あなたのIoT機器は大丈夫?

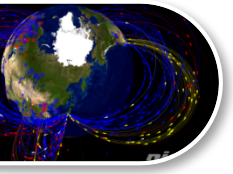
- サイバーセキュリティ研究の最前線 -

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

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）

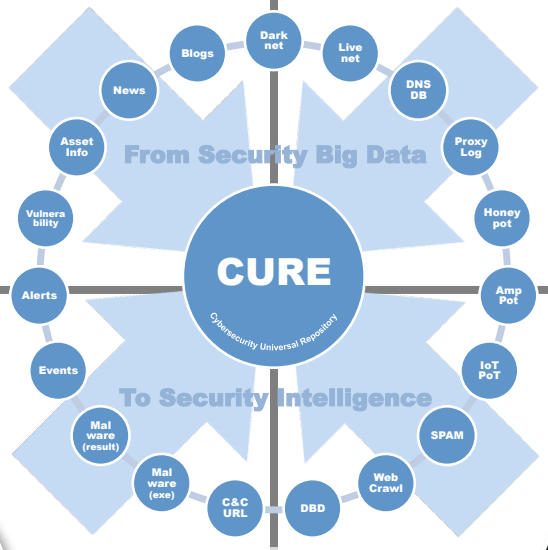
NIRVANA改弐

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

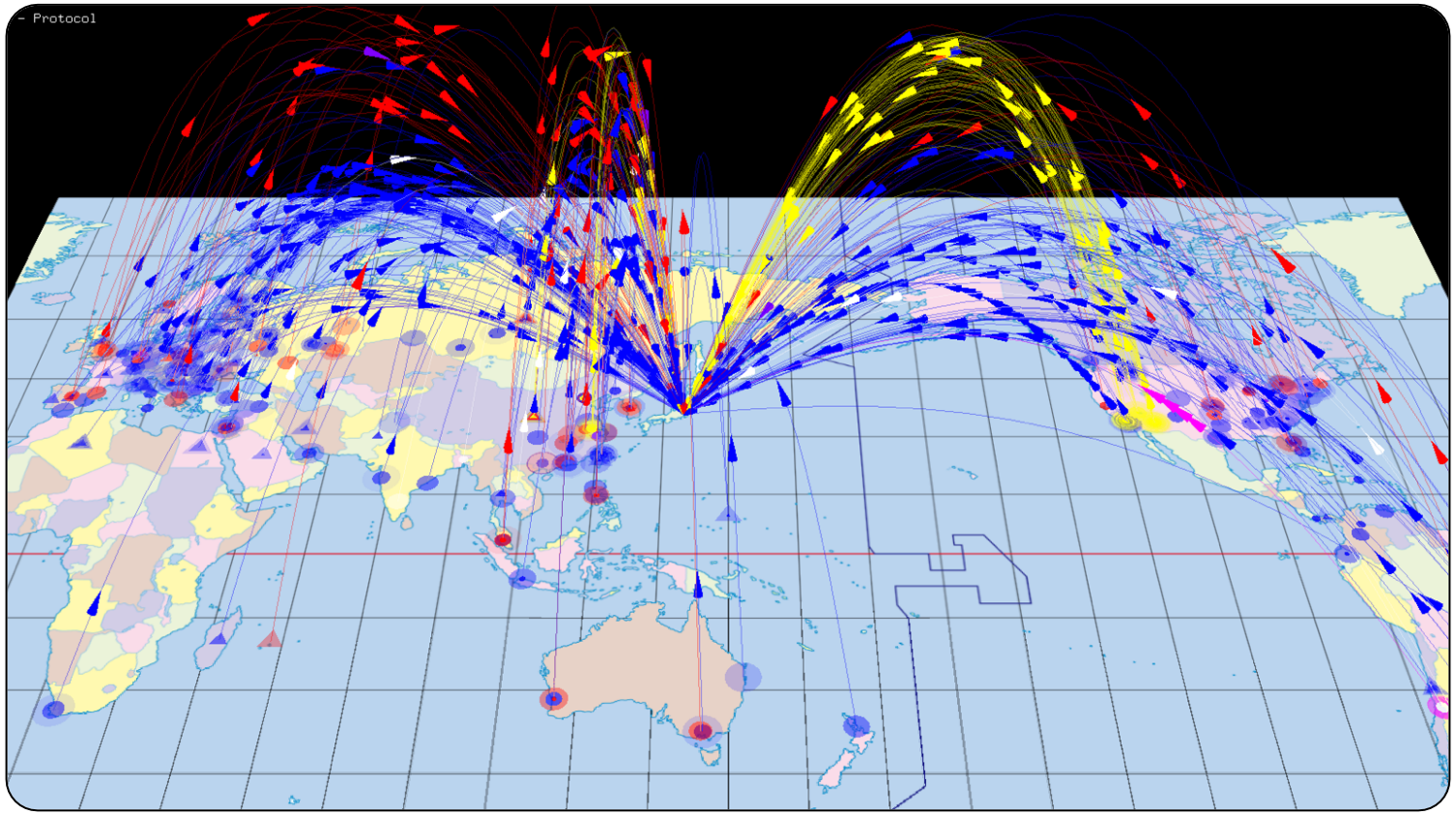
NICTER Network Incident analysis Center for Tactical Emergency Response

