nicter/DAEDALUS/NIRVANAが拓く
サイバーセキュリティの新たな地平

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
サイバーセキュリティ研究室
井上 大介

nicter video → http://www.youtube.com/watch?v=jLYs52OBh_A
DAEDALUS video → http://www.youtube.com/watch?v=f44eum6Hz50

NICT
nicter Network Incident Analysis Center for Tactical Emergency Response

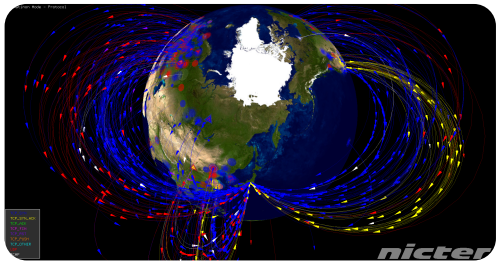
過去5年間の主なセキュリティ事案

- 2008年： Conficker（過去最悪の大規模感染ワーム）
- 2009年： Gumbler（Web媒介型攻撃）
- 2010年： Stuxnet（重要インフラ向けマルウェア）
- 2011年： Sonyへの大規模DDoS攻撃（Hacktivism）
  標的型攻撃（Cyber Espionage）
- 2012年： 不正ポップアップマルウェア（Online銀行）
  遠隔操作ウイルス（愉快犯？）

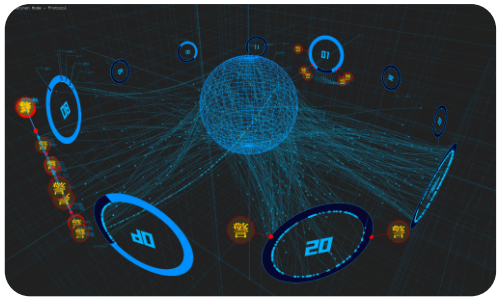
攻撃対象拡大、攻撃手法高度化

nicterとそのスピンオフ技術たち

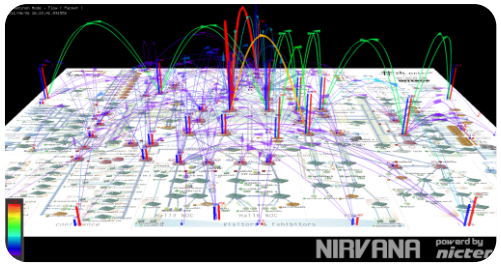
1. インシデント分析センター
   nicter



2. 対サイバー攻撃ラートシステム
   DAEDALUS

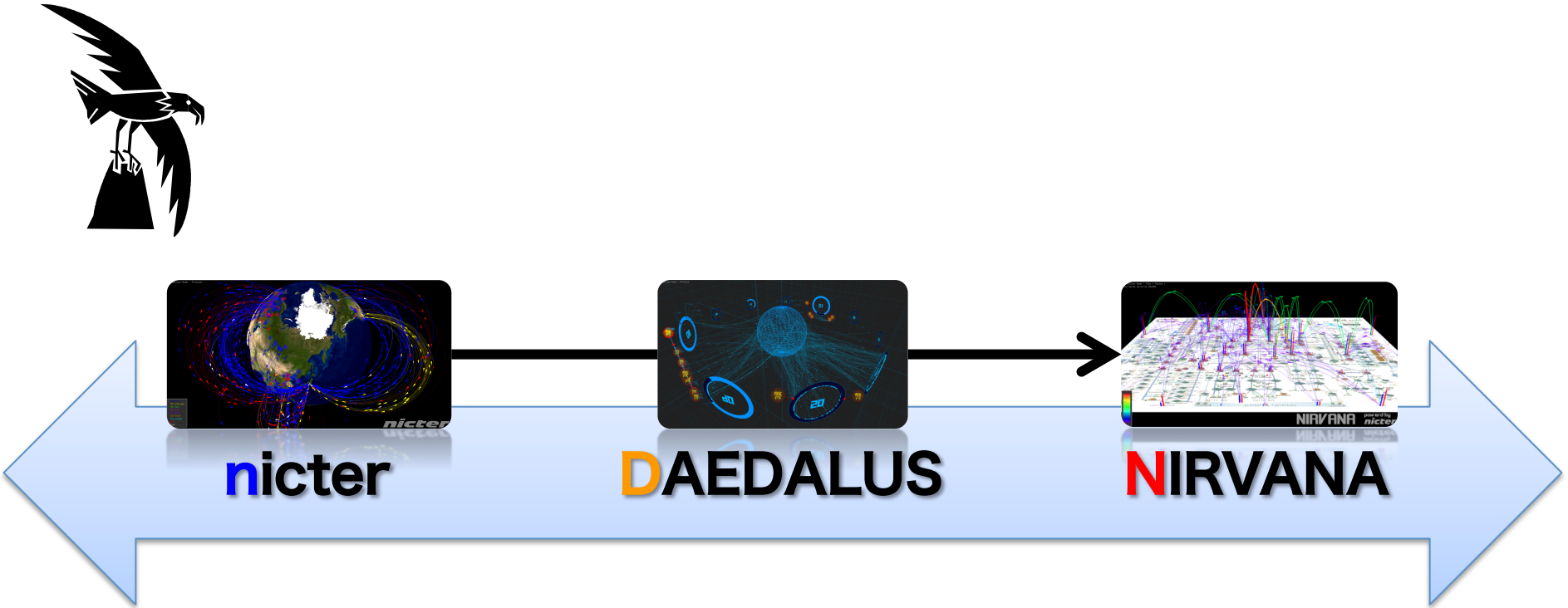


3. ネットワークリアルタイム可視化システム
   NIRVANA



nicter Network Incident Analysis Center for Tactical Emergency Response

鳥の目/虫の目



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）

Network Incident Analysis Center for Tactical Emergency Response

インシデント分析センタ

nicter

(Network Incident analysis Center for Tactical Emergency Response)

