サイバーセキュリティ領域におけるＮＩＣＴの取り組み

インシデント分析センター

NICTER とそのスピンオフ技術

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の研究開発における

NICTのミッション

● 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

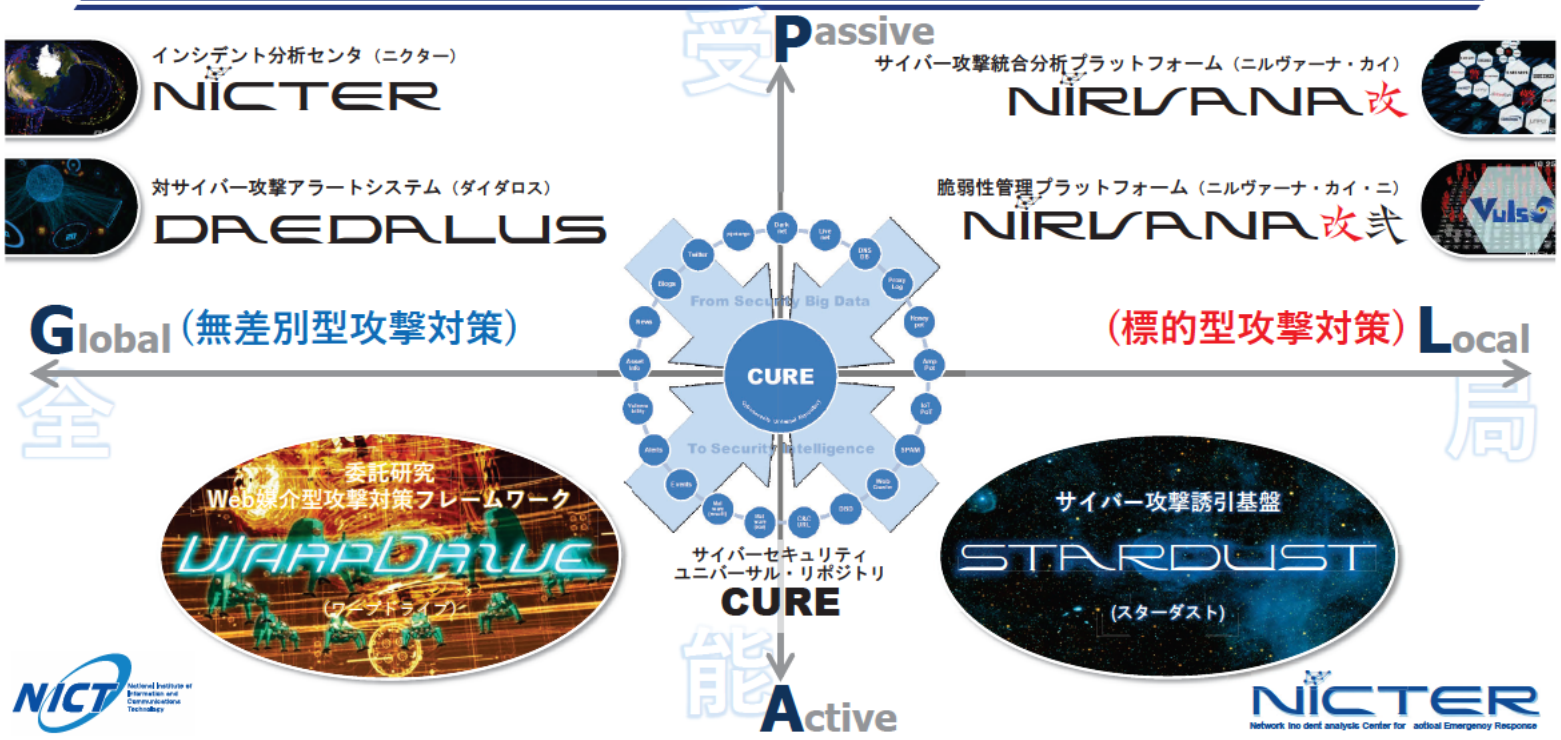
● 研究開発成果の確実な社会還元

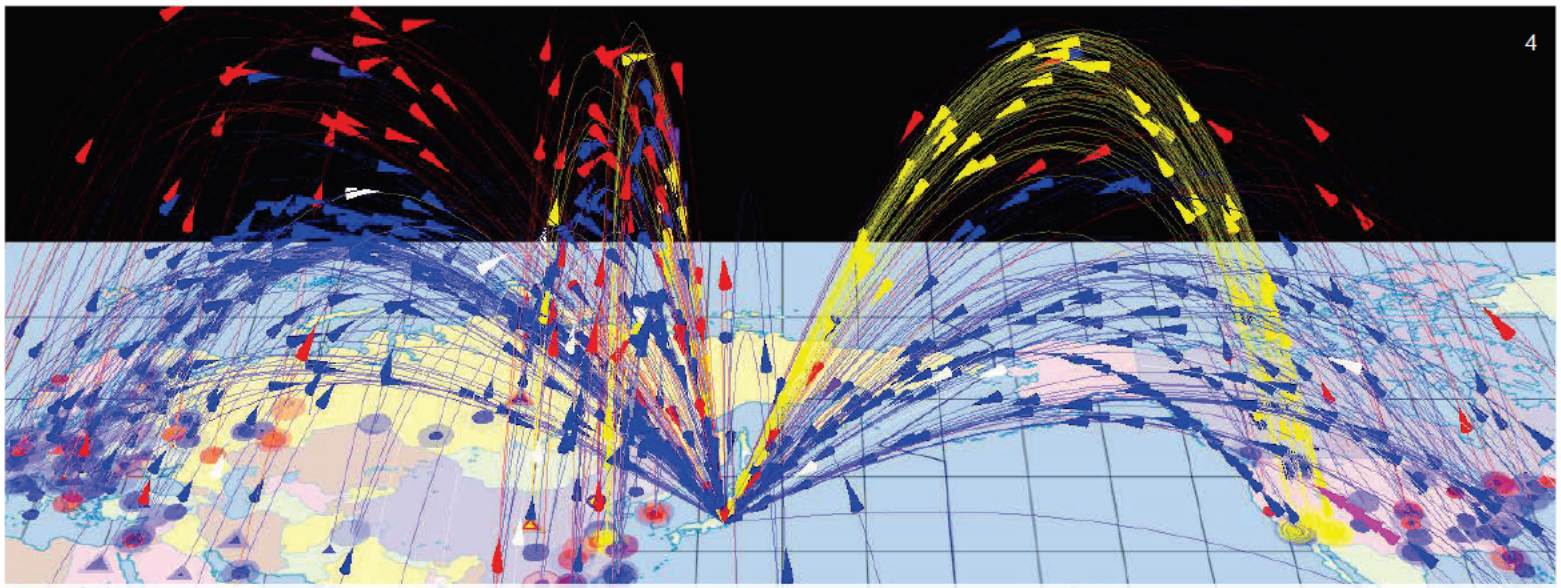
- ✓ NICTER、DAEDALUS、NIRVANA改：研究開発成果はほぼ全て実用化
- ✓ CURE：産学へのセミ・オープンなデータ提供

