ネットワークモニタリングシステム NIRVANAによる 制御システムへの攻撃検知

井上 大介

独立行政法人 情報通信研究機構

ネットワークセキュリティ研究所（NSRI）　サイバーセキュリティ研究室

サイバー攻撃対策総合研究センター（CYREC）　サイバー防御戦術研究室

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

過去7年間の主なセキュリティ事案

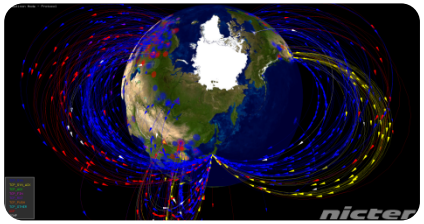
2008	Downadup (Conficker)	大規模感染ワーム
2009	Gumblar	Web媒介型攻撃
2010	Stuxnet	制御システム向けマルウェア
2011	SONYへのDDoS攻撃	ハクティビズム
	標的型攻撃	サイバーエスピオナージ
2012	バンキングマルウェア	オンライン銀行詐欺
	遠隔操作ウイルス	愉快犯、フォレンジック
2013	ブラックリスト攻撃	DNSオープンリゾルバ問題
	アカウントリスト攻撃	同一ID/パスワード問題
2014	Heartbleed	OpenSSL脆弱性
	ベネッセ個人情報漏洩	内部犯罪、アウトソーシング

攻撃対象拡大、攻撃手法高度化

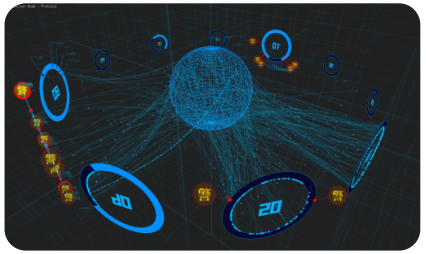
最大の経営リスクの一つ

NICTERとそのスピンオフ技術たち

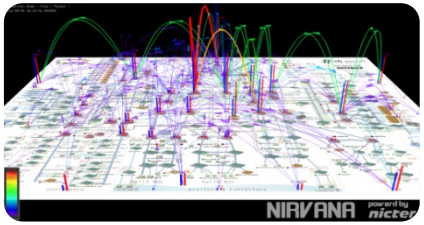
1. インシデント分析センタ
   NICTER



2. 対サイバー攻撃アラートシステム
   DAEDALUS



3. ネットワークリアルタイム可視化システム
   NIRVANA



4. サイバー攻撃統合分析プラットフォーム
   NIRVANA改

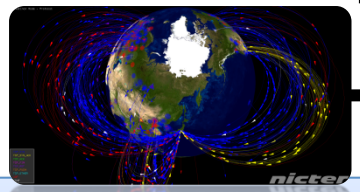
ダークネット観測

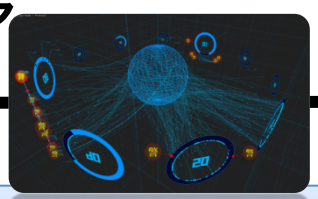
ライブネット観測

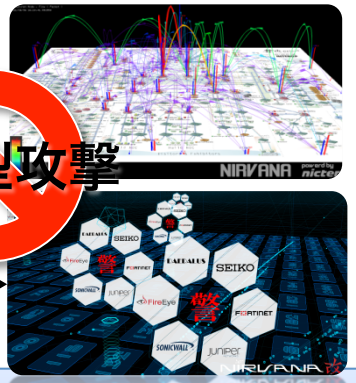
鳥の目/虫の目

大規模感染型
マルウェア

標的型攻撃







NICTER　DAEDALUS　NIRVANA
NIRVANA 改

グローバル観測
（ダークネット）

ローカル観測
（ライブネット）

National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

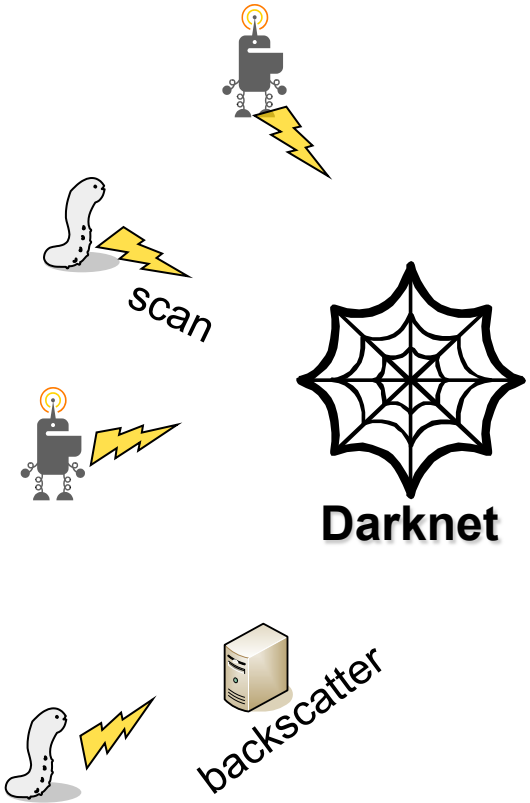
インシデント分析センタ

NICTER

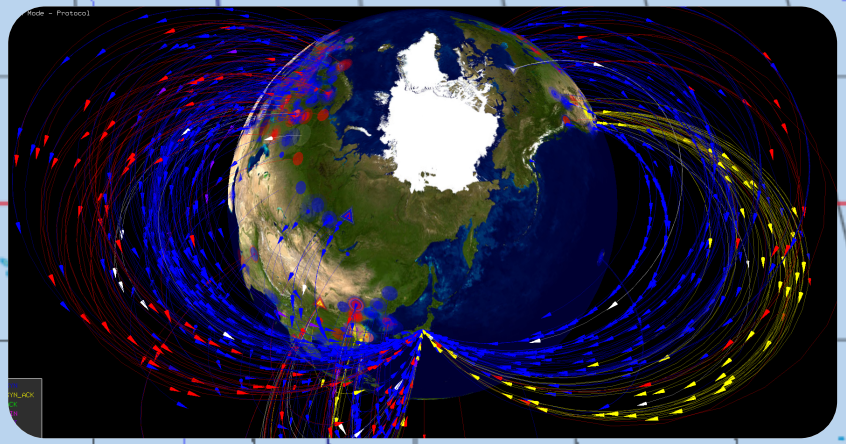
(**N**etwork **I**ncident analysis **C**enter
for **T**actical **E**mergency **R**esponse)

ダークネットで何が見えているのか？

- **マルウェアによるスキャン**
  - ✓ ワーム型マルウェアの探索活動
  - ✓ マルウェア感染の大局的傾向
  - ✓ Linux組込機器からのスキャン　新
- **DDoS攻撃の跳ね返り**
  - ✓ 送信元IPアドレス偽装されたSYN Flood
  - ✓ 被攻撃サーバからの応答（SYN-ACK）
  - ✓ DDoS攻撃の早期検知（1パケット目から）
- **設定ミス**
  - ✓ 組織内ダークネット
- **リフレクション攻撃の準備活動**　新
  - ✓ DNS Open Resolver探索
  - ✓ NTP探索　etc.