インシデント分析センター

Network **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse

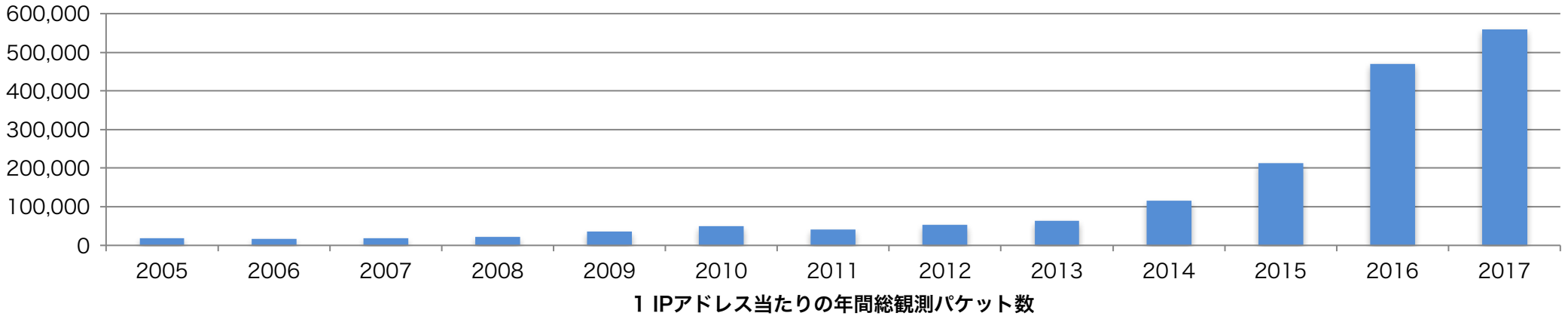
NICTER

- 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観測統計（2005-2017）

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**

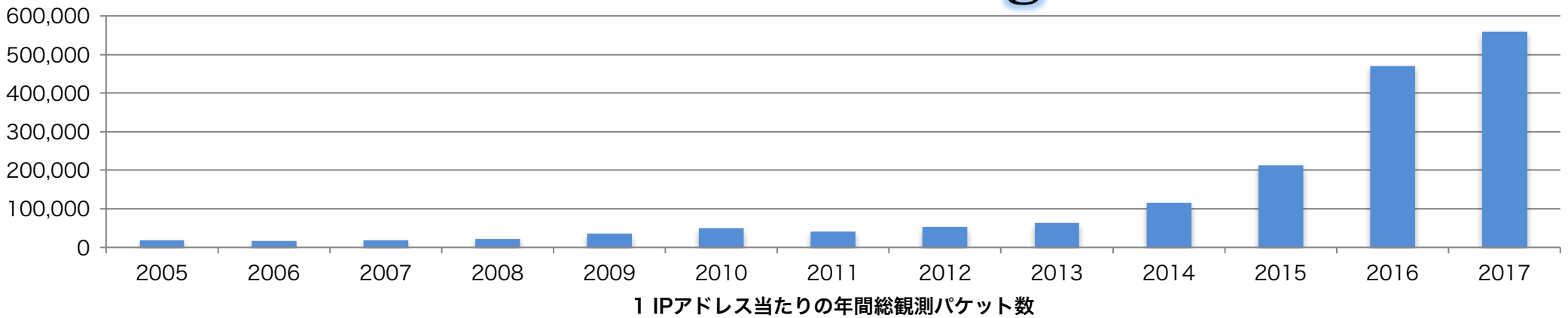


NICTER観測統計（2005-2017）

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22万	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**

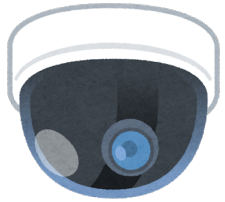
IoT

Internet of Things



感染IoT機器をさがせ！

問題：あなたの家でマルウェアに感染する可能性のある機器はどれでしょう？



Webカメラ

IP電話

ホームルータ

パソコン

ビデオレコーダ(DVR)