● 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

サイバーセキュリティ研究室 研究マップ



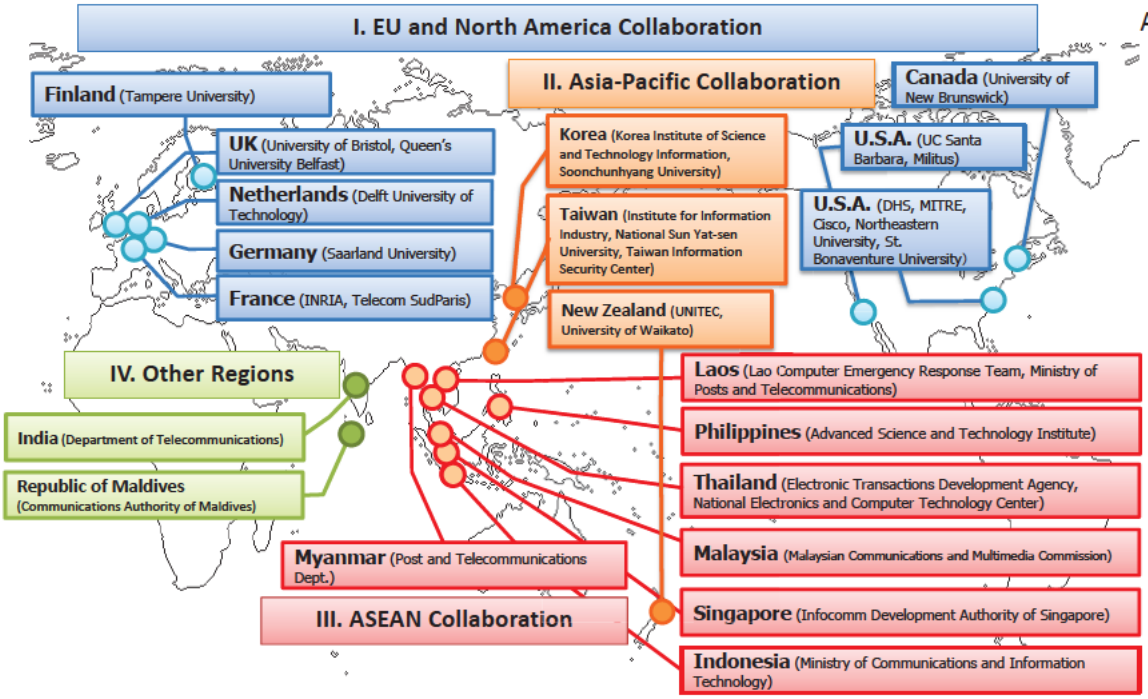


NICTER

- 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

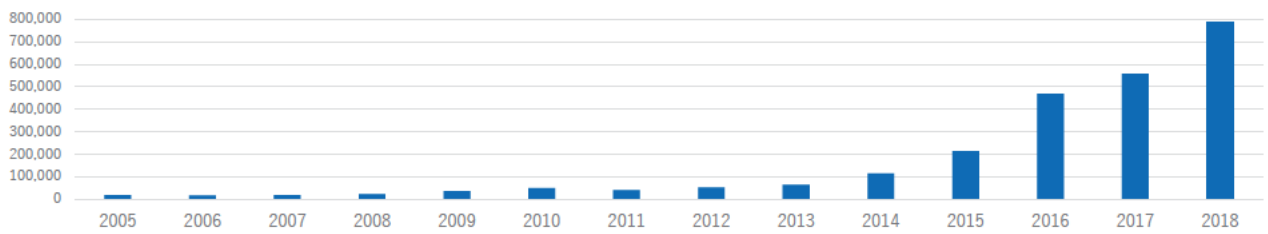
NICTERプロジェクト 国際連携マップ

As of April 2019



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

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 -

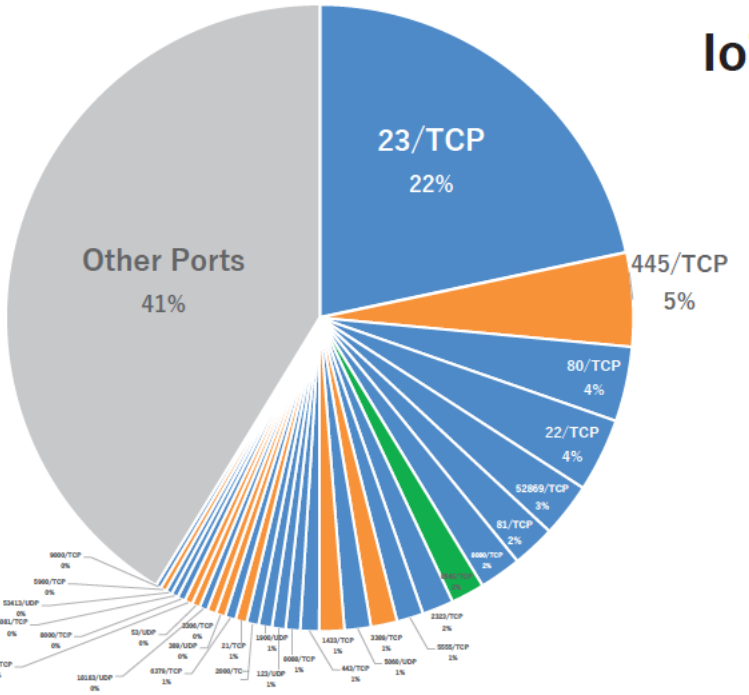
- **Surveillance camera**
  - IP camera
  - DVR
- **Network devices**
  - Router, Gateway
  - Modem, bridges
  - WIFI routers
  - Network mobile storage
  - Security appliances
- **Telephone**
  - VoIP Gateways
  - IP Phone
  - GSM Routers
  - Analog phone adapters
- **Infrastructures**