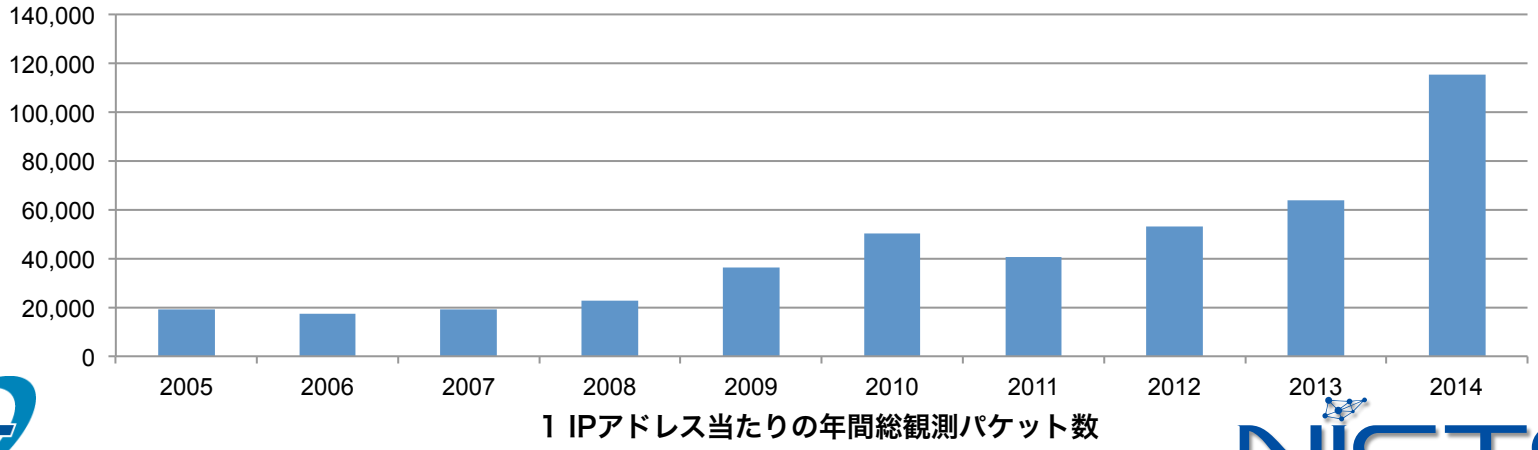


NICTER



NICTERダークネット観測統計

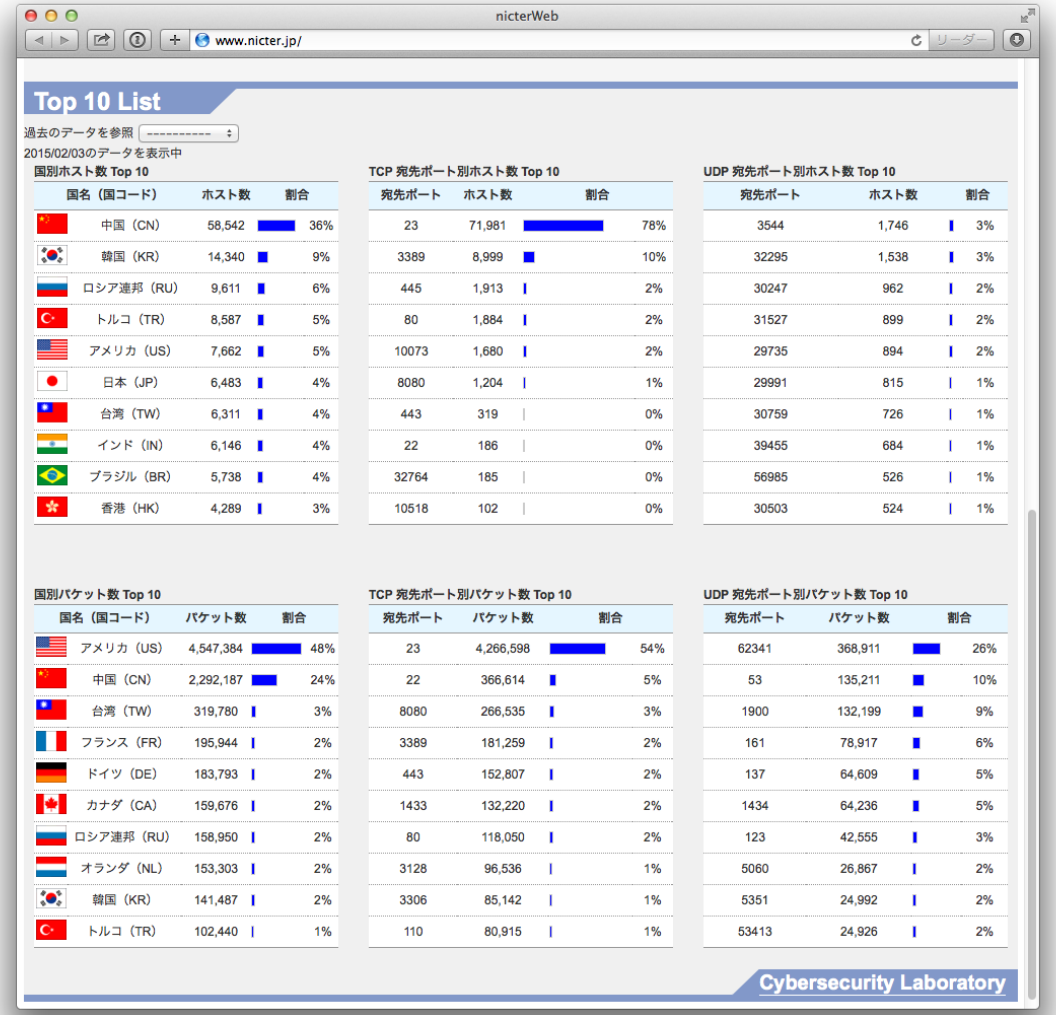
年	年間 総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの 年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	**115,323**

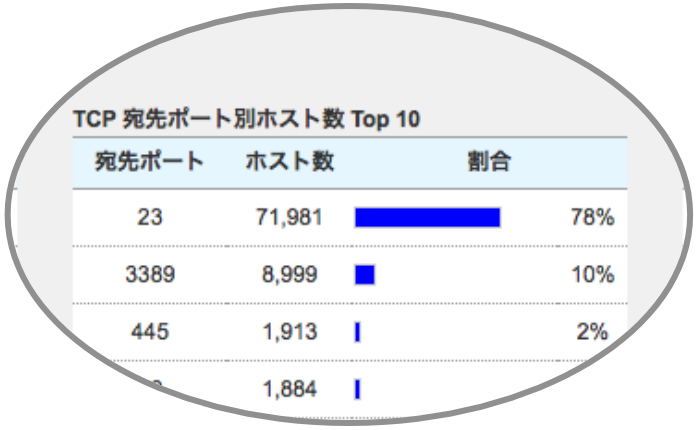


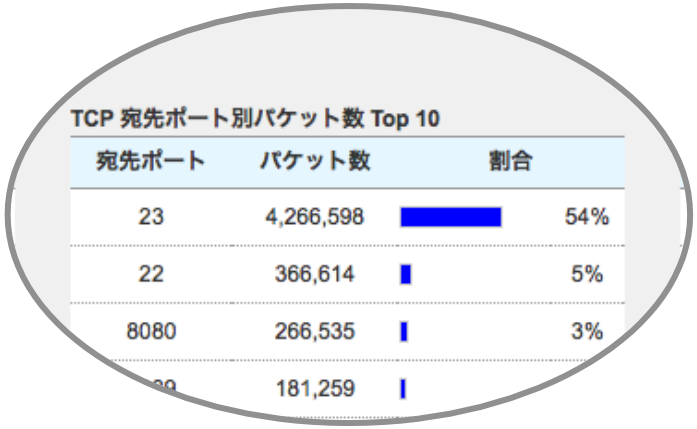
NICT

NICTER
Network Incident analysis Center for Tactical Emergency Response

ダークネットトラフィック急増の原因



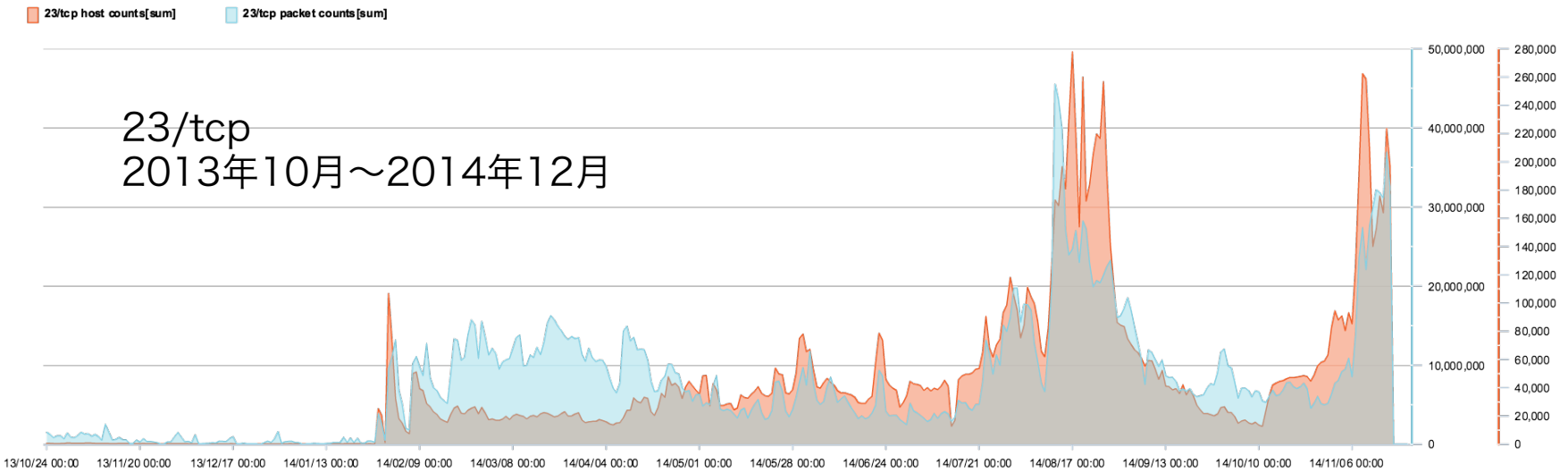




NICT

NICTER
Network Incident analysis Center for Tactical Emergency Response

組込機器からの23/tcpスキャン



- **感染機器：Linux組込機器**
  - ✓ ブロードバンドルータ
  - ✓ Webカメラ
  - ✓ NAS（Network Attached Storage）　etc.