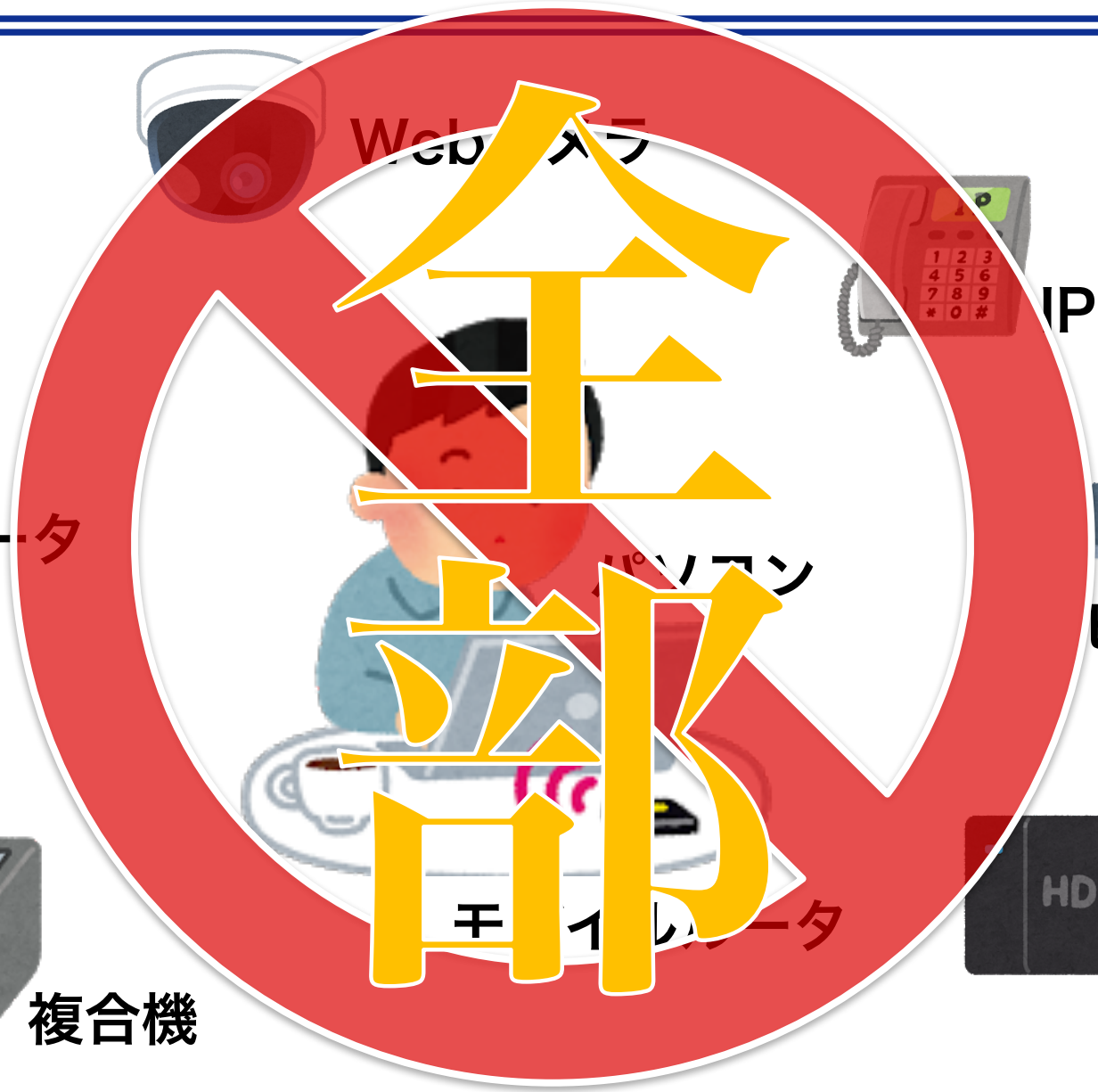
複合機

モバイルルータ

記憶媒体(NAS)

感染IoT機器をさがせ！

問題：あなたの家でマルウェアに感染する可能性のある機器はどれでしょう？



Webカメラ

IP電話

ホームルータ

パソコン

ビデオレコーダ(DVR)

モバイルルータ

HDD

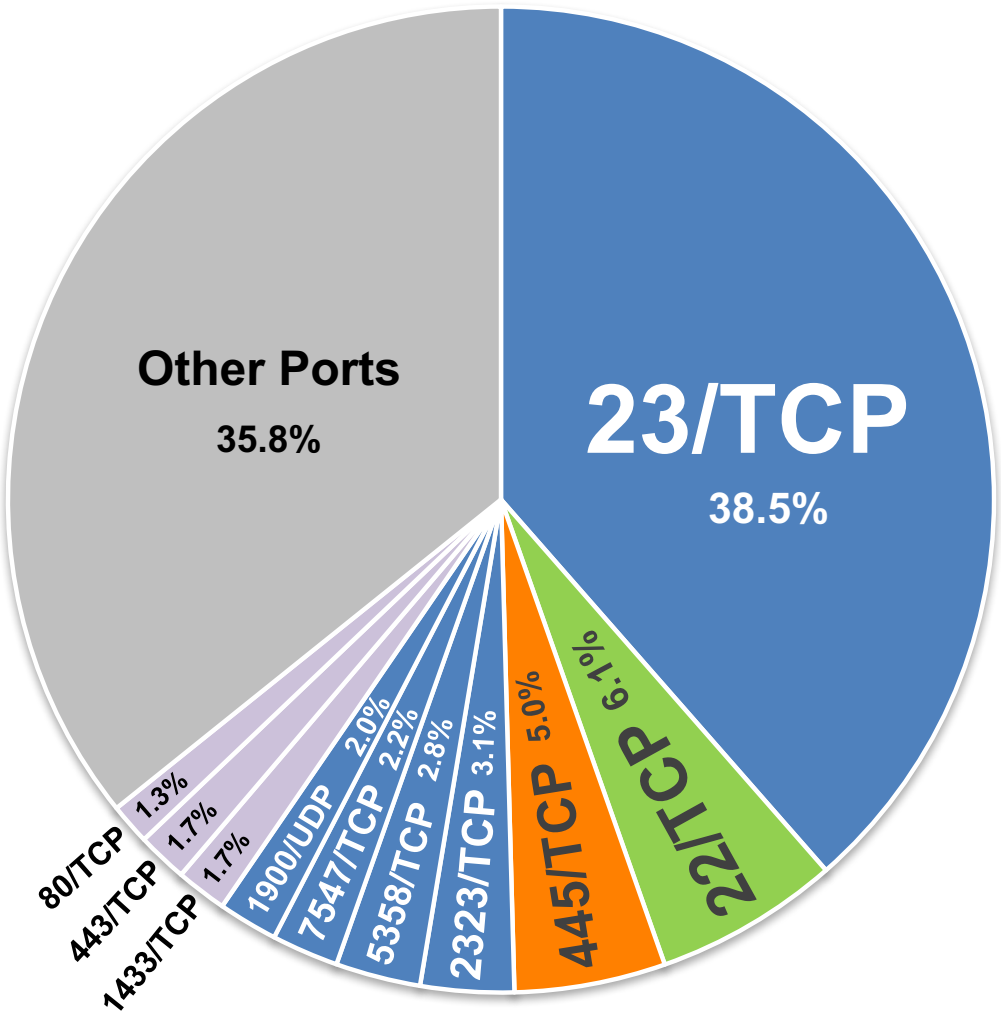
記憶媒体(NAS)