インシデント分析センタ nicter 概要

nicter = **N**etwork **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse

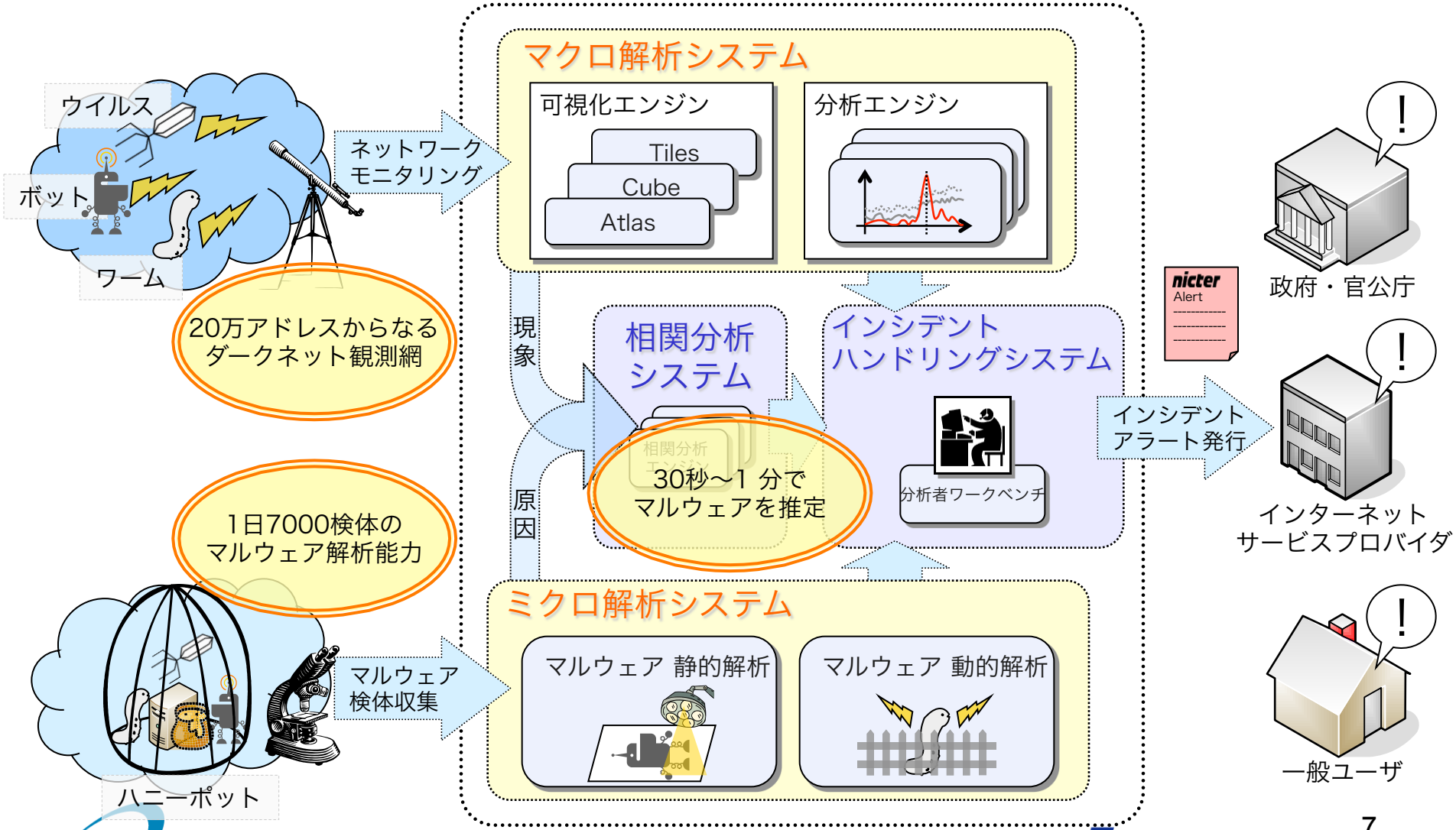
目的:

広域ネットワークにおけるセキュリティインシデント（セキュリティ事故）の迅速な状況把握・原因究明・対策導出。

主要コンポーネント

- マクロ解析システム （ネットワークモニタリング）
- ミクロ解析システム （マルウェア解析）
- マクロ-ミクロ相関分析システム （マクロとミクロの融合）

nicter の全体像



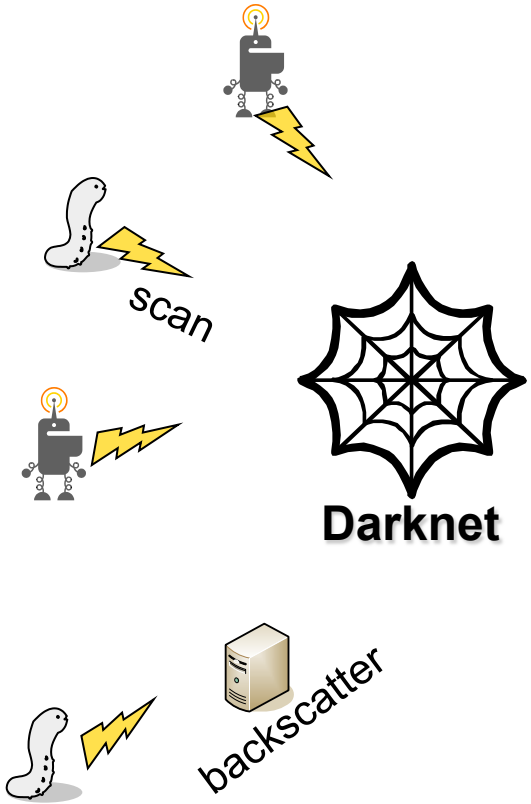
NICT

nicter Network Incident Analysis Center for Tactical Emergency Response

ダークネットとは？

- ユーザマシンやサーバが接続されていない
  未使用アドレスブロック

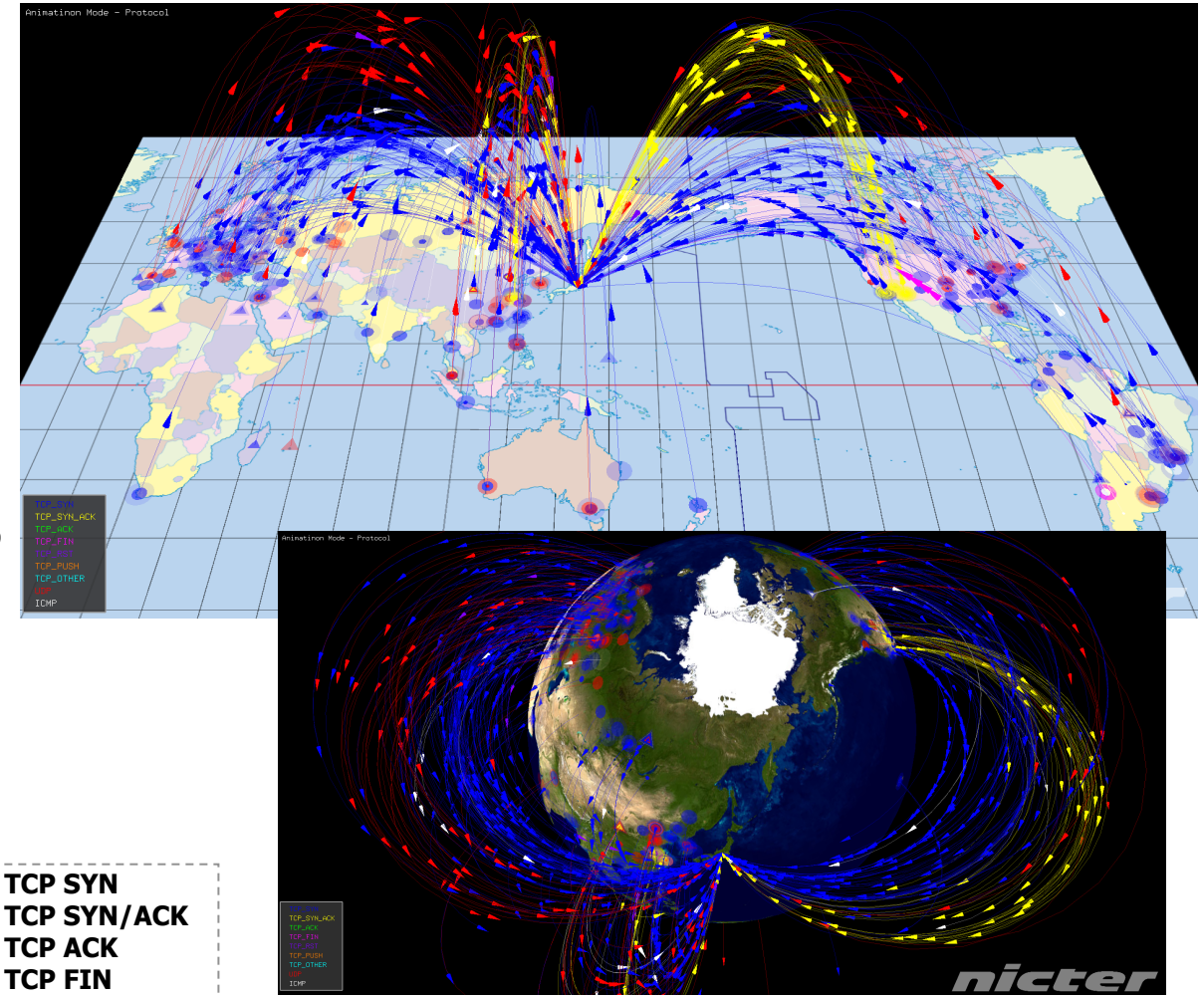
- ダークネットトラフィックはなぜ発生？
  - ✓ マルウェアによるスキャンや攻撃
  - ✓ DDoS攻撃の跳ね返り（Backscatter）
  - ✓ 設定ミス