NICT

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

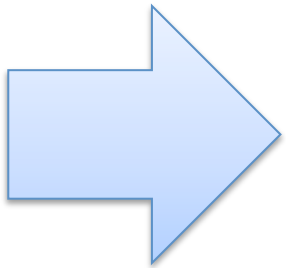
Darknet **A**nd **L**ivenet **U**nified **S**ecurity

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

マルウェア感染対策の現状 – 境界防御の限界 -

- **突破される従来の防御手法**
  - 回避される侵入検知システム
    - USBメモリによる**ネットワーク内部からの感染**
    - 標的型メールによる**「人」への攻撃**
  - 完璧ではないアンチウイルスソフト
    - 膨大な亜種ウイルスの出現により**100%の検知は困難**



- **マルウェア感染リスクのゼロ化は困難**
- **事故前提のマルウェア対策が必要**

境界防御技術とDAEDALUS

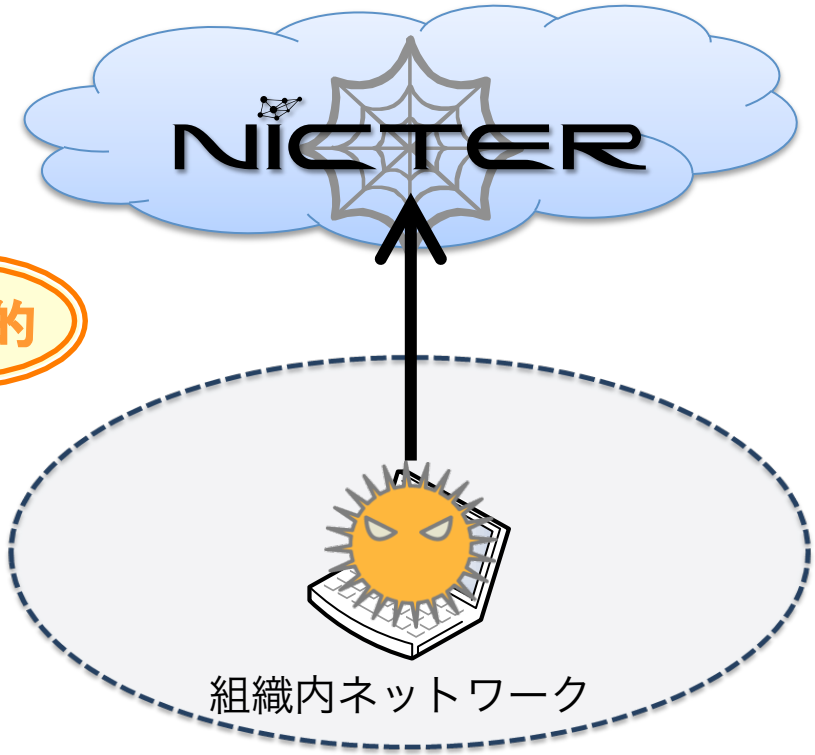
境界防御技術

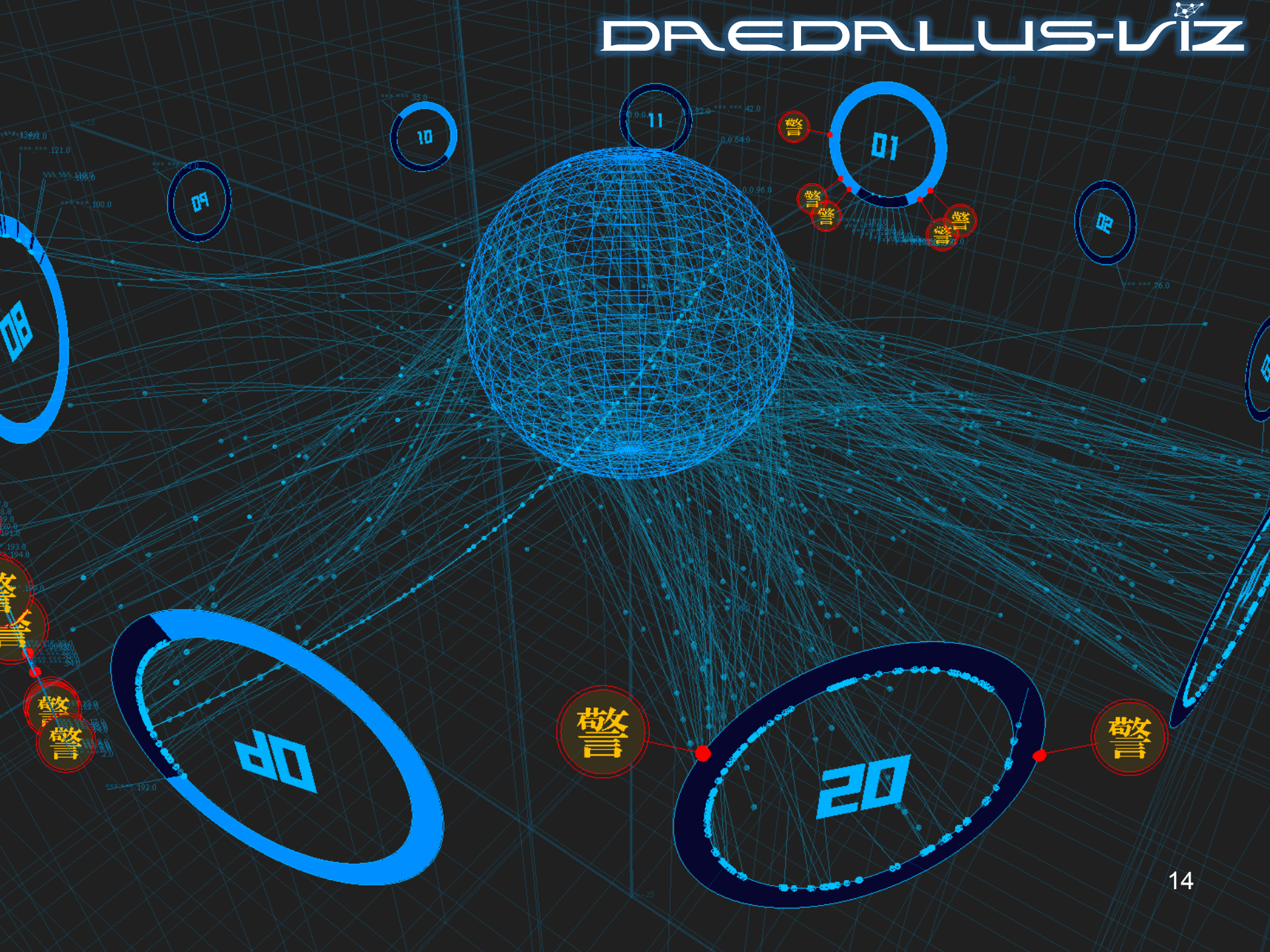
組織外からの攻撃をネットワーク境界で検出

DAEDALUS

組織内からの攻撃をネットワーク広域で検出

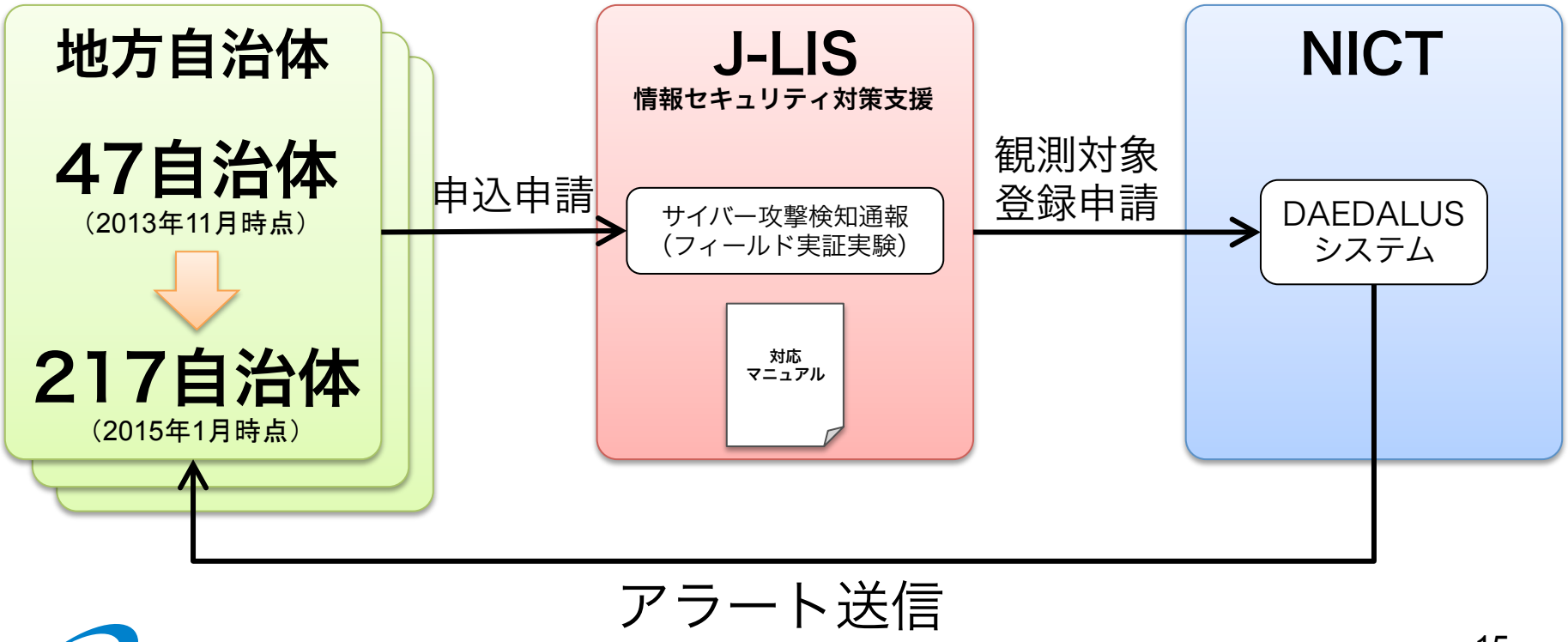
相補的




DAEDALUS-VIZ
警
01
02
08
09
10
11
20
警
警
警
警
警
警
警

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



DAEDALUSの成果展開：商用展開
一般企業へのアラート提供

- **SiteVisor：**
  DAEDALUSに基づく商用アラートサービス（クルウィット社）
- **SiteVisor Professional：**
  インシデント発生時のレスポンスサービス（ディアイティ社）