複合機

感染機器の分布（2017年）

- 宛先ポート番号別パケット数分布 -

あなたのIoTは大丈夫？



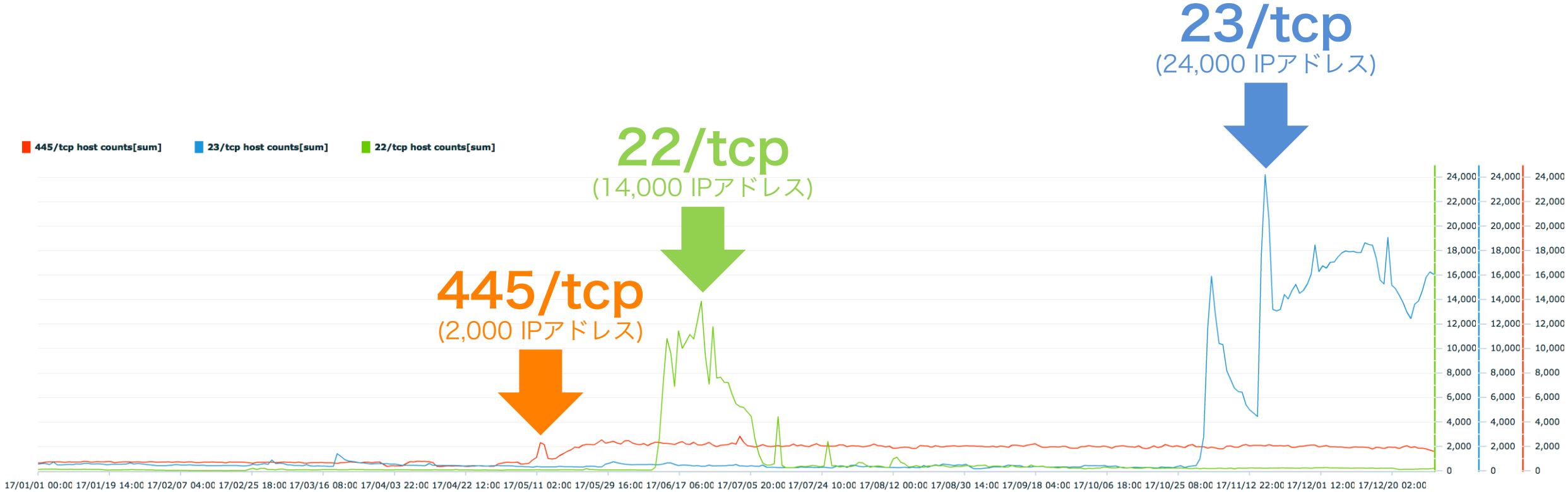
ポート番号	主な攻撃対象
23/TCP	IoT機器 （Webカメラ等）
22/TCP	IoT機器（モバイルルータ等） 認証サーバ（SSH）
445/TCP	Windows（SMB）
2323/TCP	IoT機器 （Webカメラ等）
5358/TCP	IoT機器（Webカメラ等）
7547/TCP	IoT機器（Webカメラ等）
1900/UDP	IoT機器（ホームルータ等）
1433/TCP	データベースサーバ（SQL）
443/TCP	Webサーバ（SSL/TLS）
80/TCP	Webサーバ（HTTP）

2017: IoT > 54%

(23/TCP + 22/TCP + 2323/TCP + 5358/TCP + 7547/TCP + 1900/UDP)