  - Parking management 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 -

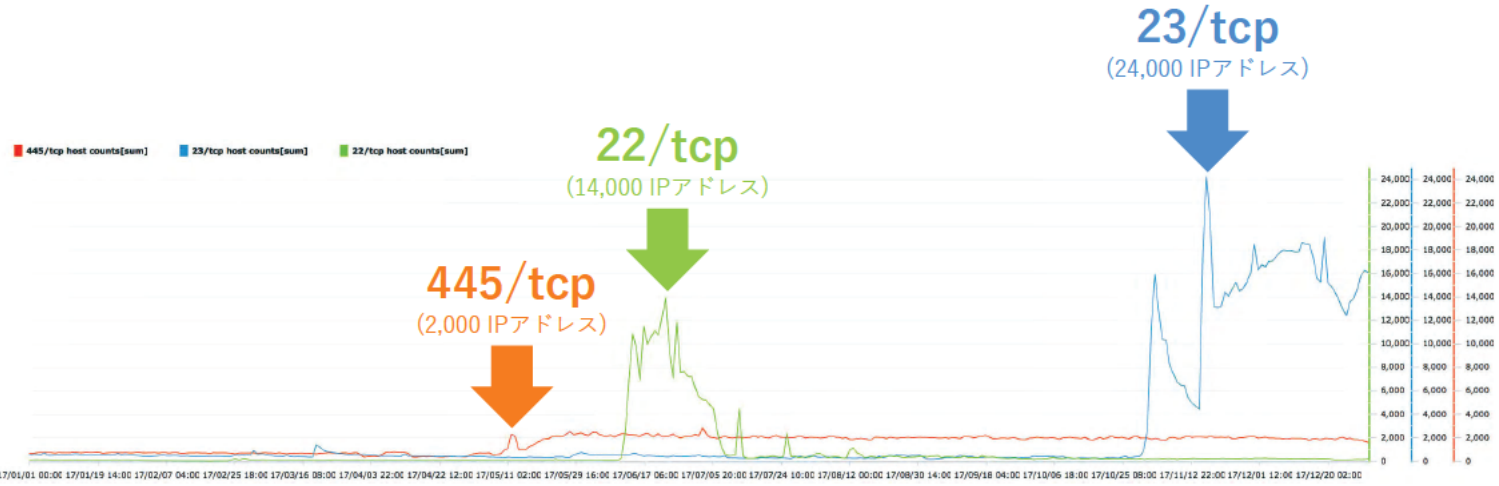


IoT ＝ **47.7%**（上位30ポート中）

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）
- **22/tcp (SSH)**
  - ✓ 2017年6月～
  - ✓ 国内モバイルルータ
- **23/tcp (telnet)**
  - ✓ 2017年11月～
  - ✓ 国内ホームルータ

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

出典：週刊アスキー
http://weekly.ascii.jp/elem/000/000/404/404196/

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 -

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～）
- ✓ サイバーセキュリティ協議会（NISC、関連組織、他） 新
  - 第二類構成員として参画（2019年～）

NICTERWEB 弐

● 観測情報一般公開

- ✓ NICTER Web (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)