クルウィット『SiteVisor』

ディアイティ『SiteVisor Professional』

National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

ネットワークリアルタイム可視化システム

NICTER Real-network Visual ANAlyzer

National Institute of Information and Communications Technology

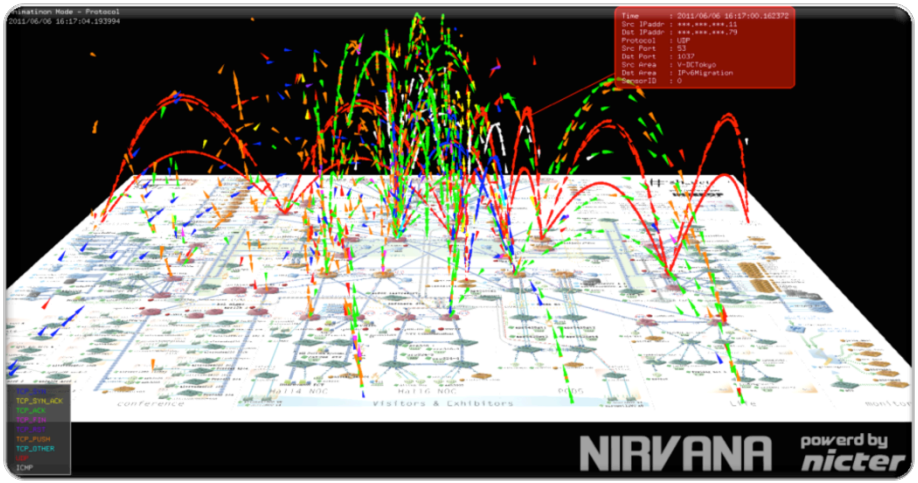
NICTER
Network Incident analysis Center for Tactical Emergency Response

NIRVANA

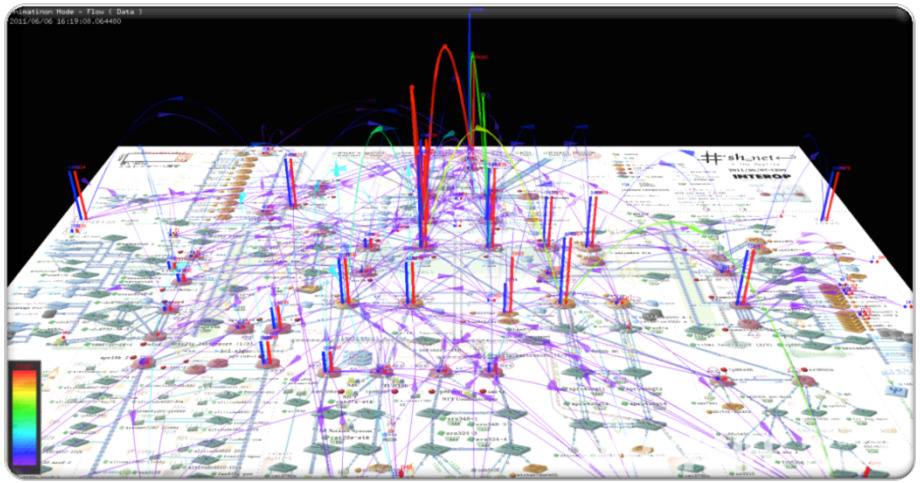
ライブネットを見える化

ネットワーク管理者の負荷を軽減
（輻輳・切断等の障害、設定ミス等を瞬時に発見可能）

管理コストの軽減
（管理の迅速化・効率化）



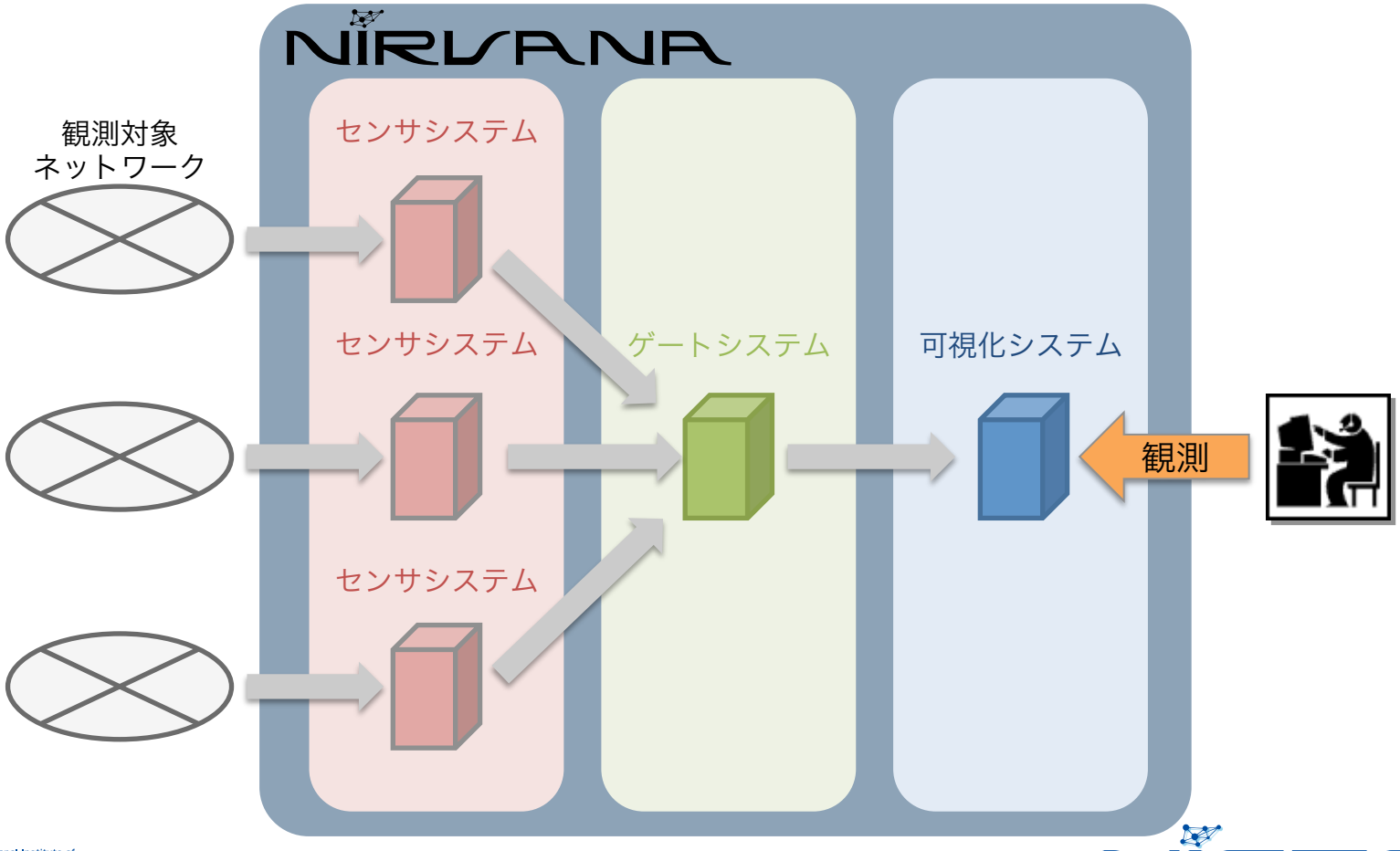
パケットモード



フローモード

システム構成

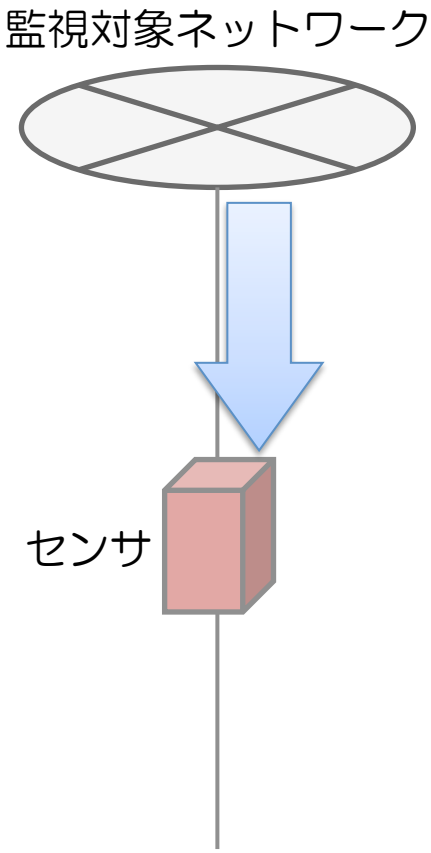
- 複数箇所にセンサを設置する基本構成。
- 複数のネットワークを集約し、観測することが可能。