- ダークネット観測のメリット
  1. 通信の秘密に抵触しない
     → ネットワークの端点で自分宛の通信のみ観測。
  2. 観測データに正・不正の区別がいらない
     → 飛んで来たものは全て不正な通信。
  3. パッシブモニタリング
     → 待っているだけで定常的に通信が到来。

Atlas: 世界地図上での可視化エンジン

- ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し世界地図上で可視化
- 色：パケットごとにプロトコルやTCPのフラグを表現
- 高度：ポート番号に比例（対数軸）



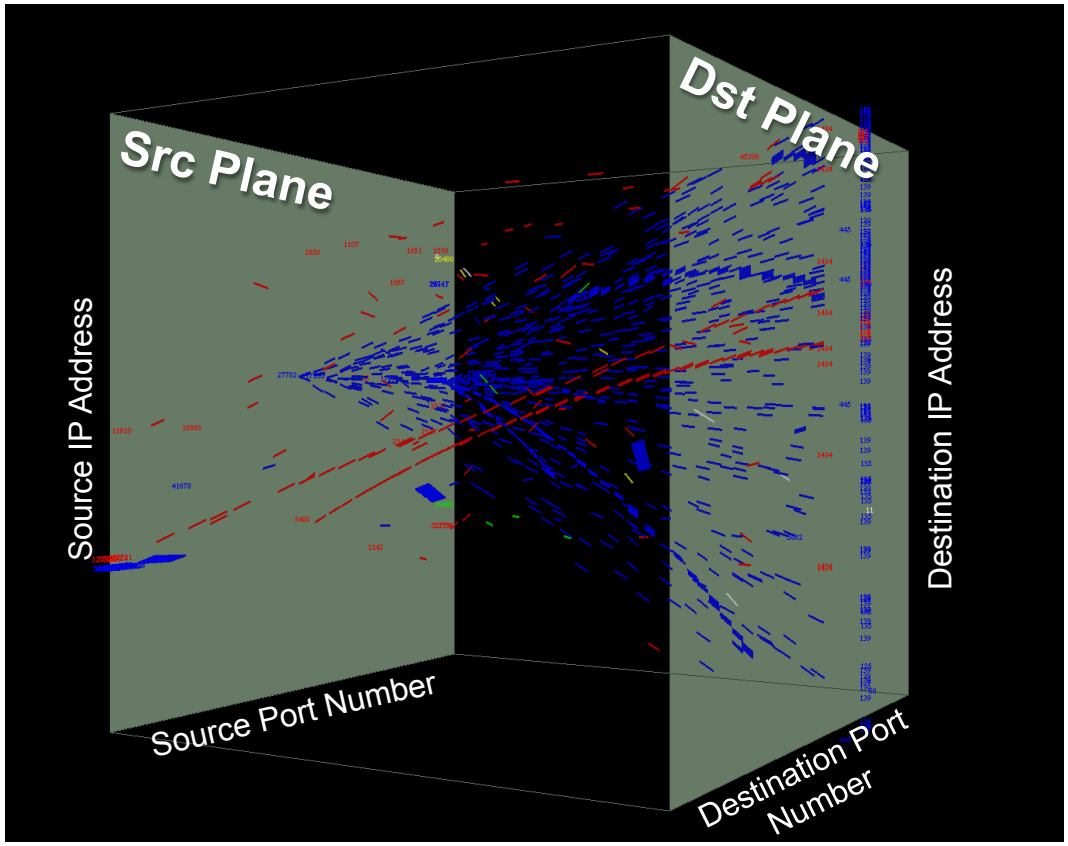
- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

NICT

nicter Network Incident Analysis Center for Tactical Emergency Response

Cube: 3次元空間上での可視化エンジン

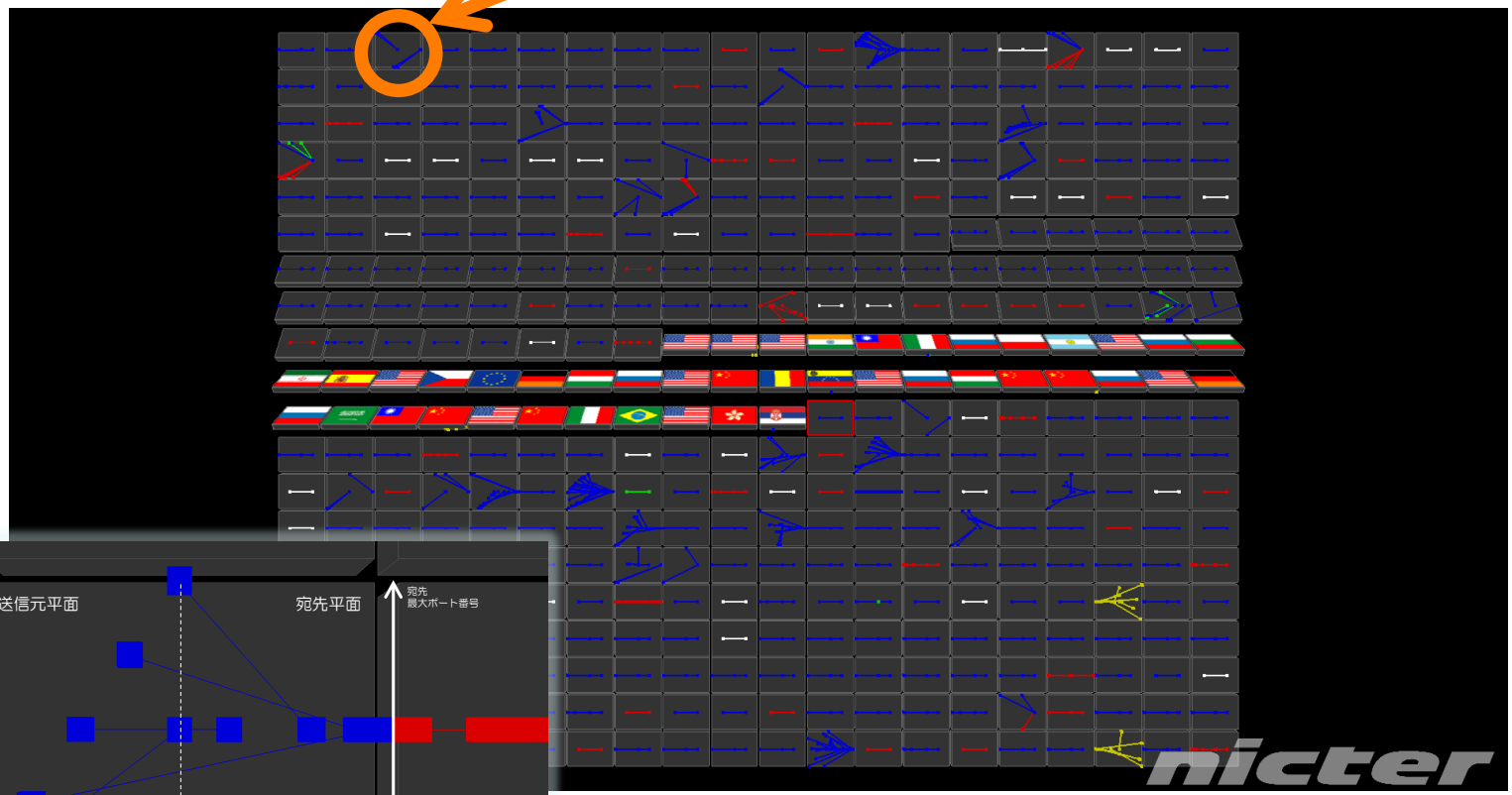
- ダークネットに飛来するパケットを3次元の立方体中に可視化
- 左平面：送信元
  右平面：宛先
- 縦軸：IPアドレス
  横軸：ポート番号