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

境界防御技術とDAEDALUS

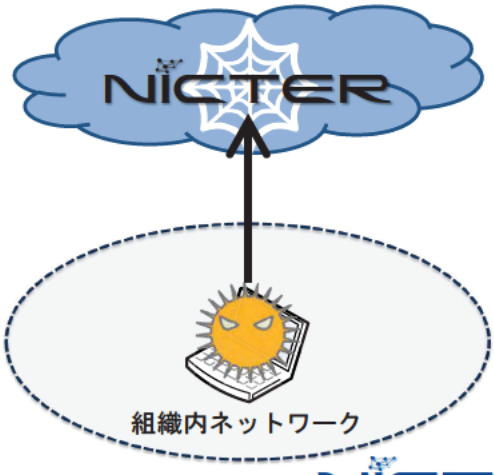
境界防御技術（従来技術）

組織外からの攻撃をネットワーク境界で検出

相補的

DAEDALUS

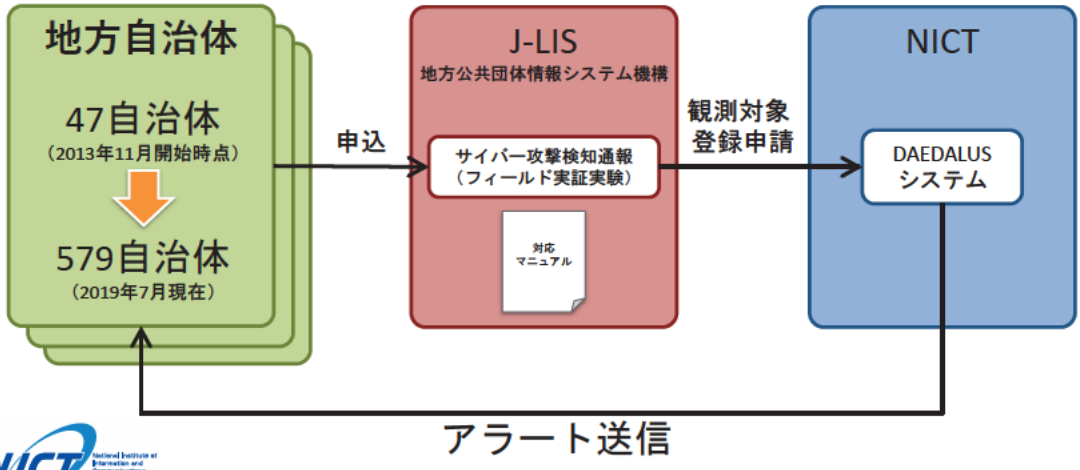
組織内からの攻撃をネットワーク広域で検出



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

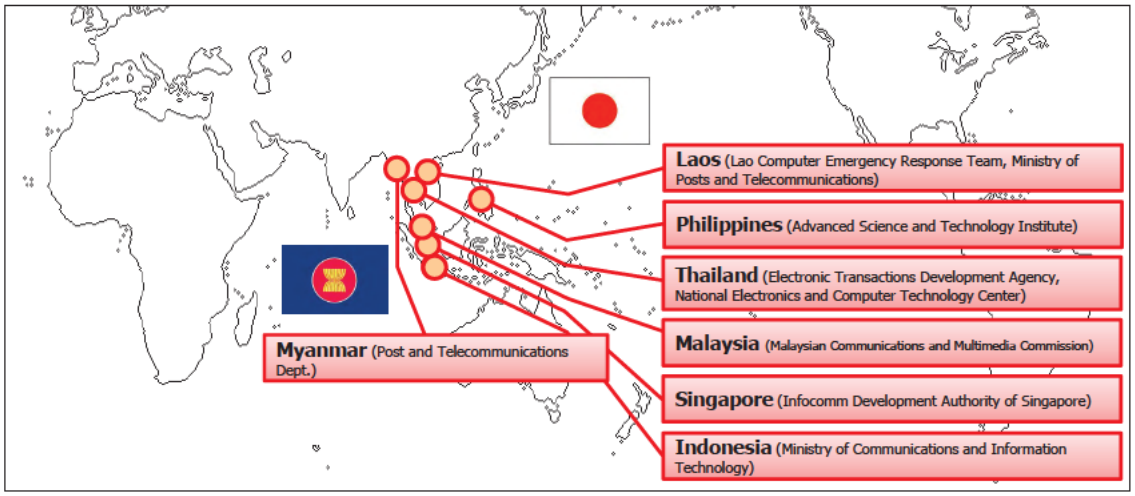


サイバー攻撃検知通報

DAEDALUSの成果展開：国際展開

ASEAN諸国へのアラート提供

- **JASPER：Japan-ASEAN Security Partnership**
  - ✓日・ASEANの技術協力強化プロジェクト※
  - ✓2013年よりASEAN諸国へのDAEDALUSアラート提供を開始



※2013年9月「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」の共同閣僚声明に基づく。

DAEDALUSの成果展開：商用展開

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』

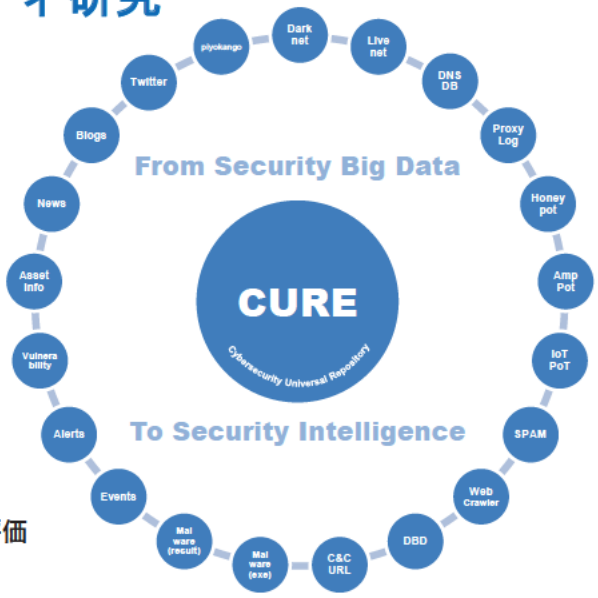
サイバーセキュリティの研究開発における
今後の重点課題

● 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



NICTER
Network Inc dent analysis Center for aotical Emergency Response

---

サイバーセキュリティ人材の育成

・多様化・悪質化するサイバー攻撃に対抗し、社会の安全を守っていくには、その担い手となるサイバーセキュリティ人材の育成を一層加速することが必要
・研究成果や技術的知見を最大限に活用することにより、実践的なサイバートレーニングを企画・推進する組織「ナショナルサイバートレーニングセンター」を設置（平成29年4月1日）