センサへのトラフィック入力方法

- **リアルタイム系**
  - ✓ Switchのミラーポート
  - ✓ TAP
  - ✓ sFlow（RFC 3176）

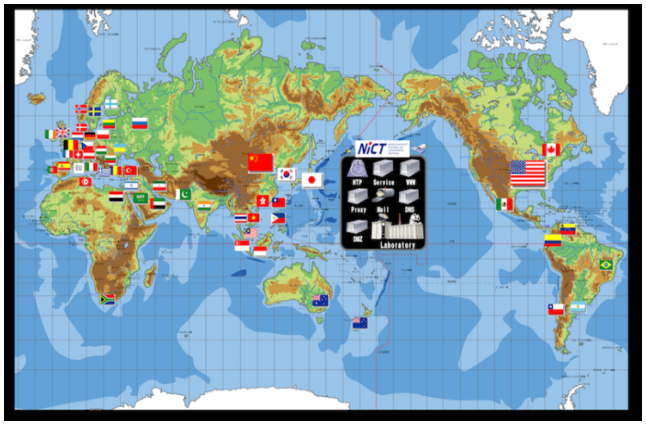
- **再現系**
  - ✓ PCAPファイル
    ※ 可視化エンジンへの直接入力



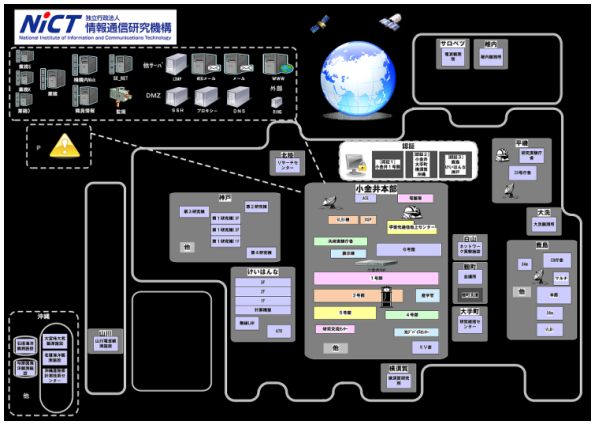
背景画像の作成

- Microsoft Visio 2007で作成し、IP アドレスと座標を自動設定
- 用途に応じて柔軟な画面構成が可能

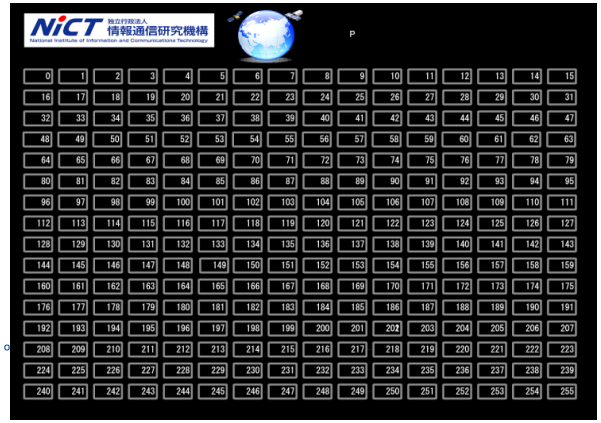
世界地図上でのトラフィックの可視化



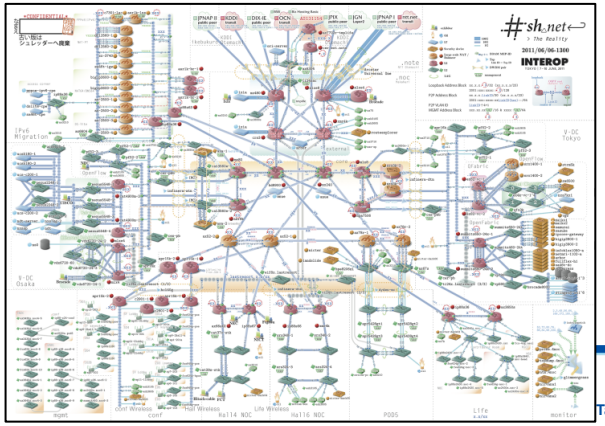
組織拠点間トラフィックの可視化



アドレスブロック間のトラフィックの可視化

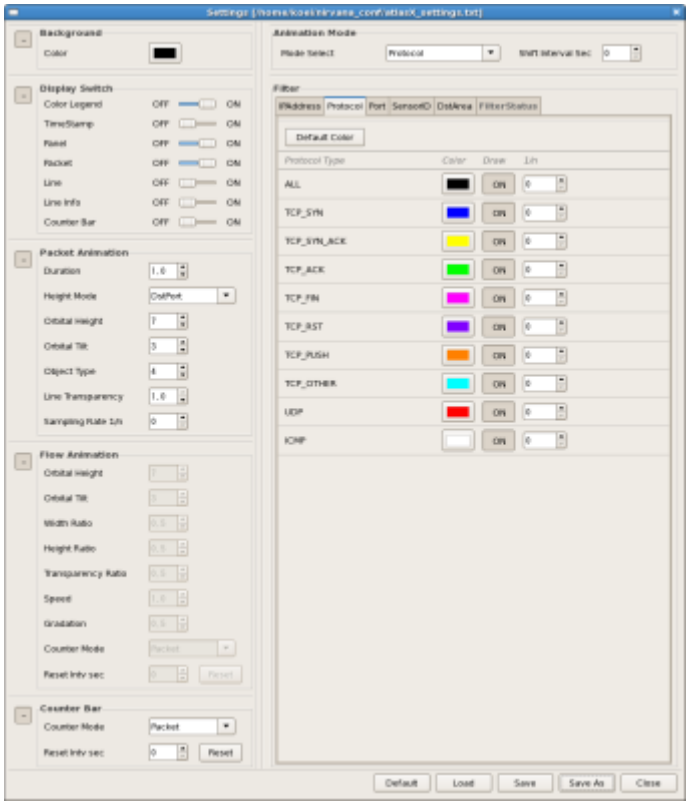


トポロジ図上でのトラフィックの可視化



多彩なフィルタ機能

フィルタリング機能により、特定の通信の強調や絞り込みが可能。



- **IPアドレス**
  - ✓ Src/Dst IPアドレスによる通信のフィルタリング。
- **プロトコル**
  - ✓ プロトコルの種類毎のフィルタリング。
- **ポート番号**
  - ✓ ポート番号毎のフィルタリング。
- **センサID**
  - ✓ センサID：センサに一意に割り当てられるID。
  - ✓ トラフィック取得地点毎のフィルタリング。
- **エリア**
  - ✓ エリア：Visioファイル内で定義する、各ネットワーク機器が属するグループ。
  - ✓ 営業拠点毎のエリア定義や建物のフロア毎のエリア定義などが可能。
  - ✓ 宛先エリア毎のフィルタリング。

