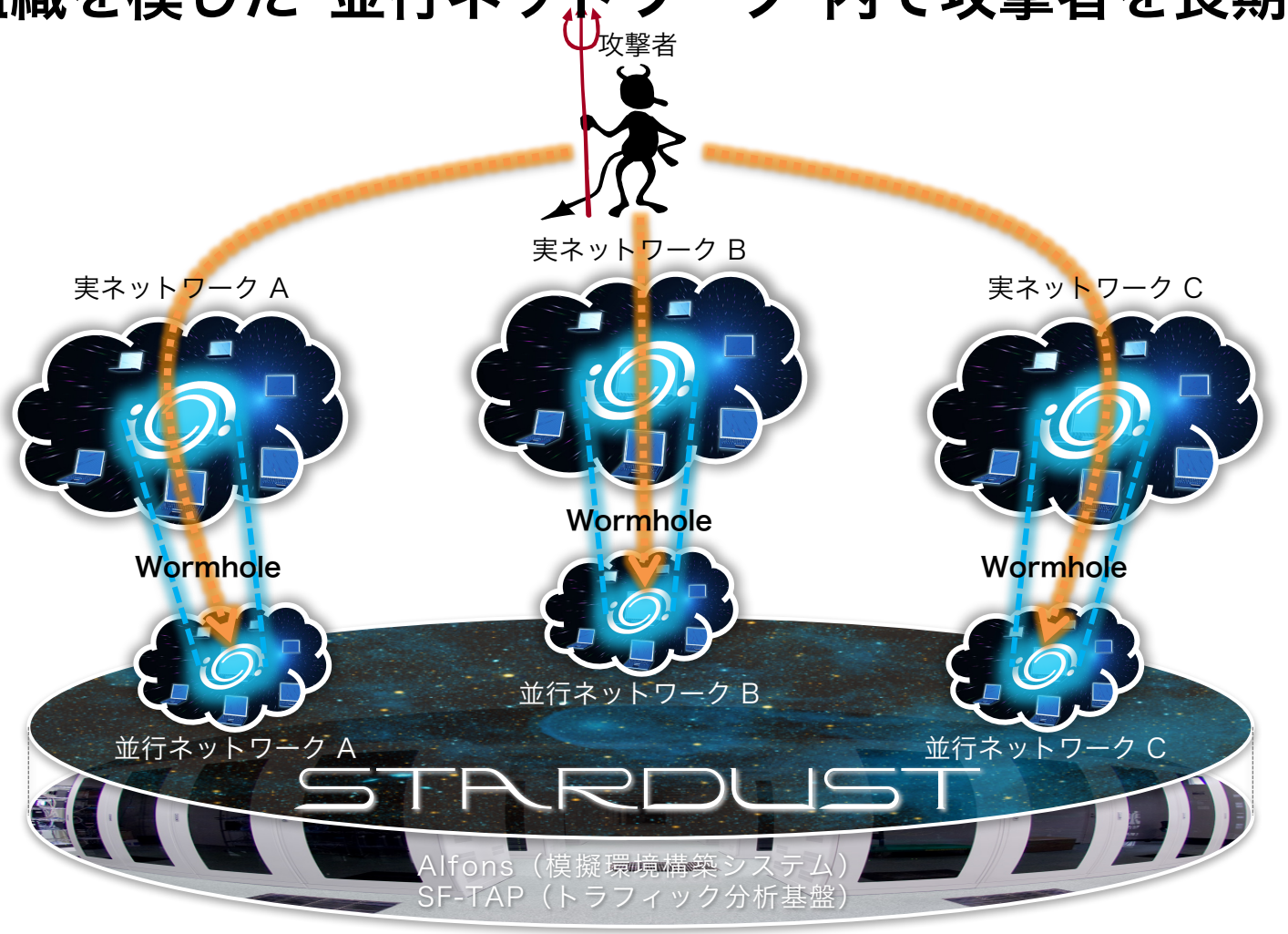
NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