実践的サイバー防御演習（CYDER）

東京2020大会に向けた人材育成（サイバーコロッセオ）

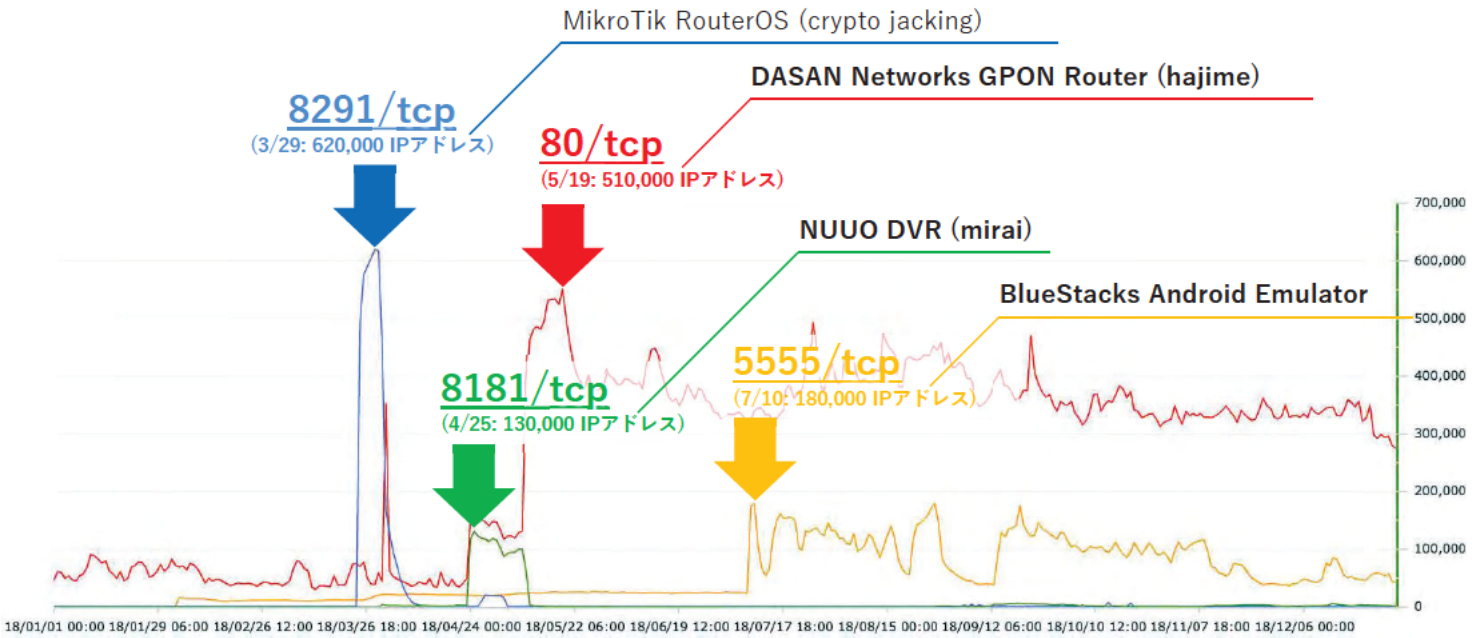
若手セキュリティイノベーター育成プログラム（SecHack365）

2018年度

初級レベルと中級レベルの演習を47都道府県で107回開催し、2,666名が参加	演習（初級・中級・準上級コース）、カレッジ、合わせて22回開催し、延べ484名が参加	25歳以下を対象に1年間かけてセキュリティ開発技術を指導。345名応募、46名が修了

【補足資料】

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）

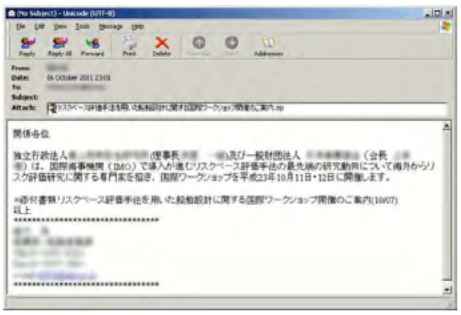
サイバー攻撃誘引基盤

STARDUST

標的型攻撃

- 特定組織を標的にした長期に渡る執拗なサイバー攻撃
- 周到な内容のメールに添付されたマルウェアで組織に侵攻
- 組織内ネットワークに潜伏・浸透し重要情報を収奪

標的型攻撃のCyber Kill Chain



TECH.ASCII.jp「9.5社に1社が対象に！シマンテックが明かす日本の標的型攻撃」
http://ascii.jp/elem/000/000/652/652712/ （2011-11-30）

標的型攻撃研究の難しさ（2011年当時）

- **標的型攻撃の実データが集まらない！**
  - ✓NICTERのような大規模観測網に掛からない
  - ✓攻撃を受けた被害組織からデータが出てこない
    - ログを長期間保存していない
    - ログが攻撃者に消されている
    - ログが存在しても機微情報が含まれ提供不可
  - ✓マルウェアを解析しても初期侵入の表層的情報のみ
    - バックドアを仕掛けた後は攻撃者による手動の攻撃