NIRVANAの成果展開：商用展開

NIRVANA Rapps

- NIRVANAをパッケージ化した商用アプライアンス
- 日本ラッド社、BIGLOBE社より販売中

日本ラッド

BIGLOBE

National Institute of Information and Communications Technology

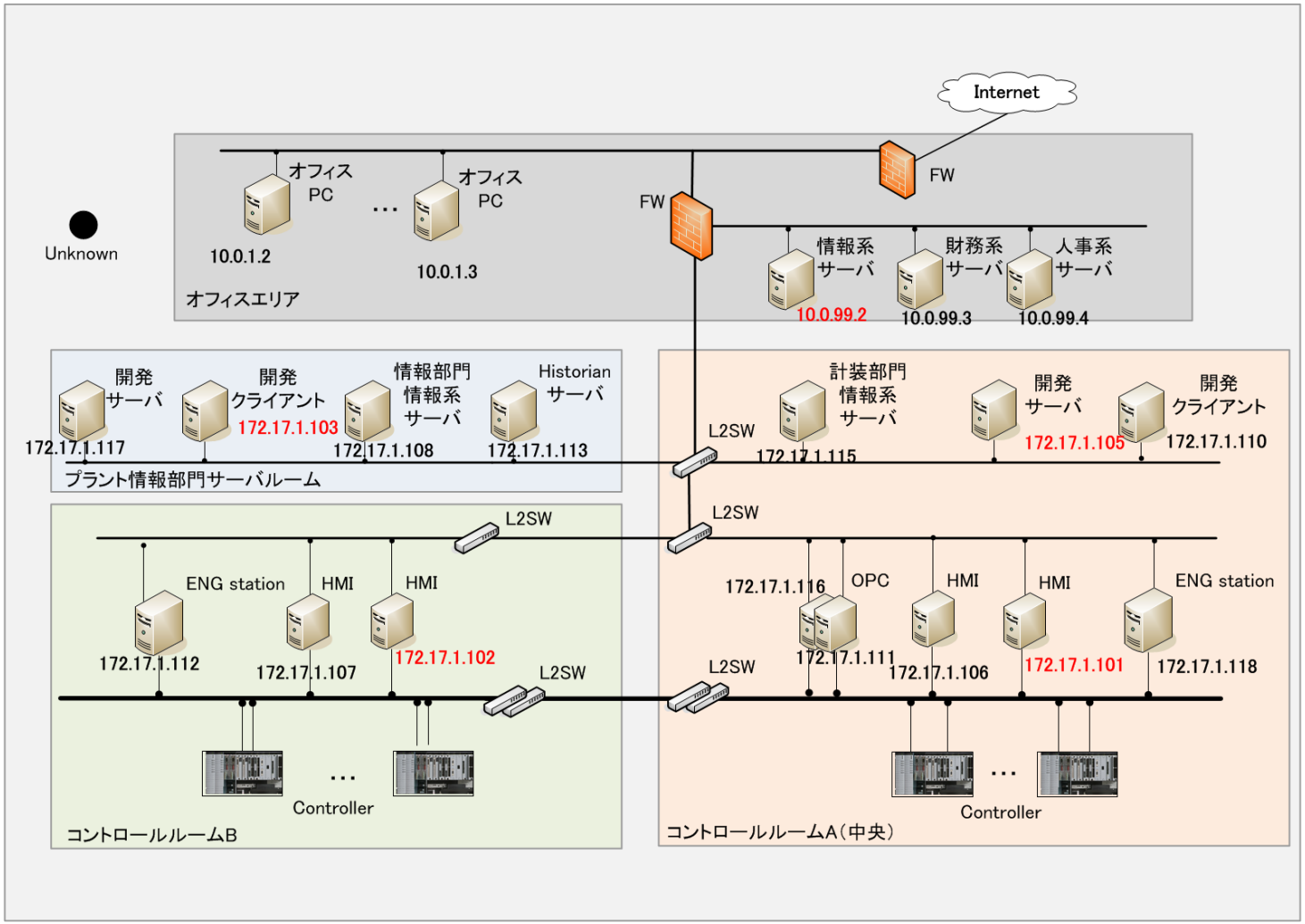
Network Incident analysis Center for Tactical Emergency Response

制御システムへのNIRVANAの適用

- **経緯**
  - ✓2007年～ 横河電機とNICTで共同研究を開始
  - ✓NICTから横河電機にNIRVANAを技術移転
  - ✓横河電機でNIRVANAを用いた
    制御システム向けセキュリティサービスを開始
  - ✓某プラントに於いて実証実験を実施

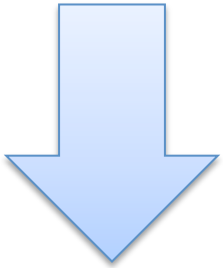
YOKOGAWA ◆ + NICT National Institute of Information and Communications Technology

典型的な制御系システムの構成



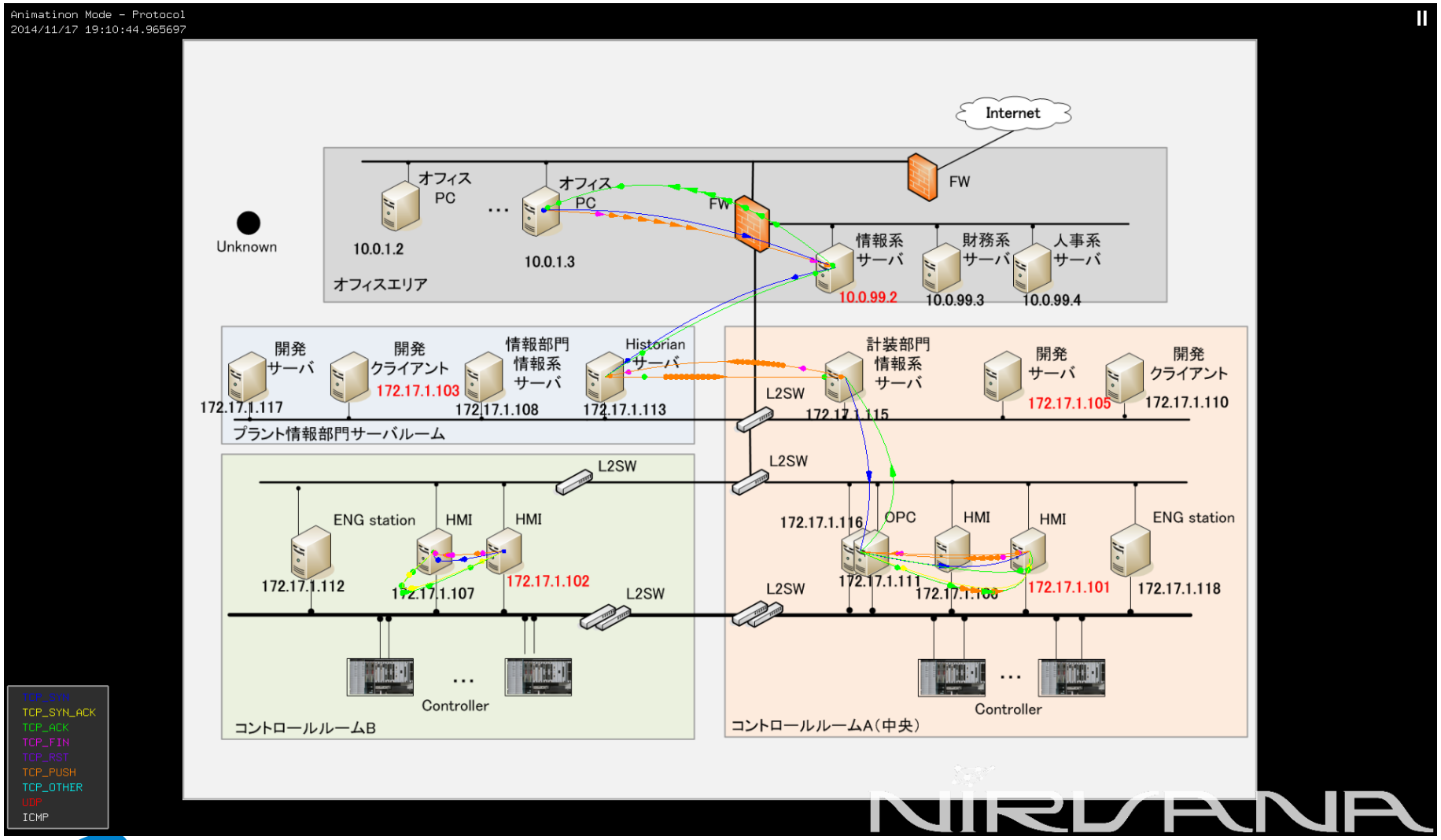
制御システムに関するGood News

- **ネットワーク機器の把握が比較的容易**
  - ✓機器構成は設計・構築時からほぼ固定
- **機器間の通信もほぼ固定**
  - ✓通信相手、通信内容ともほぼ不変