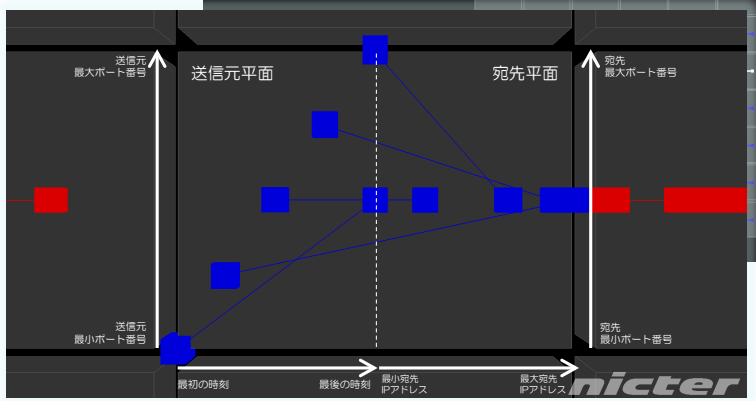


- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

Tiles: 振舞分析エンジン

- 1ホストごとの30秒間の挙動を1つのタイルで表現
- ホストの挙動は自動分類されデータベースに蓄積される
- 蓄積された情報を基に新規の攻撃パターンを検出可能





nicter Network Incident Analysis Center for Tactical Emergency Response

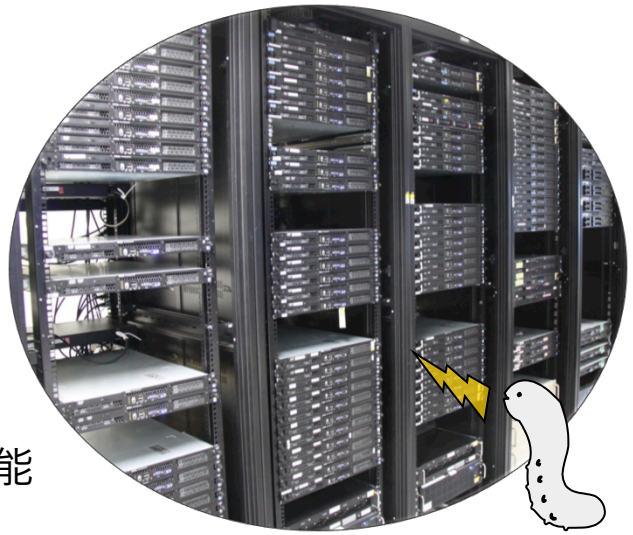
ミクロ解析システム

目的：

- 隔離環境下でのマルウェアの完全自動解析
- マルウェアの内部的挙動および外部的挙動を抽出

特徴：

- 完全自動解析システム
  - OS復元機能付き実マシン上でマルウェアを実行
  - 隔離環境の中にダミーインターネットを構築
- 1検体あたり6～10分で解析完了
  - 並列化で1日約7000検体の大規模動的解析が可能