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

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

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）

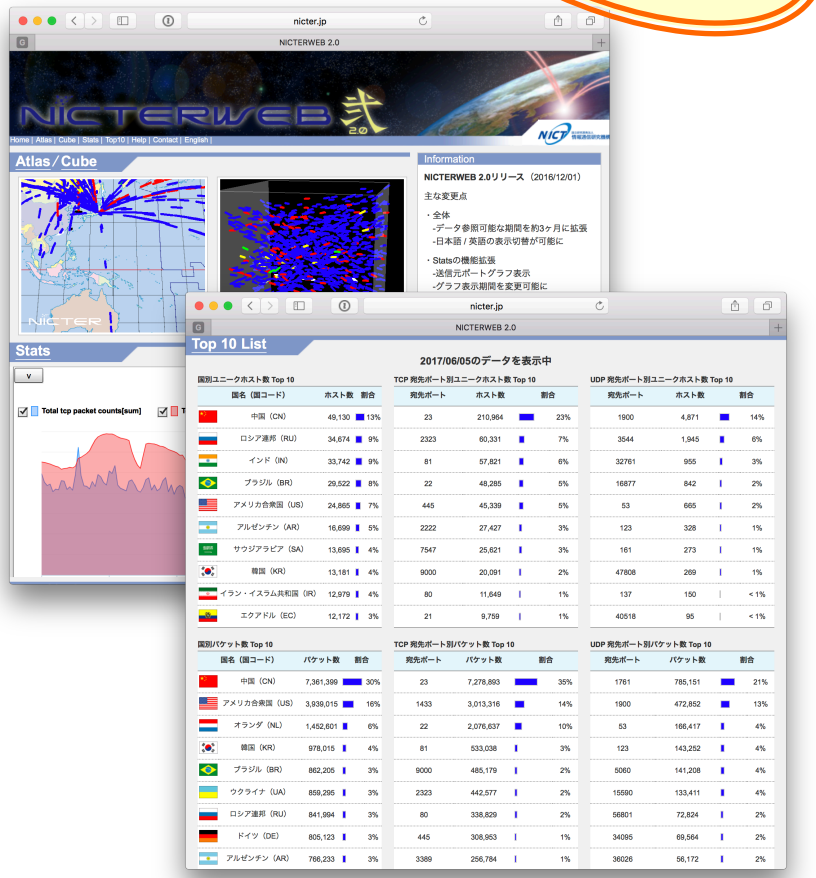
2. **ファームウェアのアップデート**（脆弱性を塞ぐ）
3. **ID/パスワードを変更**（初期パスワードでの侵入を防ぐ）
4. **インターネット側からのアクセス拒否設定**（外から繋がせない）
5. **ゲートウェイ機器の内側に設置**（直接インターネットに繋がない）
6. **古い機器は買い換える**（自動アップデート機能がない機器はNG）

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～）



NICTERWEB

● 観測情報一般公開

- ✓ NICTERWEB (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)