通常の通信状態を定義可能
（異常検出が比較的容易）

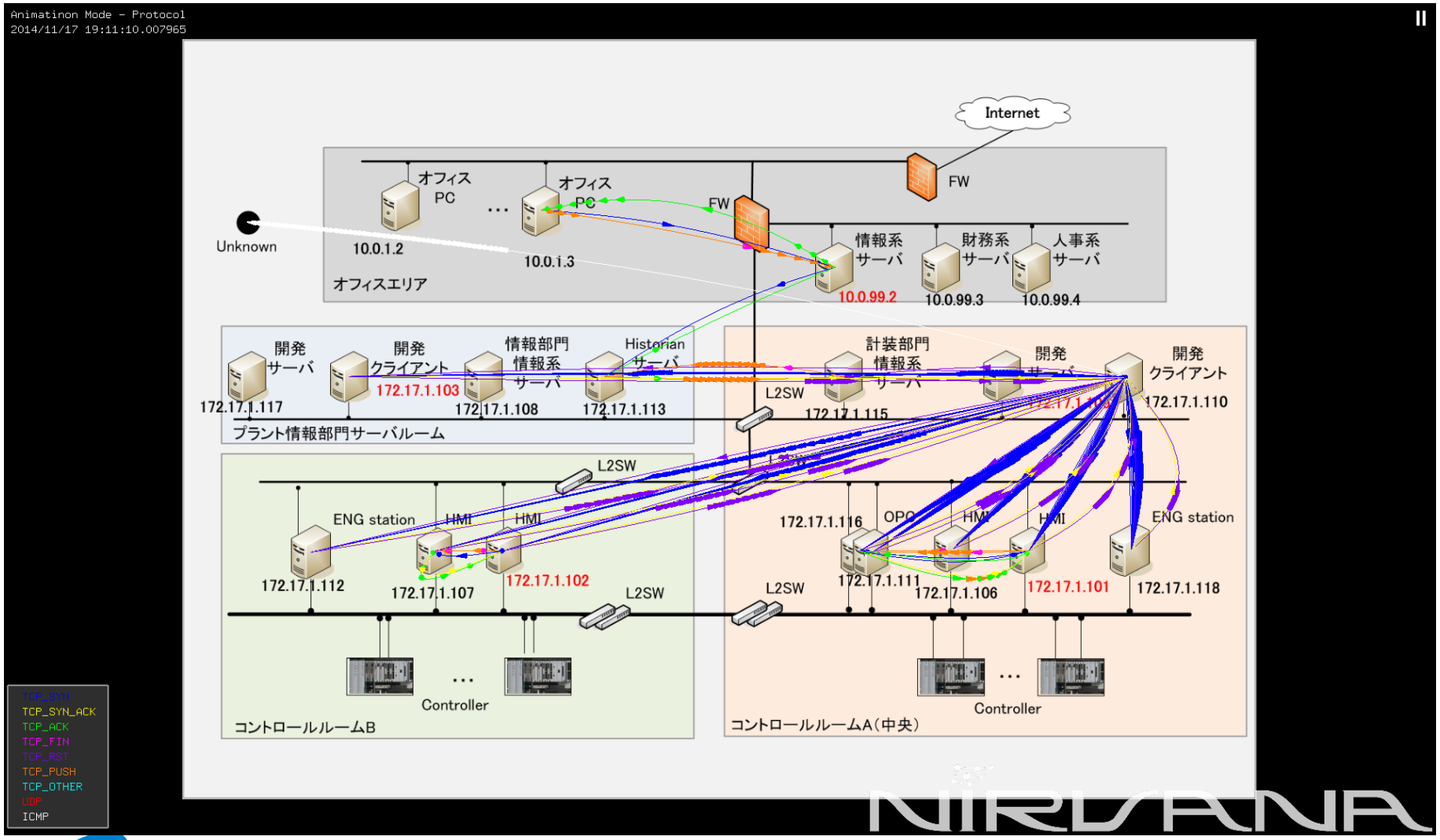
通常の通信状態



National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

異常な通信状態



National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

横河電機：ネットワーク健全性確認サービス

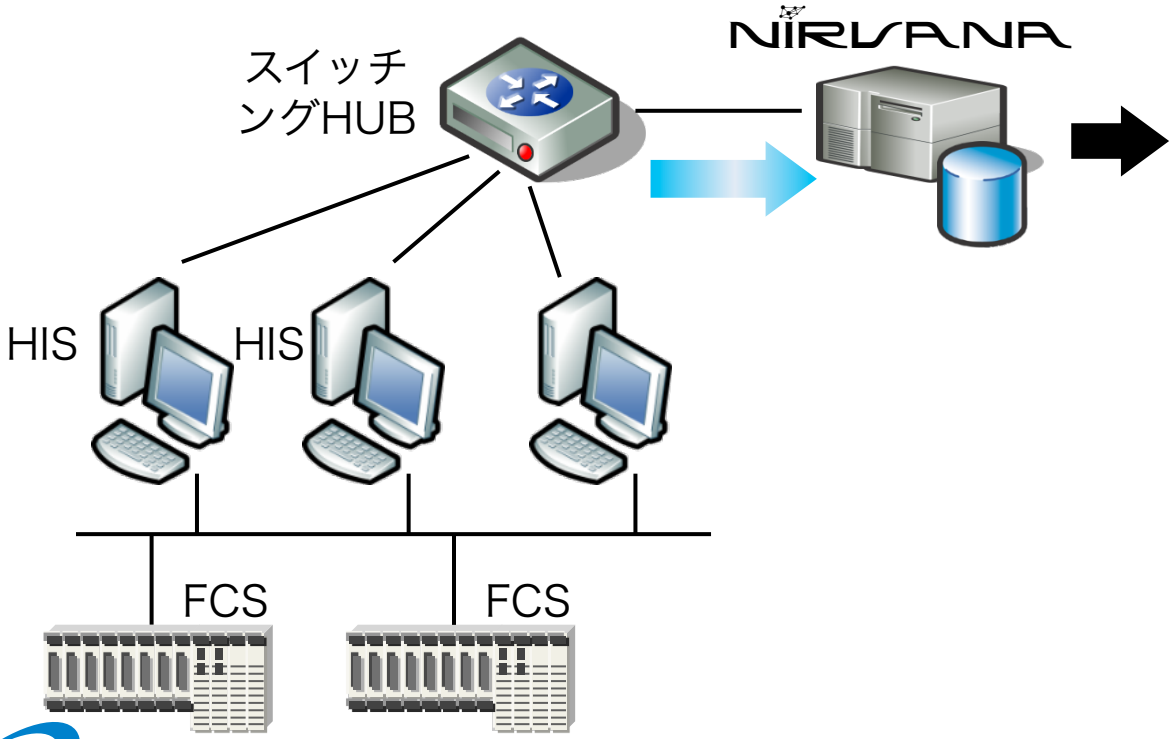
- NIRVANAによるネットワークモニタリング
- 送信元/宛先をマトリクス化し、通常の通信状態を学習
- 定期的にマトリクスの差分チェックを行い異常検知

National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

実証実験

- **実施場所**：石油加工品のプラント（2箇所）
- **実施期間**：2014年 3月末～10月末
- **実験方法**：NIRVANAを設置し、定期的な差分チェック



解析レポート

目に見えないネットワーク通信情報を分析し，健全性を評価した結果をレポートで提示
予期しない通信はピックアップし問題有無を調査

実証結果

- **異常検知例**
  - ✓新規通信パスの検出
    - 新規の送信元/宛先のペアを検出
    - 445/tcp（ファイル共有）
    - 3389/tcp（リモートデスクトップ）
  - ✓新規IPアドレス（固定）の検知
    - 初回学習時に確認されなかったIPアドレスを検知
  - ✓新規IPアドレス（DHCP割り当て失敗）
    - DHCPの割り当て失敗時のIPアドレスを検知

サイバー攻撃統合分析プラットフォーム

NICTER Real-network Visual ANAlyzer KAI

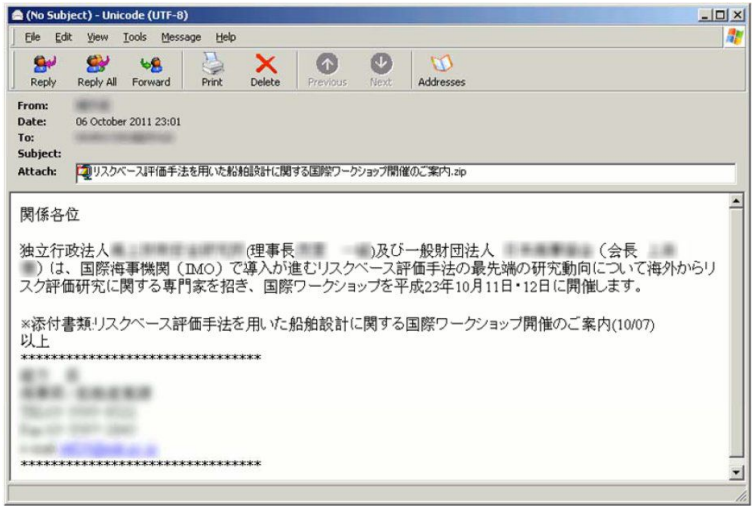
National Institute of Information and Communications Technology

NICTER
Network Incident analysis Center for Tactical Emergency Response

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

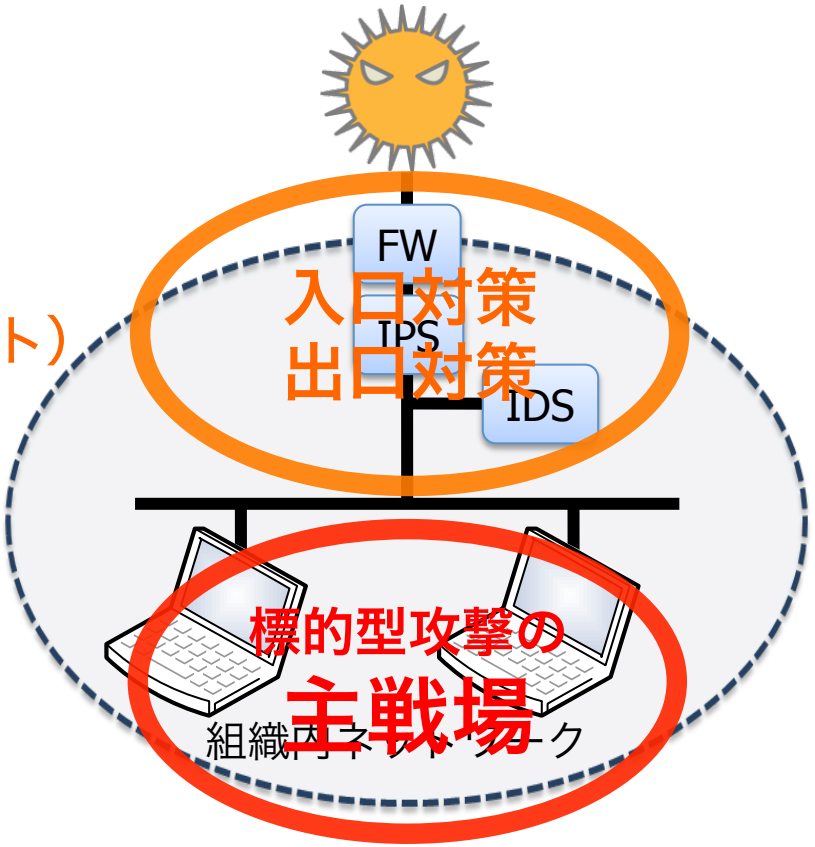


TECH.ASCII.jp「9.5社に1社が対象に！シマンテックが明かす日本の標的型攻撃」
http://ascii.jp/elem/000/000/652/652712/ （2011-11-30）