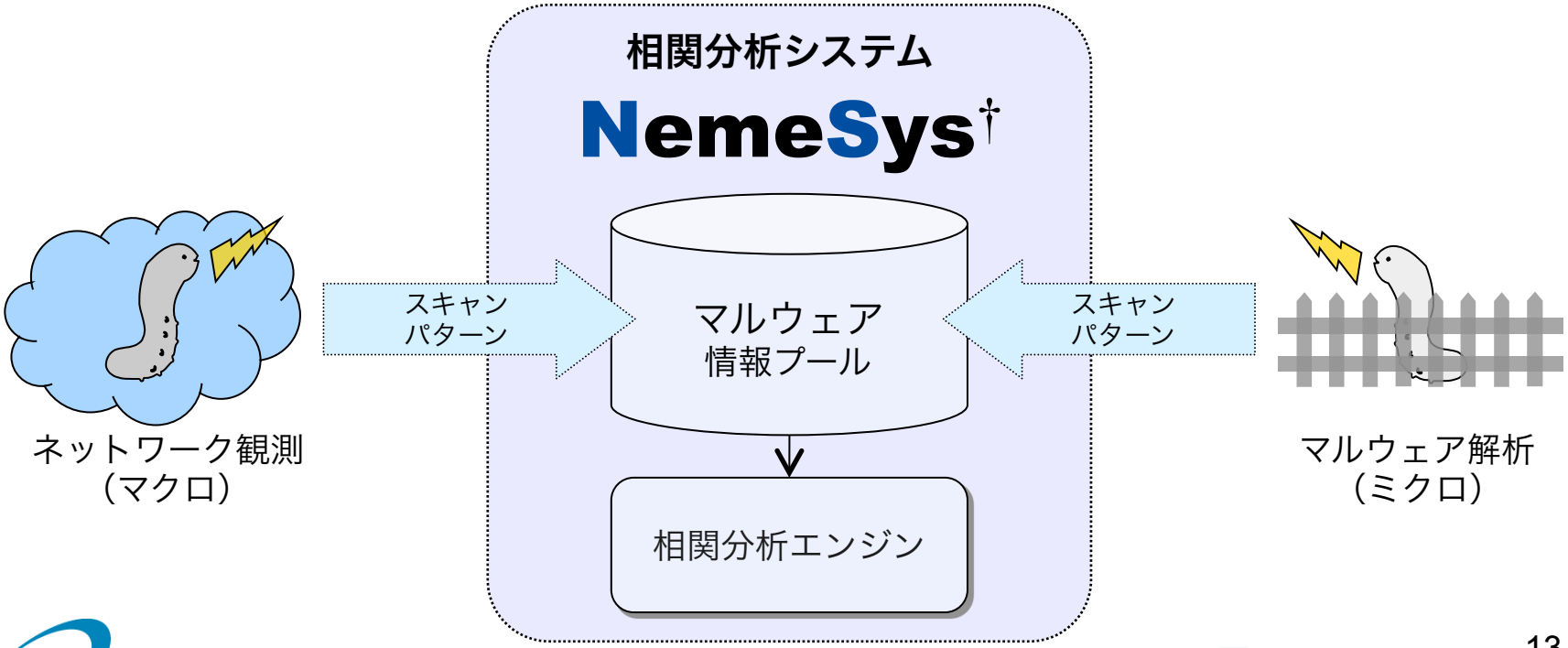


ミクロ解析システム概観

マクロ-ミクロ相関分析システム

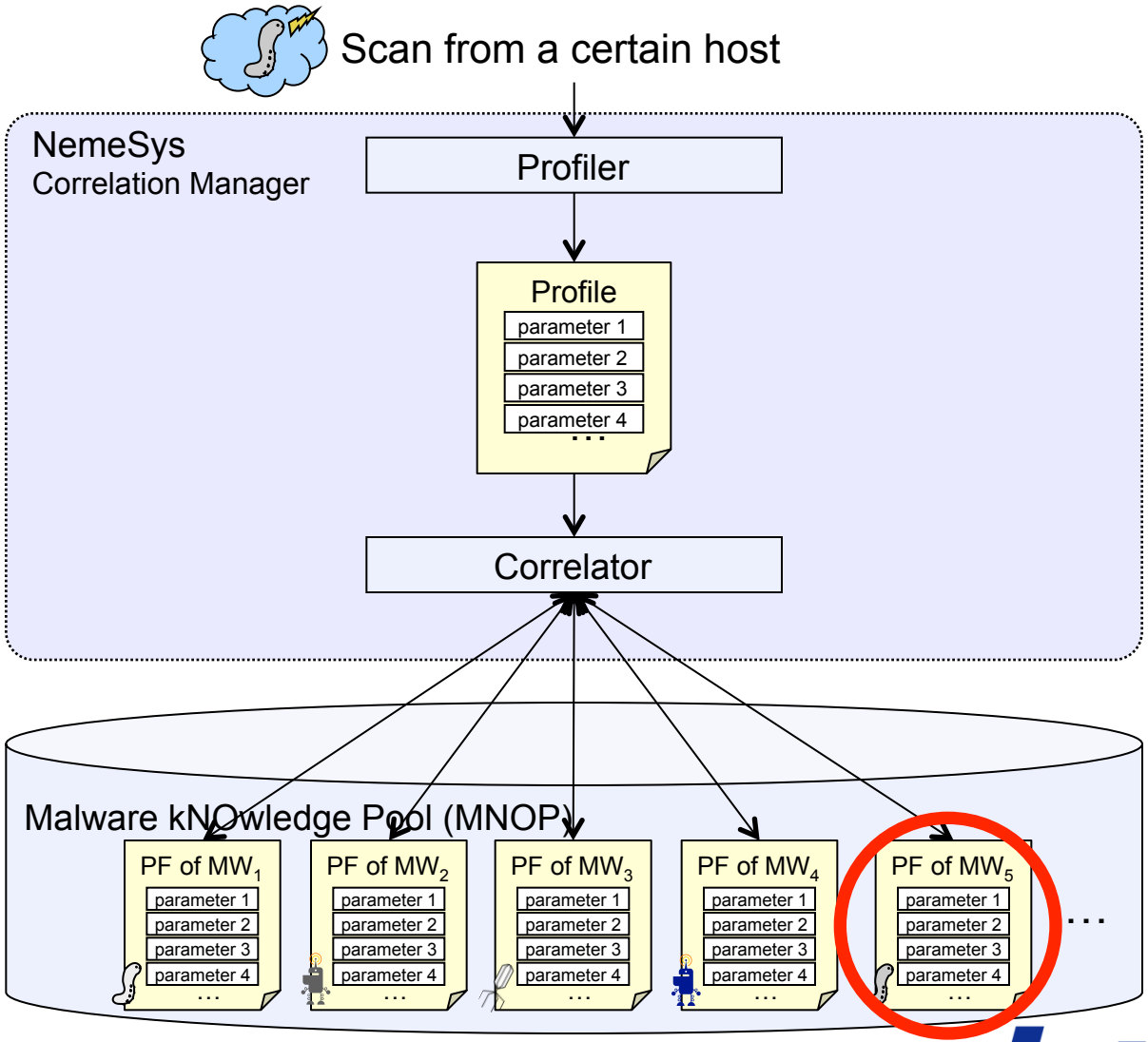
目的：

マクロ解析システムにおいて観測されたスキャンと
ミクロ解析システムにおけるマルウェアのスキャンの
相関を調べることで、現象と原因を関連付ける。



†network and malware enchaining system

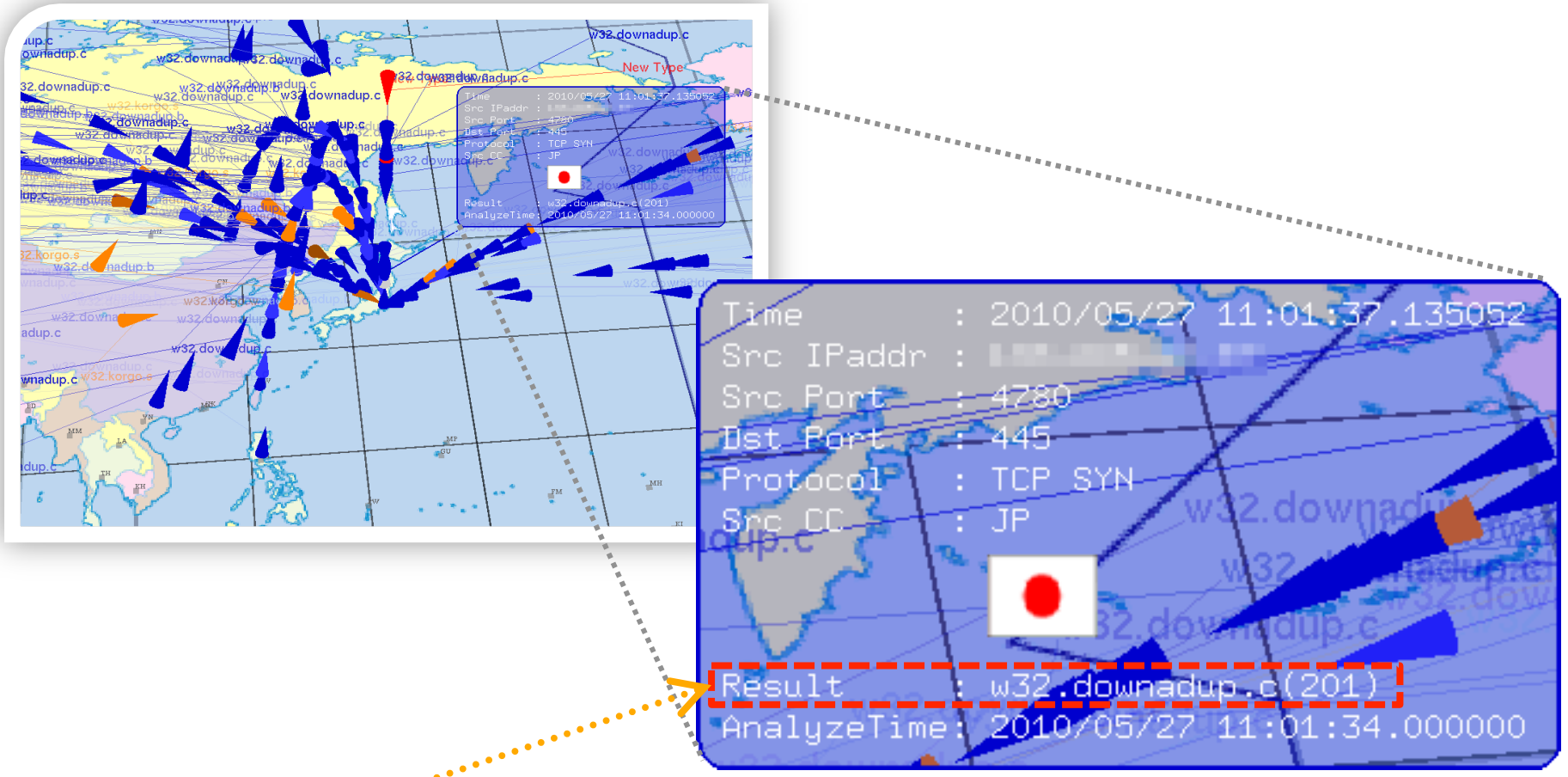
マクローミクロ相関分析システム 概観



1st Candidate

Network Incident Analysis Center for Tactical Emergency Response

相関分析結果のリアルタイム可視化 (1/2)