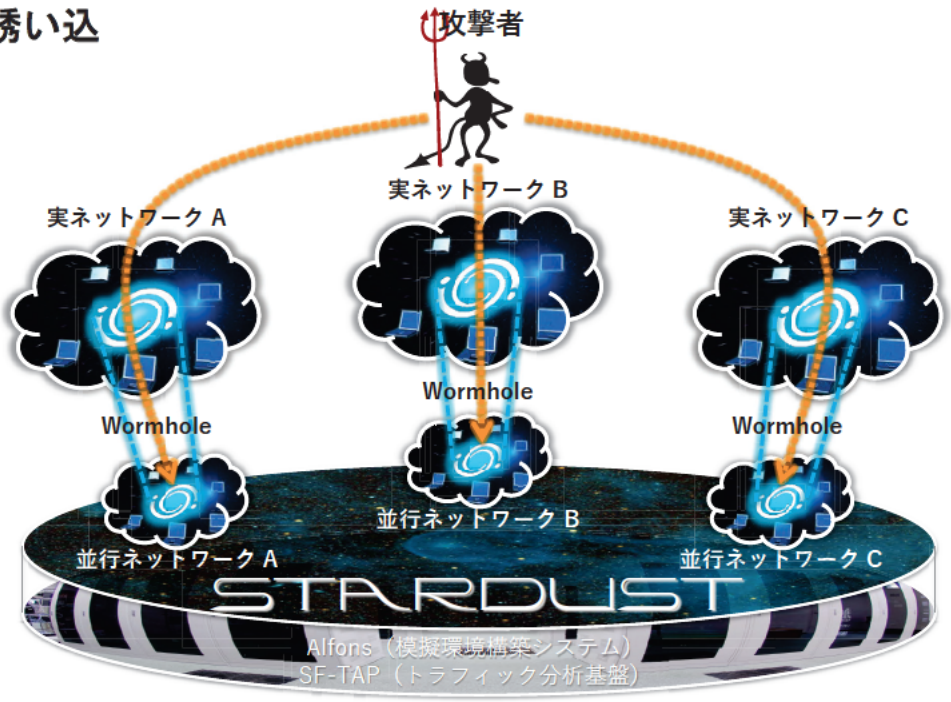
攻撃者の挙動を観測できる研究基盤が必要！

NICT National Institute of Information and Communications Technology

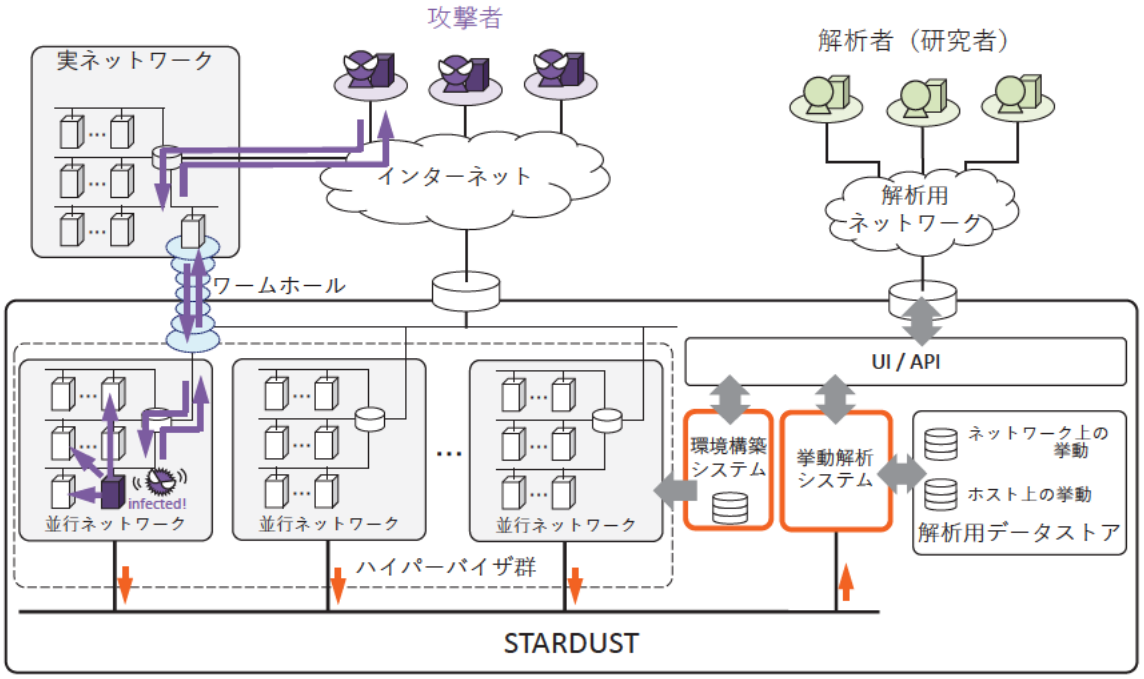
NICTER Network Incident analysis Center for Tactical Emergency Response

STARDUST

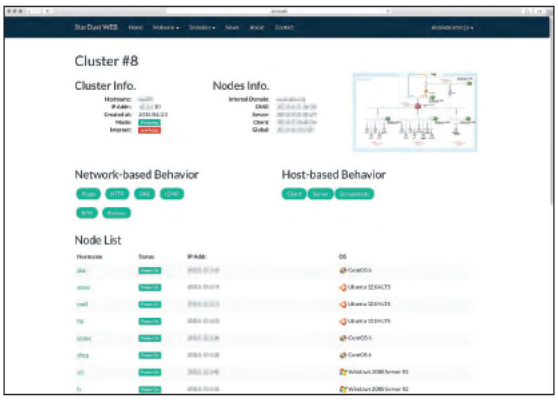
- 標的型攻撃等の攻撃者を誘い込むサイバー攻撃誘引基盤
- 組織を精巧に模擬した“並行ネットワーク”を高速・柔軟に自動生成
- 並行ネットワーク中で攻撃者を長期誘引し、ステルスに挙動を解析



STARDUST システム概要



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

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

攻撃者誘引実験 ケーススタディ

- **日本を標的にした攻撃グループを解析**
  - DragonOK（2016年3月～4月）
  - Powershell Empire（2017年7月）

- **解析のワークフロー**
  1. マルウェアの動的解析によりC&Cサーバのドメインを入手
  2. 上述のC&Cサーバへの接続性を検証
  3. 並行ネットワーク上のホストでマルウェアを実行
  4. C&Cサーバと接続できなくなれば解析終了