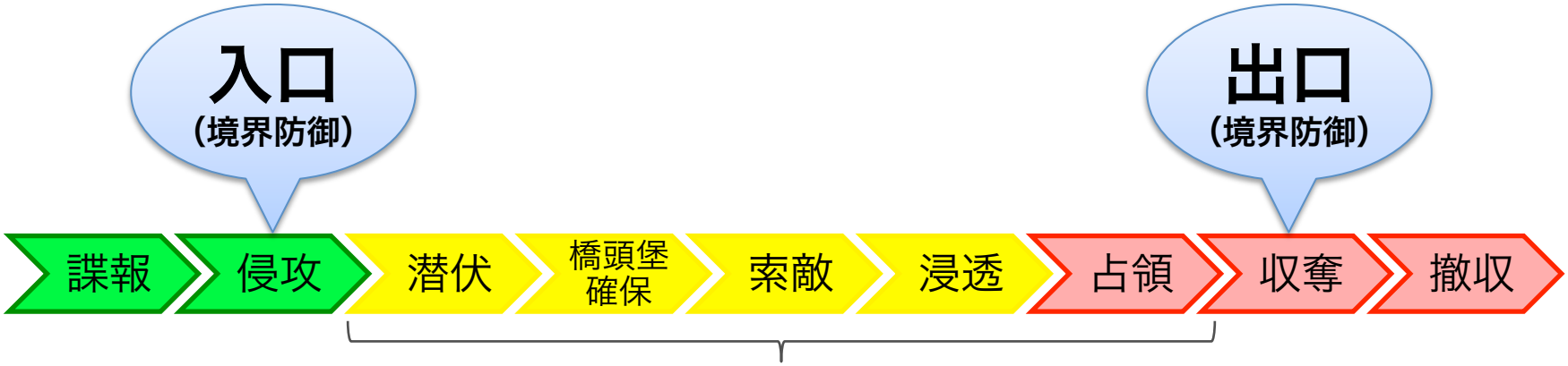
入口対策/出口対策

入口対策/出口対策 = 境界防御

- **FW**
  - ✓ 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**
  - ✓ 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**
  - ✓ シグネチャで攻撃を<u>防止（遮断）</u>
  - ✓ インライン



入口対策/出口対策



ネットワークの内側でも対策を！

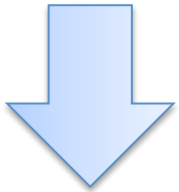
（組織内ネットワークのリアルタイム観測・分析）

NIRVANA改

= NIRVANA ＋ セキュリティ分析機能

NIRVANA改

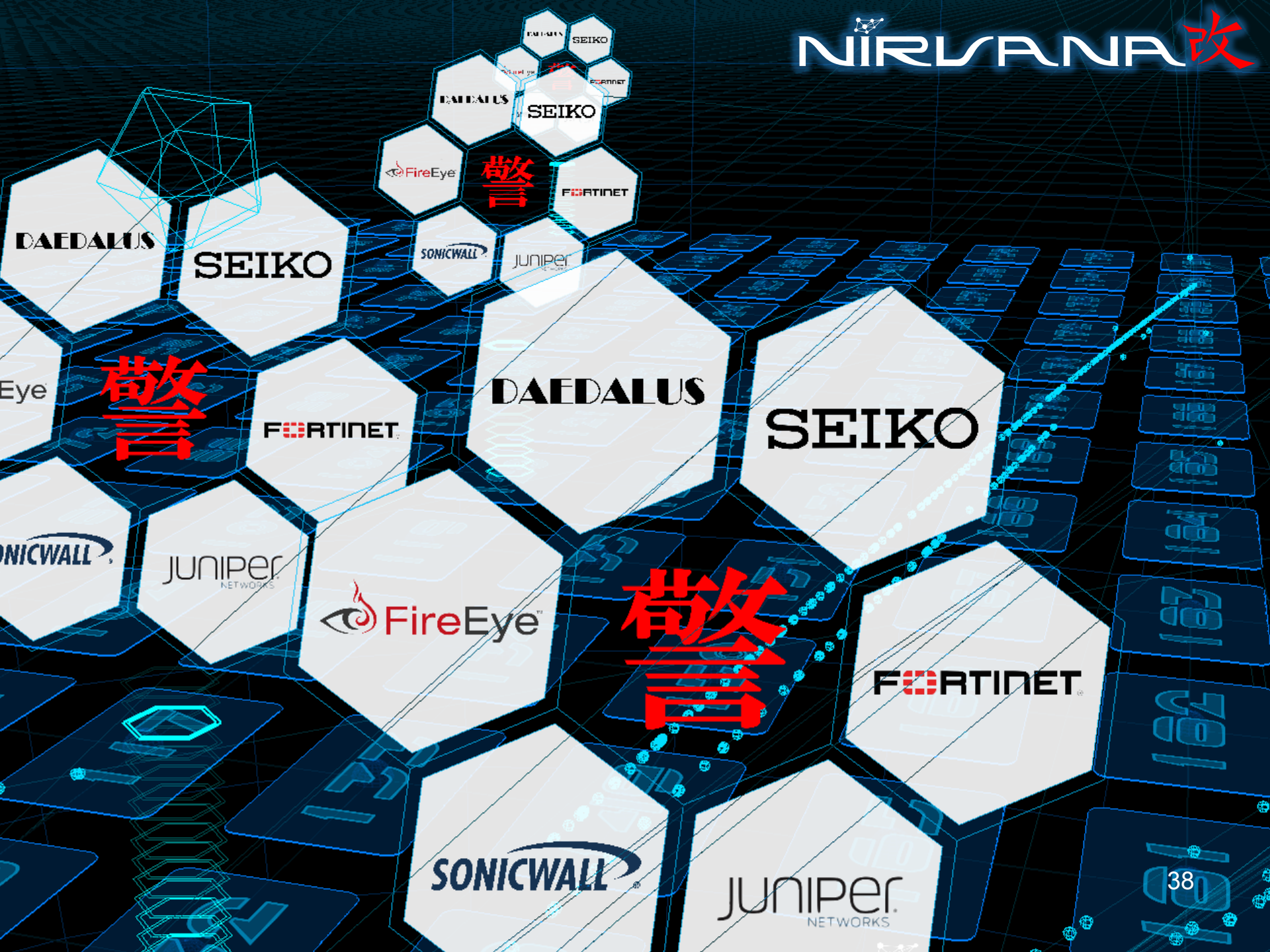
- NIRVANAによるライブネット観測
- 各種の**リアルタイム分析エンジン**（新規開発中）
- 既存セキュリティアプライアンスのアラート集約
- 各種アラートを基にした**メタ分析**（相関分析）
- ドリルダウン機能付き可視化エンジン



組織内ネットワークを守る

統合分析プラットフォーム

の確立に向けて研究開発中


NIRVANA改
DAEDALUS
SEIKO
FireEye
警
FORTINET
SONICWALL
JUNIPER
NETWORKS

現在開発中！

- **NIDS（ネットワークベースの侵入検知）**
  - ✓ ホワイトリスト検知エンジン
  - ✓ ブラックリスト検知エンジン
  - ✓ スロースキャン検知エンジン etc.

- **HIDS（ホストベースの侵入検知）**
  - ✓ FFRI Yaraiとの連携
  - ✓ カーネル内観測・分析エンジン
  - ✓ プロセス–通信突合エンジン etc.

- **NIDS-HIDS連携システム**
- **メタ分析フレームワーク**
- **防御エンジン（アクチュエーション）** etc. etc...

まとめ

- **ダークネット：広がる応用・高まる効用**
  - ✓ ワーム型マルウェアの傾向把握・大規模感染検知
  - ✓ 国内外・産学官へのアラート提供
  - ✓ Linux組込機器がターゲットに
- **ライブネット：入口/出口、次の一手**
  - ✓ 組織内ネットワークのリアルタイム観測・分析
  - ✓ 新規＆既存対策技術を統合したメタ分析
  - ✓ 制御システムへの適用

Made in Japanのサイバーセキュリティ技術を日本に、そして世界に！