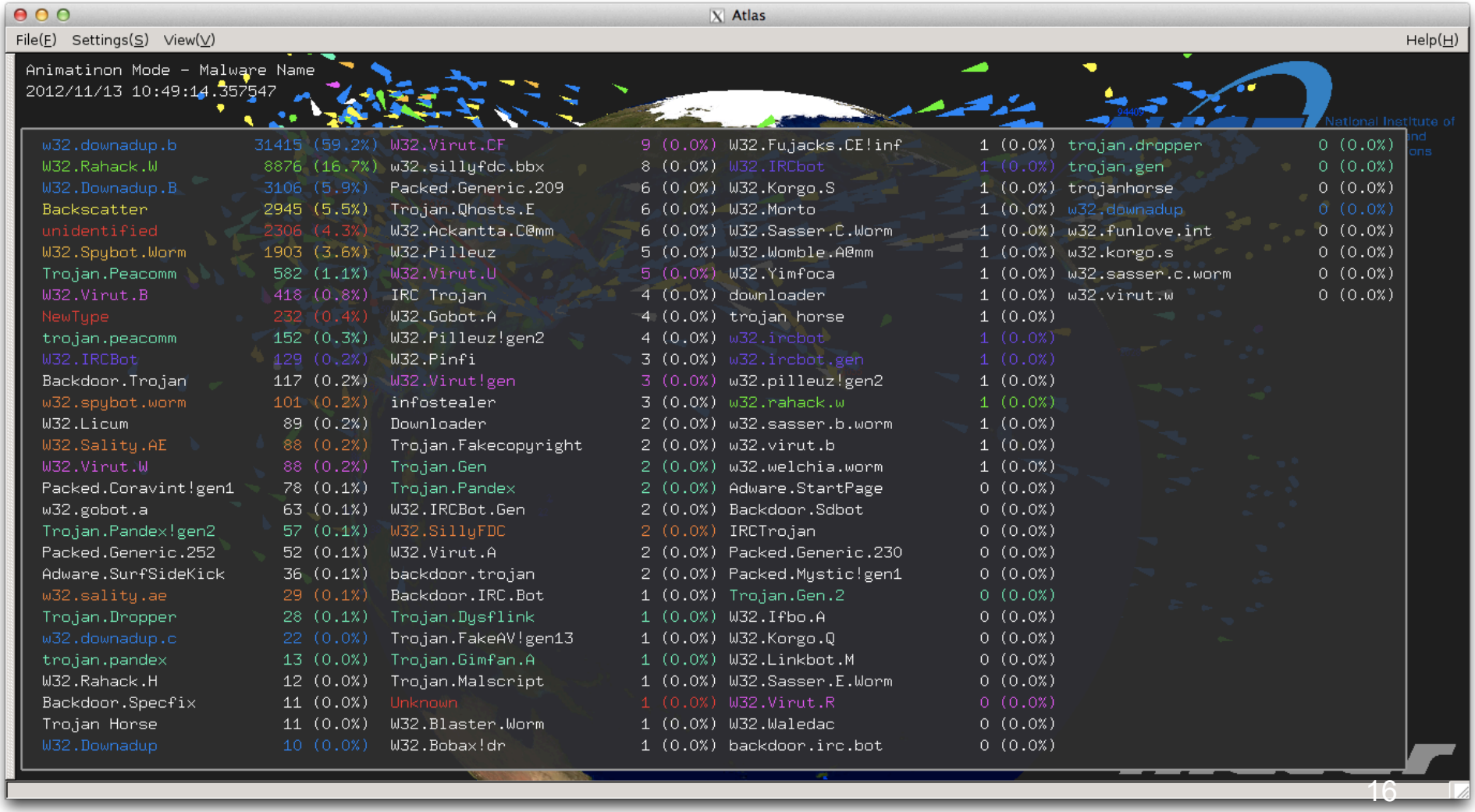


ダークネットへの攻撃を行ったホストに
感染しているマルウェアをリアルタイムで特定

NICT

nicter Network Incident Analysis Center for Tactical Emergency Response

相関分析結果のリアルタイム可視化 (2/2)



nicterアラートシステム

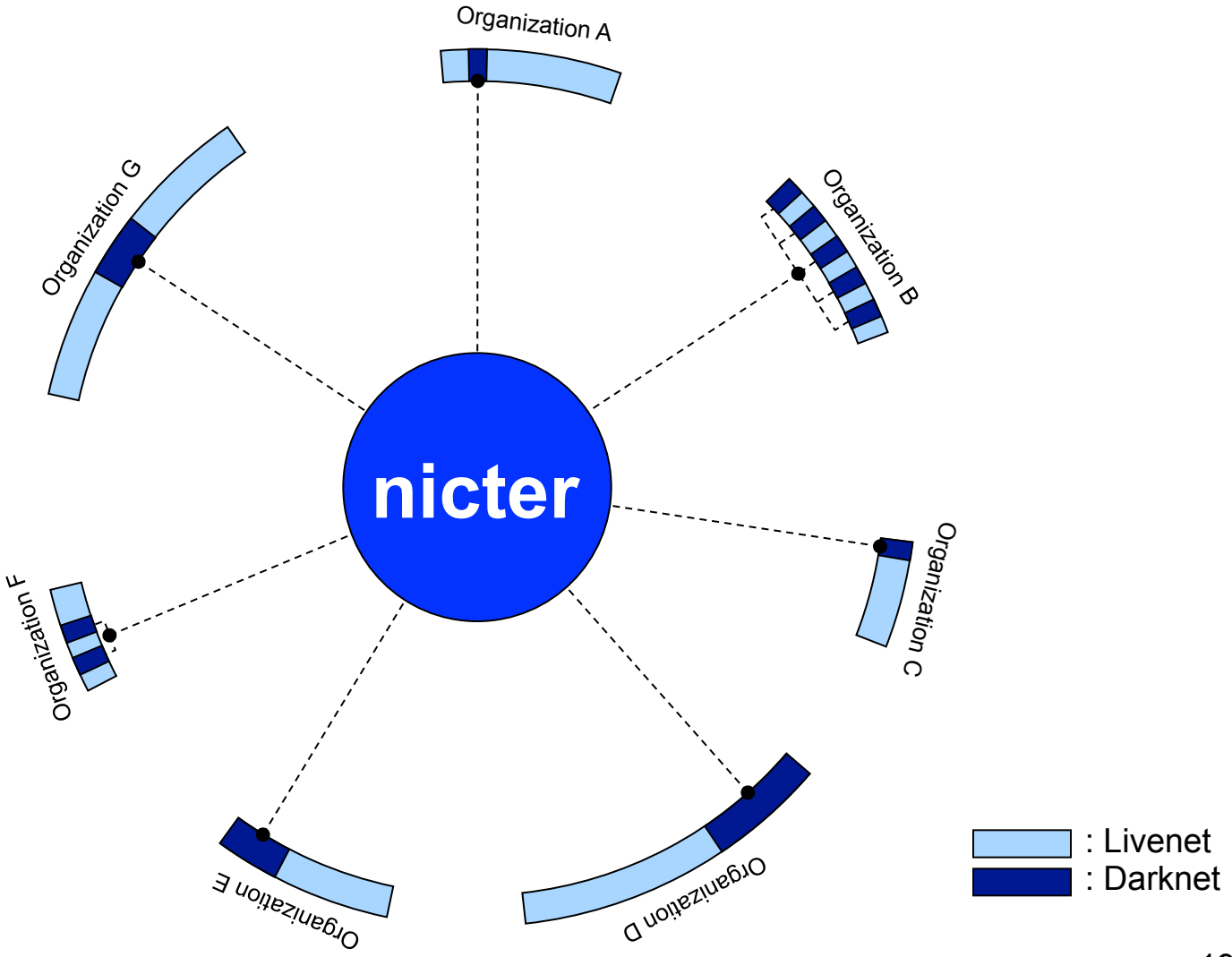
DAEDALUS

(Direct Alert Environment for Darknet And Livenet Unified Security)