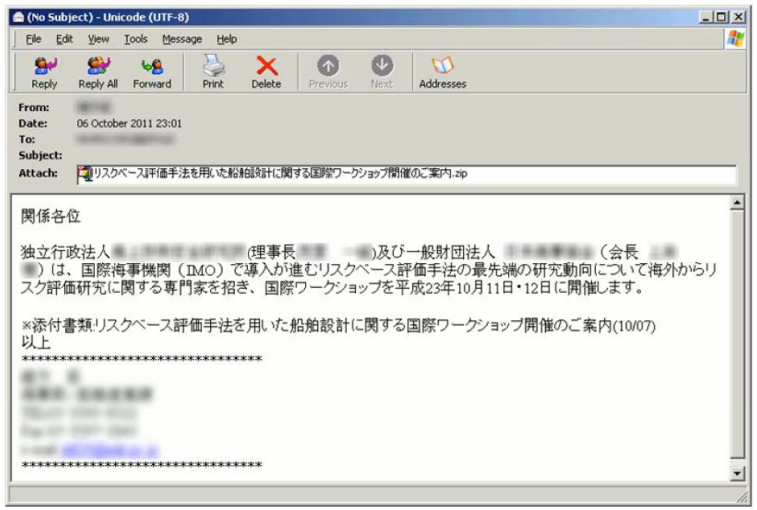
サイバー攻撃統合分析プラットフォーム

NICTER **R**eal-network **V**isual **ANA**lyzer KAI

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

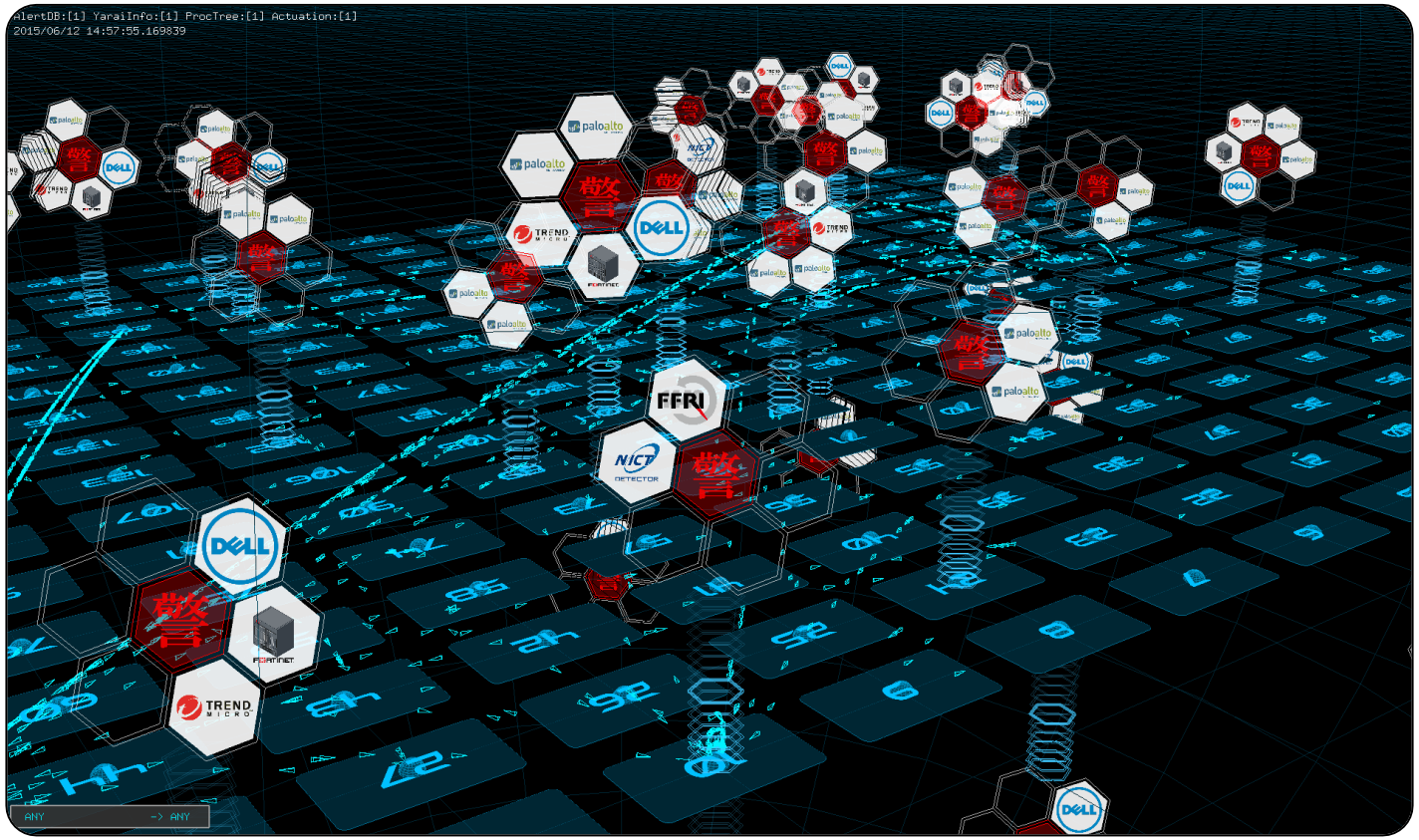


TECH.ASCII.jp「9.5社に1社が対象に！シマンテックが明かす日本の標的型攻撃」
http://ascii.jp/elem/000/000/652/652712/ （2011-11-30）

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

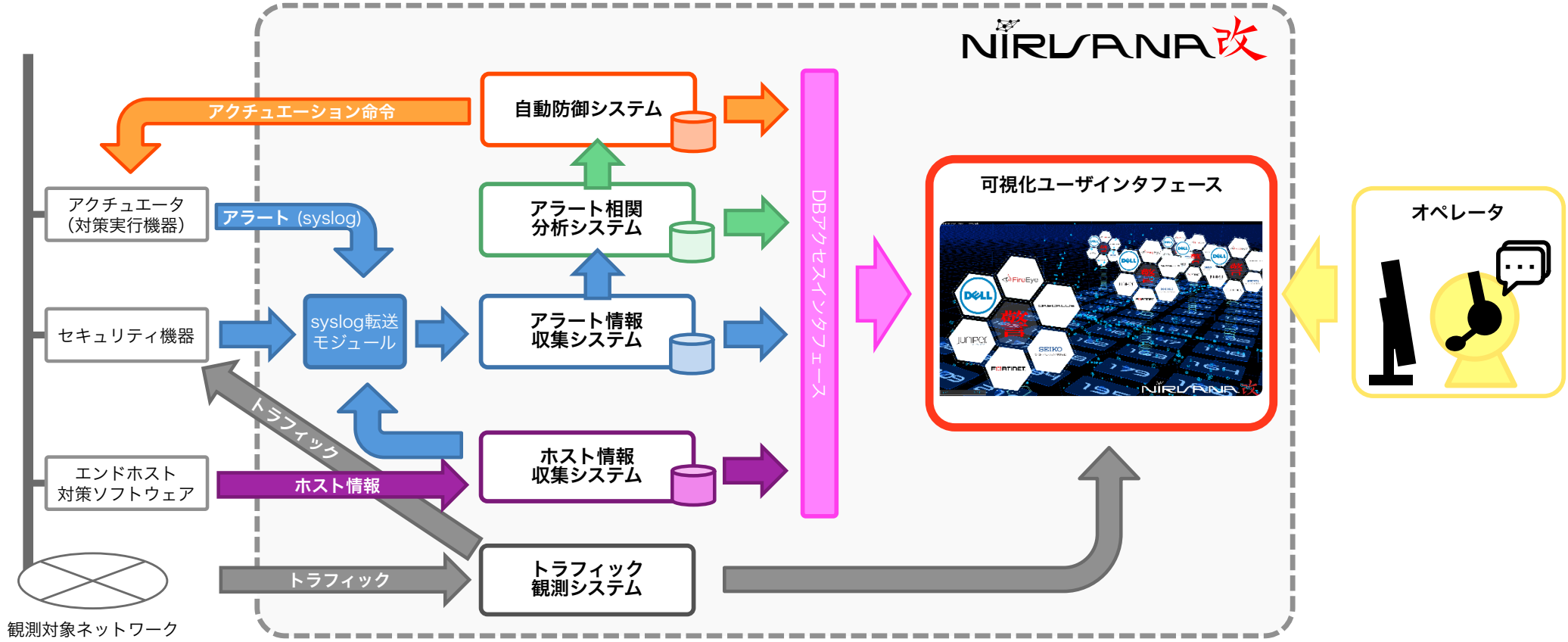
- セキュリティオペレーションを効率化する統合分析プラットフォーム
- セキュリティ機器群からのアラートを集約・分析・トリアージ
- 組織の末端までセンサを設置しトラフィック観測・分析・可視化