#	解析日	攻撃グループ	マルウェア（MD5）	C&Cサーバの場所	並行ネットワークの設定
1	2016/03/25～2016/04/11	DragonOK	251c0f90bfe9a302c471bf352b259874	US	• ADのドメインに参加 • ファイルやメールを設置
2	2017/07/25～2017/07/26	Unknown	25dacaf77a7c4c0f5ea4ddafe83e103	NL	• ADのドメインに参加 • ファイルやメールを設置

Case 1: DragonOK

```
net view
systeminfo
whoami
tasklist
dir c:¥users¥nito¥desktop¥
dir "c:¥program files¥"
dir d:¥
dir c:¥users¥nito¥
dir c:¥users¥nito¥documents¥
dir c:¥users¥nito¥downloads¥
dir ¥x03"c:¥Program Files (x86)¥"
netstat –an
dir c:¥users¥nito¥documents¥¥x03Credential
ipconfig /all
```

```
whomai /groups | find /i "level”
whoami
whoami /groups
net group
net view
arp –a
netstat –ano
ping 10.136.8.4 –n 1 <IP addr. of proxy>
tasklist
netstat –an
net view
tracert
net view ¥¥win05
```

- **net, tasklist, ping**等のコマンドでネットワークやホストを調査
- whoamiコマンドを**whomaiとタイポ**（攻撃者は手動）
- 他のケースで観測した攻撃者も**類似のコマンド群を使用**

Case 2: Powershell Empire

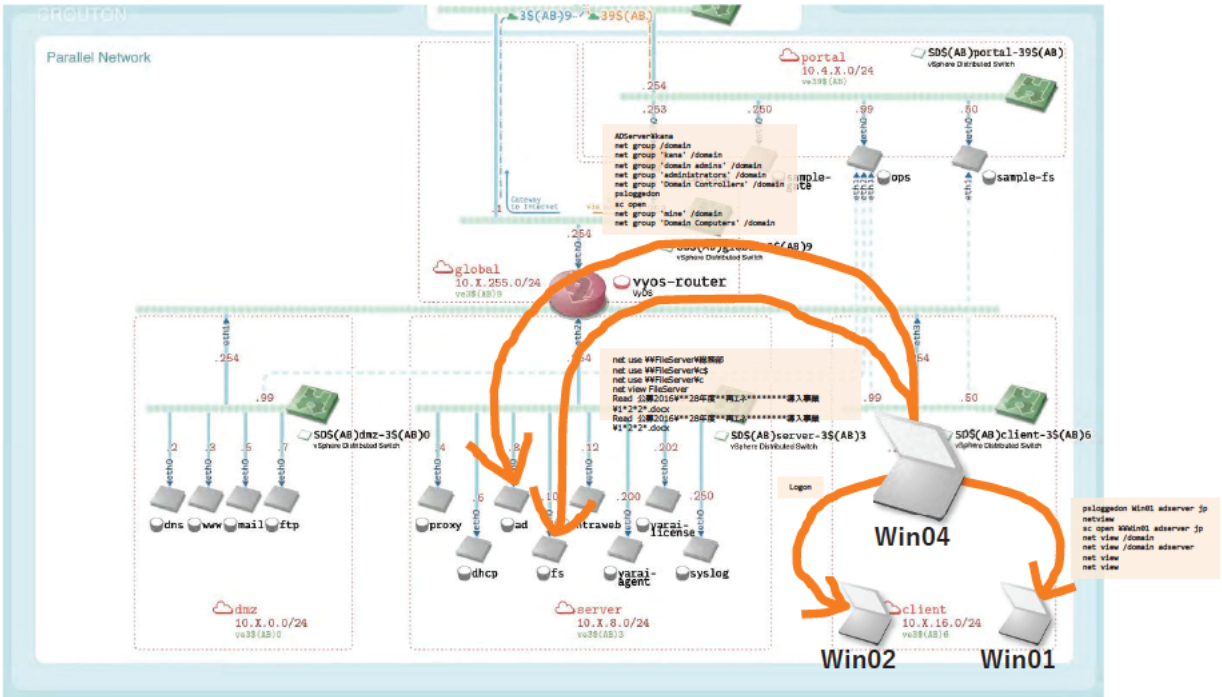
```
1  net group /domain adserver.jp
2  net group 'kana' /domain
3  net group 'domain admins' /domain
4  net group 'administrators' /domain
5  net group 'Domain controllers' /domain
6  psloggedon ADserver.adserver.jp
7  sc open ¥¥ADserver.adserver.jp
8  net group 'mine' /domain
9  net group 'Domain Computers' /domain
```

```
10 net use ¥¥FileServer¥総務
11 net group 'kana' /domain
12 net use ¥¥FileServer¥c$
13 net use ¥¥FileServer¥c
14 net view FileServer
15 READ 公募2016¥**28 年度**再エネ
   ********導入事業¥1*2*2*.docx
16 READ 公募2016¥**28 年度**再エネ
   ********導入事業¥1*2*2*.docx
```

```
17 psloggedon Win01.adserver.jp
18 netview
19 sc open ¥¥Win01.adserver.jp
20 net view /domain
21 net view /domain adserver
22 net view
23 net view
24 Logon
```

- 富士通研究所の**高速フォレンジック技術「PSYUN」**をSTARDUSTに導入して観測
- **psloggedonコマンド**でコンピュータにログオンしているユーザを特定
- ADサーバやファイルサーバ、他のWindows端末に**横展開**を試みる

図解：Case 2



STARDUST：攻撃者誘引実験結果

- **通説1：標的型攻撃は国家が関与した高度な攻撃**
  → **多くの攻撃者がマニュアルに沿った類似性の高い挙動**（アルバイト？）
- **通説2：攻撃者は組織内で不用意なスキャンをしない**
  → **組織内部調査のために頻繁にスキャン等を行う**（ネットワークで容易に観測可能）
- **通説3：攻撃者は潜入先のユーザの挙動を模して慎重に行動**
  → **一般ユーザが使用しないコマンドを多数使用**（エンドホストで容易に観測可能）