基本アイデア

登録されたIPアドレスから
ダークネットに飛んできたら
アラート。

想定環境



Network Incident Analysis Center for Tactical Emergency Response

DAEDALUS：アラート送信の3ケース

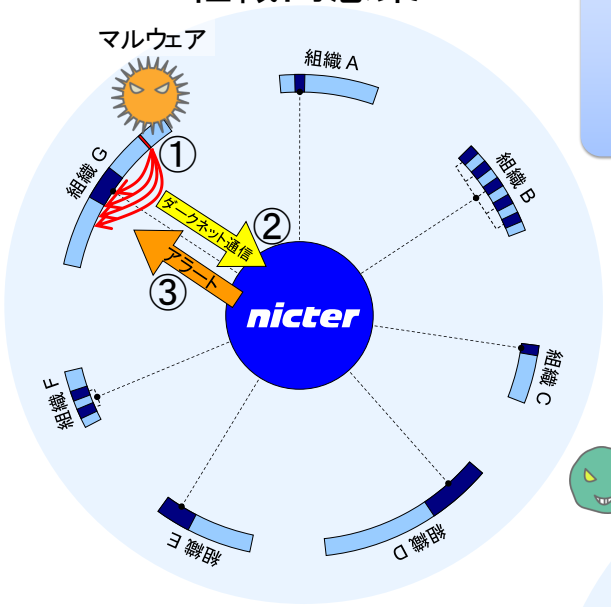
DAEDALUSの仕組み（3ステップ）

① マルウエアや攻撃者が攻撃パケットを送信。

② nicterがダークネット通信を収集・分析し、観測対象組織からの攻撃パケット（またはDoS攻撃の跳ね返り）を検出。

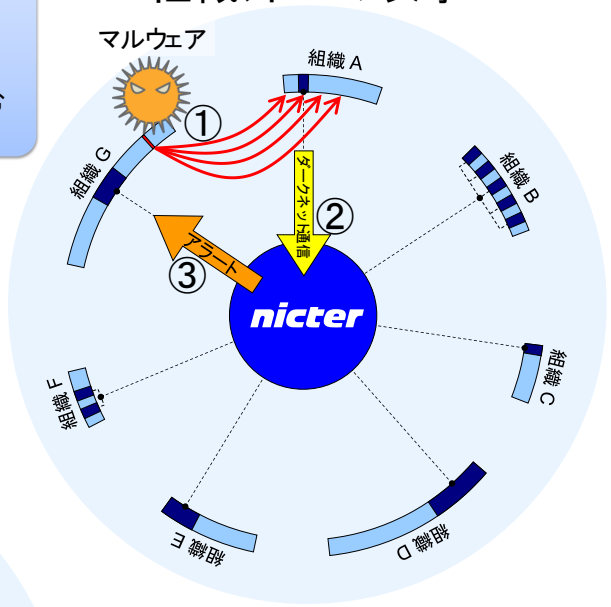
③ 観測対象組織へ攻撃ホストの情報を含むアラートを送信。

【ケース1】
組織内感染

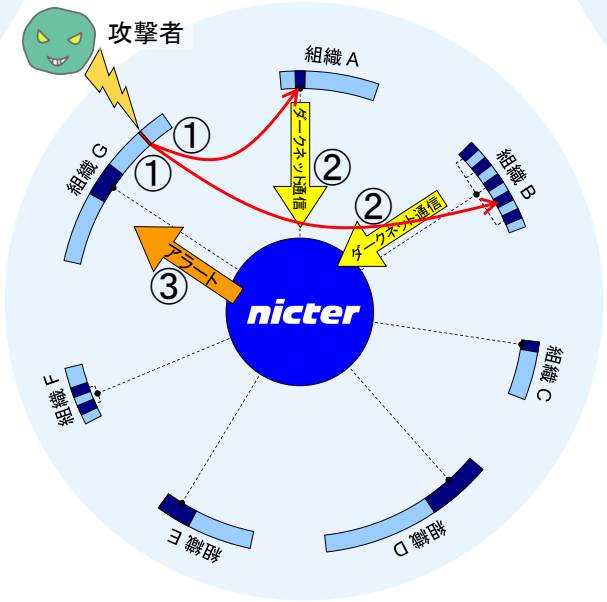


：ライブネット
：ダークネット

【ケース2】
組織外への攻撃



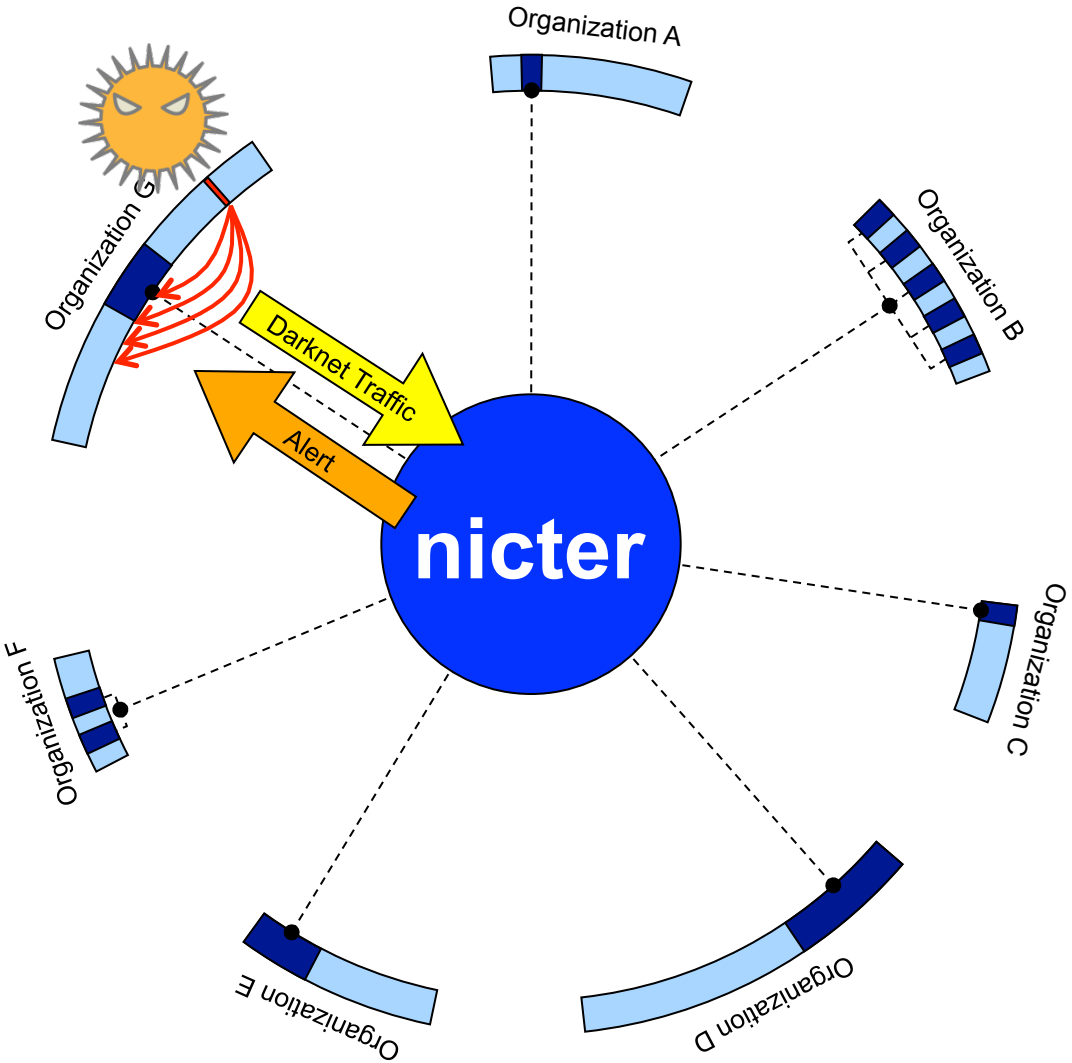