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 2018

- セキュリティ・オーケストレーション@Interop Tokyo 2018 -

● アラート連携アプライアンス・ソフトウェア：38種（21社）

Vendor Name	Appliance / Software Name
NICT	DAEDALUS
Future	Vuls
FFRI	yarai
NEC	Aterm SA3500G
The Univ. of Tokyo	phish-finder
	syn-picture
Trendmicro	TippingPoint
	TippingPoint SMS
	Deep Discovery Inspector
	Deep Discovery Analyzer
A10 Networks	Thunder 14045 TPS
Arbor	SP7000
	TMS HD1000
CarbonBlack	CbResponse
CheckPoint	SandBlast
Cisco Systems	Firepower9300
	Threat Grid
	FTDv
	Firepower Management Center
	Stealthwatch + ETA

Vendor Name	Appliance / Software Name
Cylance	CylancePROTECT
	CylanceOPTICS
DAMBALLA	Network Insight
Deep Instinct	Deep Instinct
F5	Big-IP AFM i10800
Fortinet	FortiGate6501F
	FortiSandbox
	FortiGate500E
Juniper Networks	Juniper ATP
Keysight	ThreatARMOR
Lastline	Lastline Breach Defender
	Lastline Enterprise
Palo Alto Networks	PA5280
	PA220R
	PA3260
	WildFire
	M200
ProtectWise	ProtectWise Grid

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**：新日鉄住金ソリューションズ社によるセキュリティ製品