観測結果に基づくリーズナブルな対策は可能！

サイバー攻撃統合分析プラットフォーム

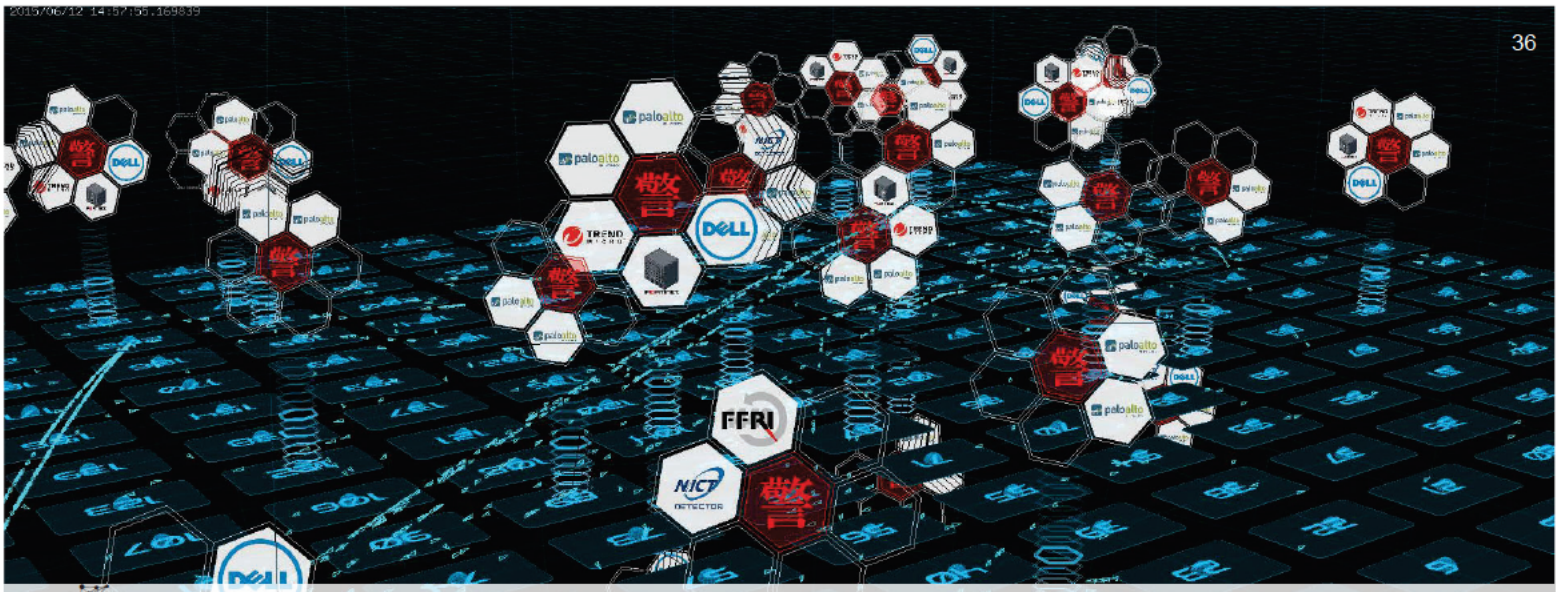
NIRVANA改

NICTER Real-network Visual ANAlyzer KAI

セキュリティオペレーション現場の悩み（その１）

- 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！



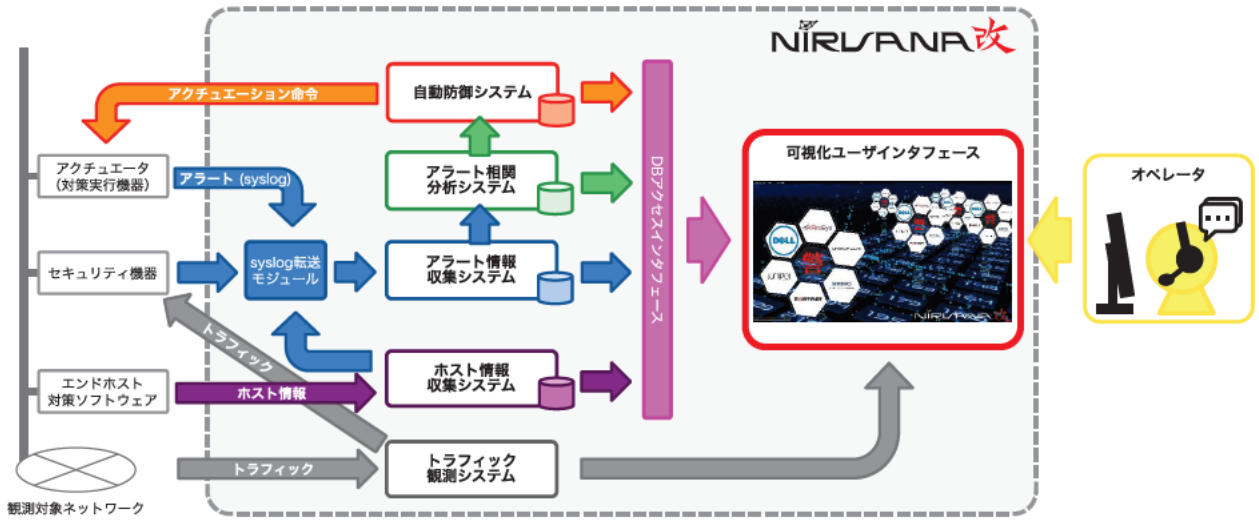
NIRVANA改

- 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



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）

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response