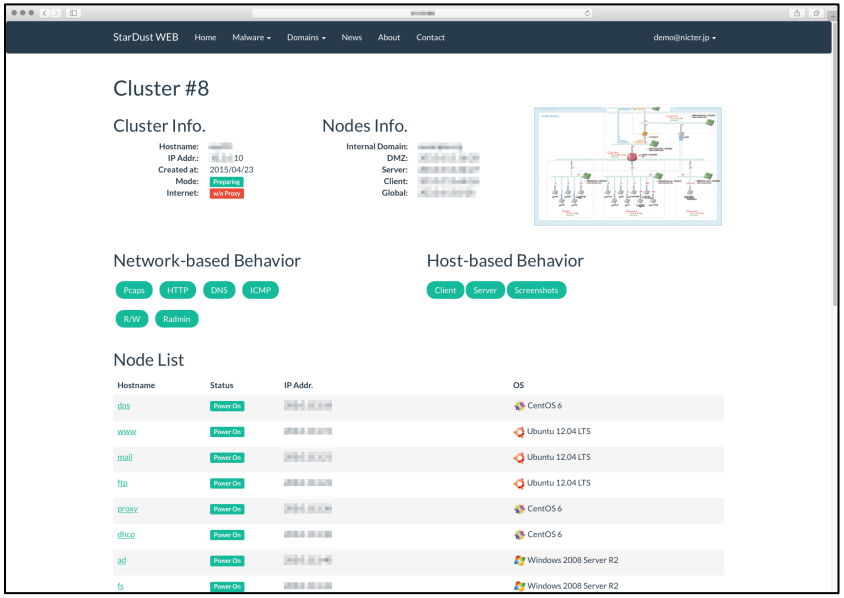
サイバー攻撃誘引基盤（スターダスト）

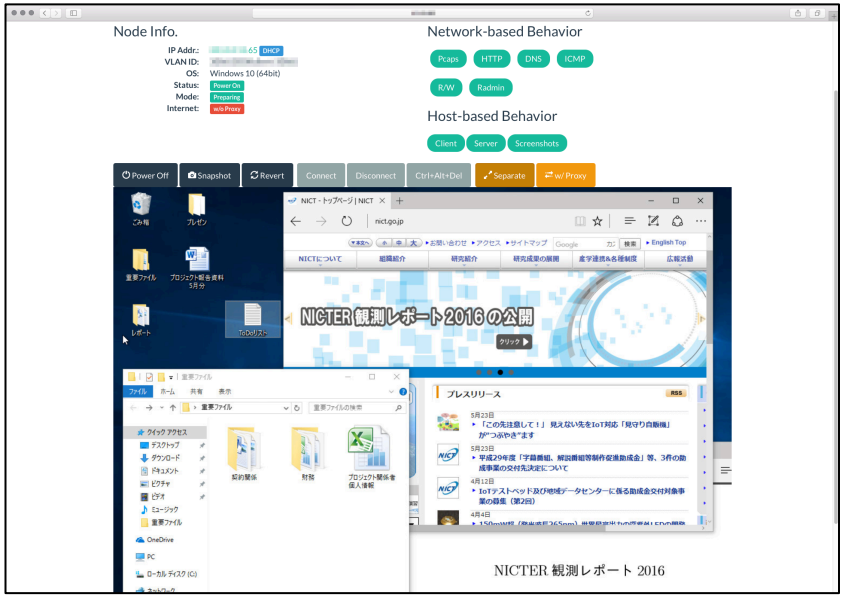
STARDUST

- 標的型攻撃等の攻撃者を誘い込む**サイバー攻撃誘引基盤**
- 組織を模した“並行ネットワーク”内で攻撃者を長期分析



STARDUST
- 並行ネットワークと模擬ノード -





- **並行ネットワーク**
  - ✓ 政府や企業等を精巧に模した模擬環境
  - ✓ 各種サーバやPCが数十台～数百台稼働
  - ✓ 数十の並行ネットワークを同時稼働可能
- **模擬ノード**
  - ✓ 並行ネットワーク内で稼働するPC端末
  - ✓ 組織の情報資産を模した模擬情報を配置
  - ✓ 模擬ノード内外の挙動をステルスに観測

標的型攻撃をリアルタイムに観測・分析可能に

サイバーセキュリティの研究開発における
NICTの役割

- **中長期的・高リスクな研究開発**
  - ✓ NICTER: 2005年から約12年間観測継続（Blaster → IoTマルウェア）
  - ✓ STARDUST：着想から実現までに5年以上
- **中立性を活かした研究開発**
  - ✓ ダークネット観測網：国内外の複数の協力機関が30万のIPアドレスを提供
  - ✓ NIRVANA改：複数ベンダを連携させる統合分析プラットフォーム
- **研究開発成果の確実な社会還元**
  - ✓ NICTER、DAEDALUS、NIRVANA改：研究開発成果はほぼ全て実用化
  - ✓ CURE：産学へのセミ・オープンなデータ提供
- **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