DIT
『WADJET』

新日鉄住金ソリューションズ
『えぬえすみはる』

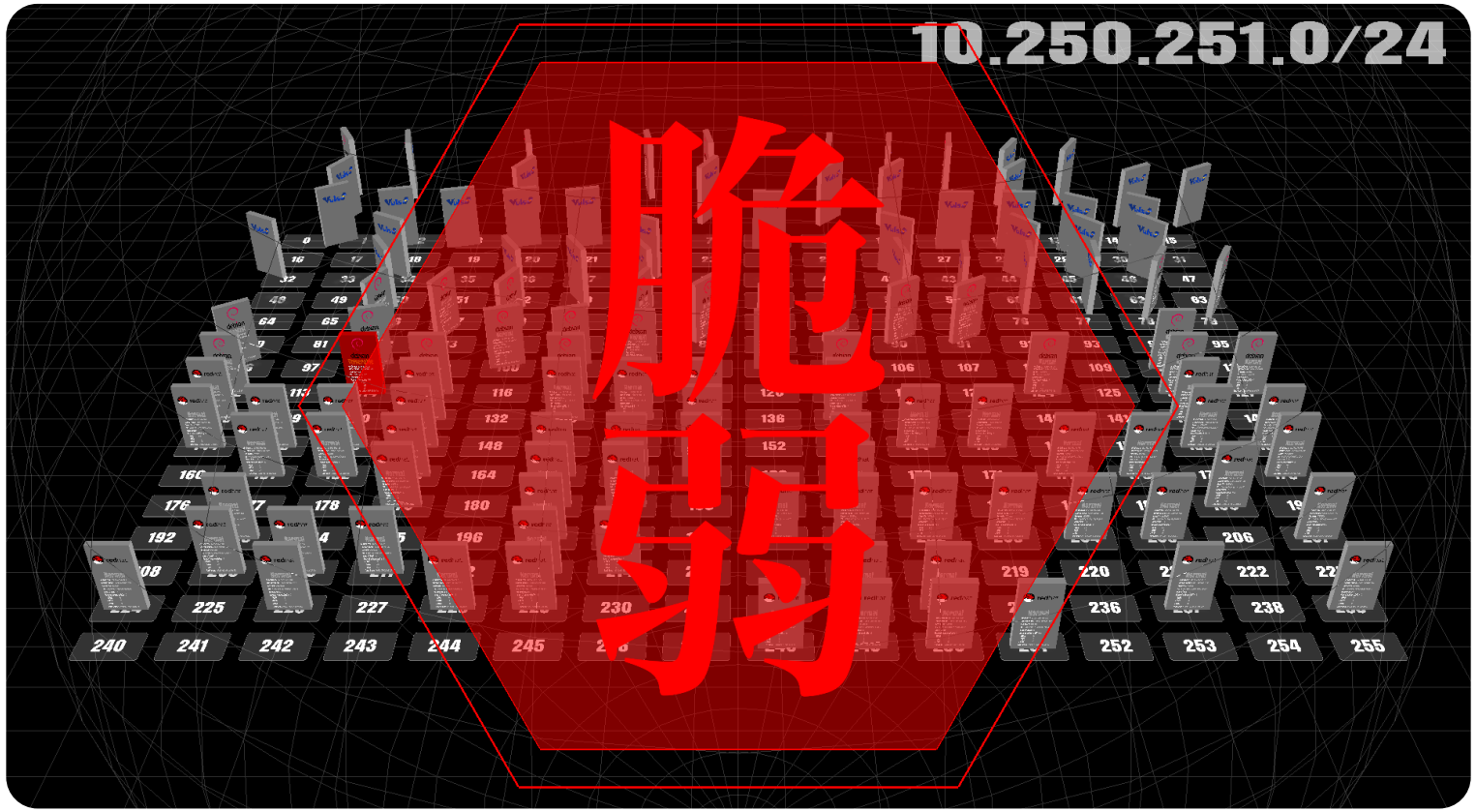
脆弱性管理プラットフォーム

NICTER **R**eal-network **V**isual **ANA**lyzer KAI2

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）

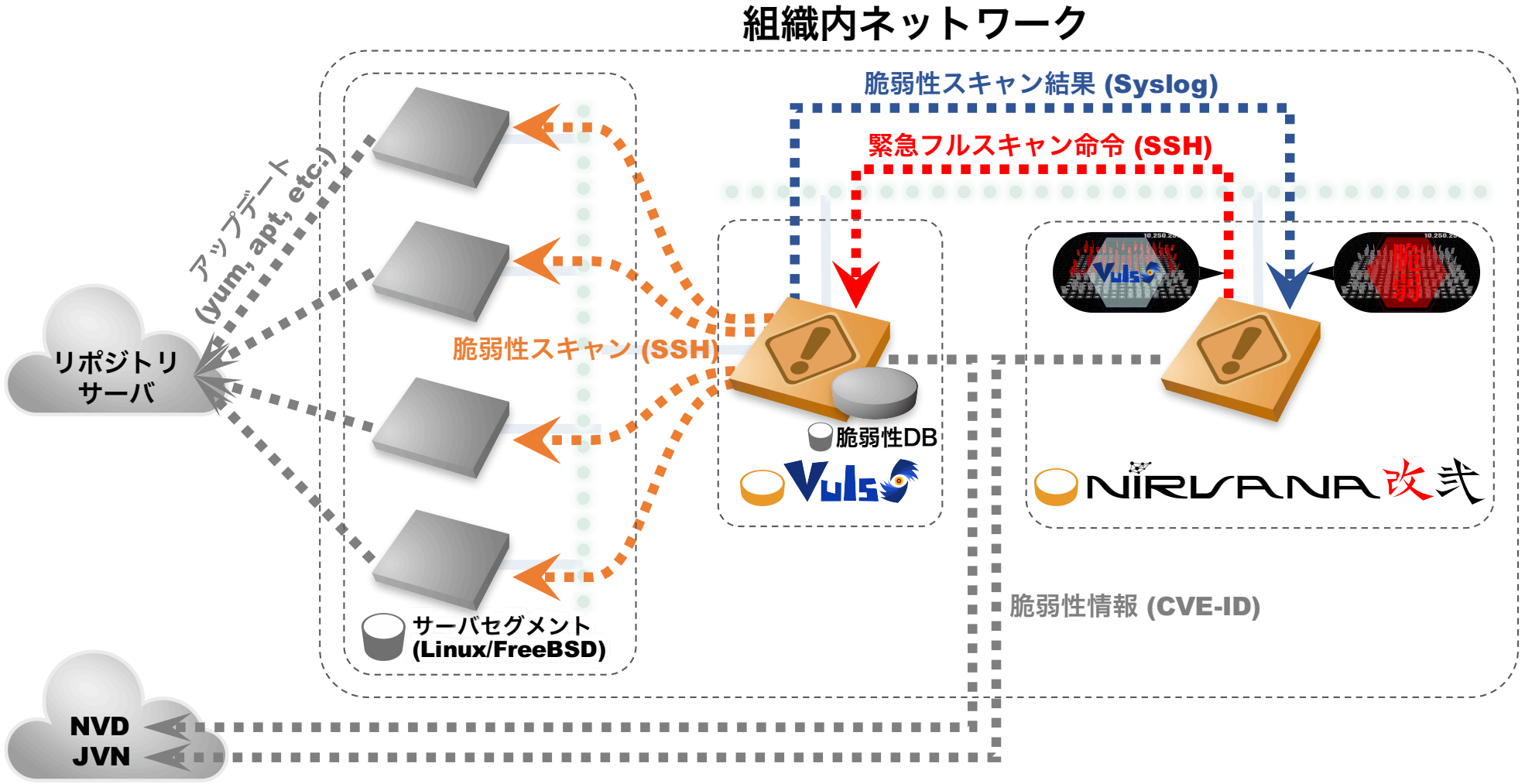
NIRVANA改弐

- 組織のシステム監視を省力化する脆弱性管理プラットフォーム
- 国産OSS脆弱性スキャナ『Vuls』によるリアルタイム脆弱性検査
- アクチュエーション（自動対処）機能による緊急フルスキャン

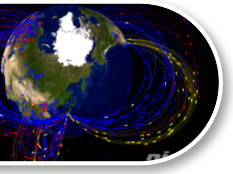


NIRVANA改弐 システム構成

NIRVANA改弐 = NIRVANA改 + Vuls



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）

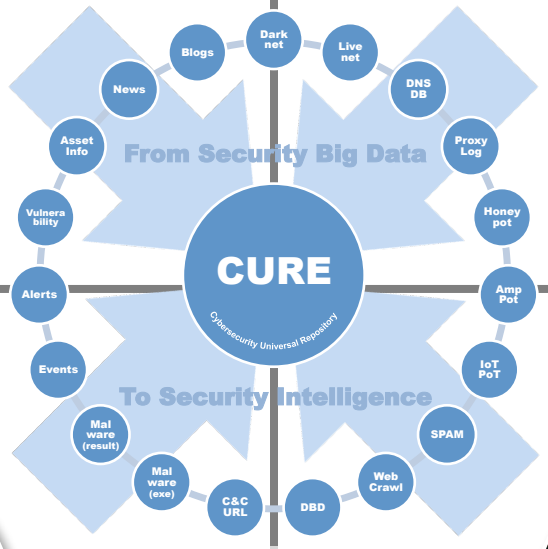
NIRVANA改弐

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

National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response