【ケース3】
DoS攻撃の跳ね返り



Network Incident Analysis Center for Tactical Emergency Response

ケース1

組織内感染（内部アラート）

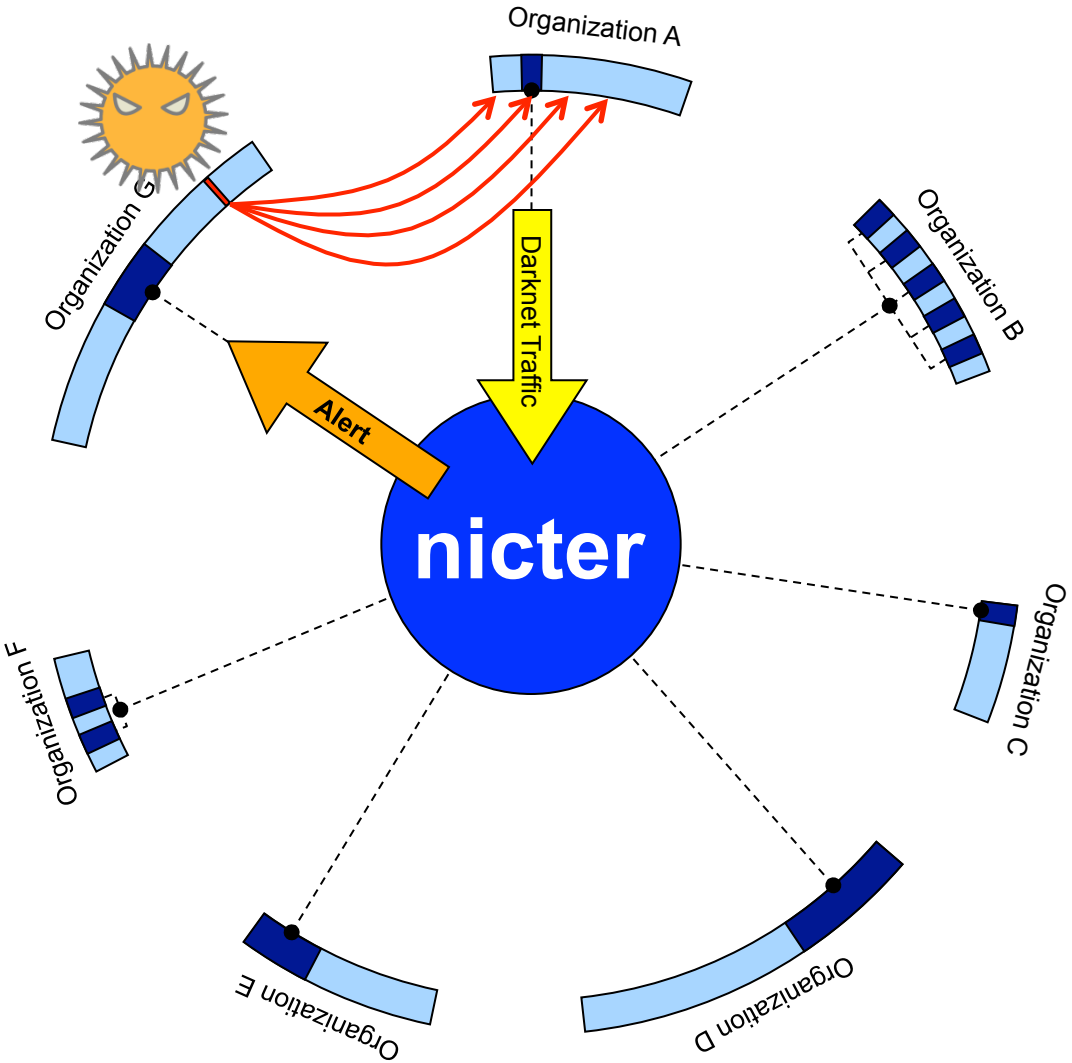


NICT

nicter Network Incident Analysis Center for Tactical Emergency Response

ケース2

組織外への攻撃（外部アラート）

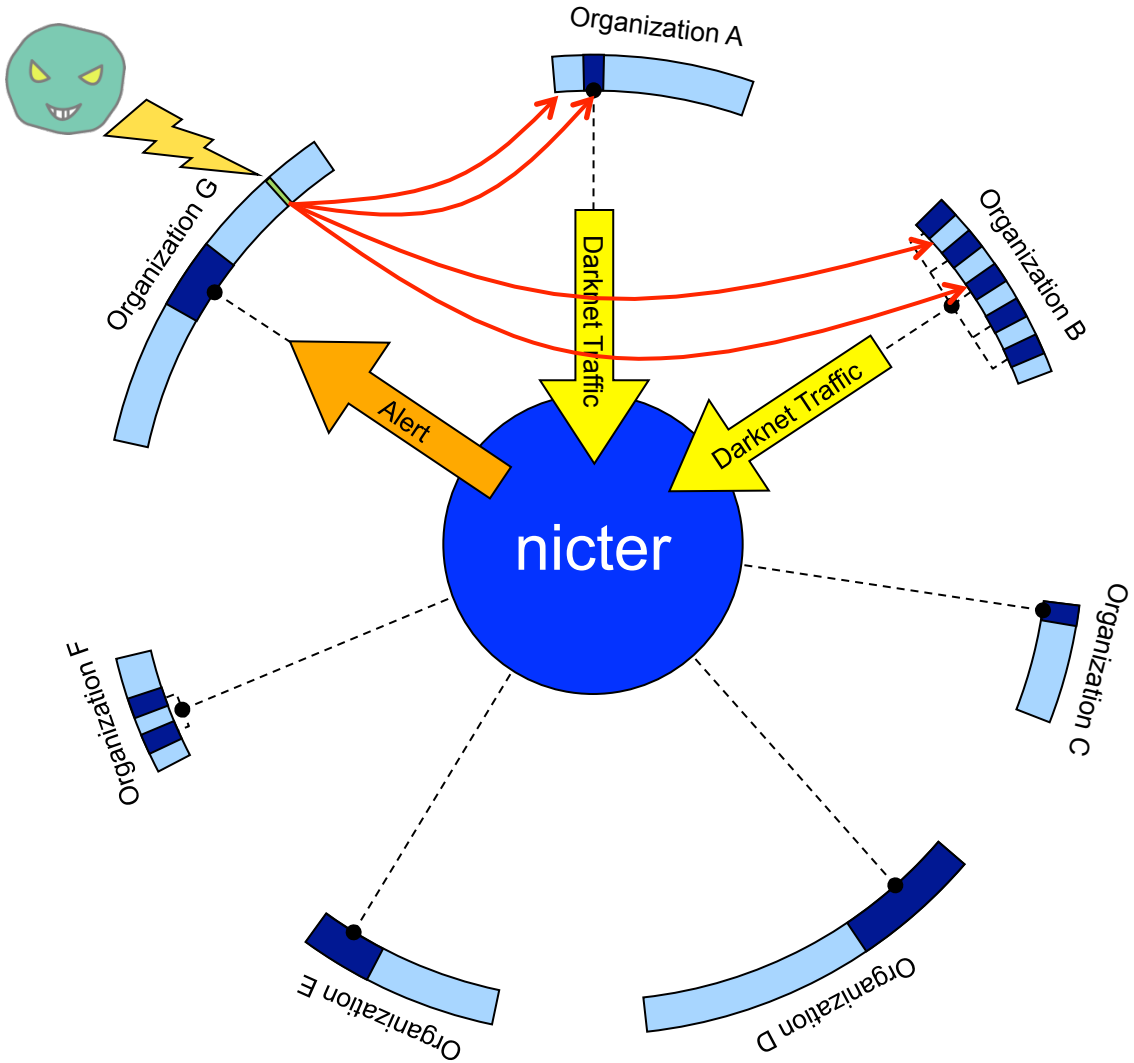


NICT

nicter Network Incident Analysis Center for Tactical Emergency Response

ケース3

DDoS攻撃の跳ね返り（バックスキャッタ）




DAEDALUS-VIZ
(DAEDALUS可視化エンジン)

ネットワークリアルタイム可視化システム

NIRVANA

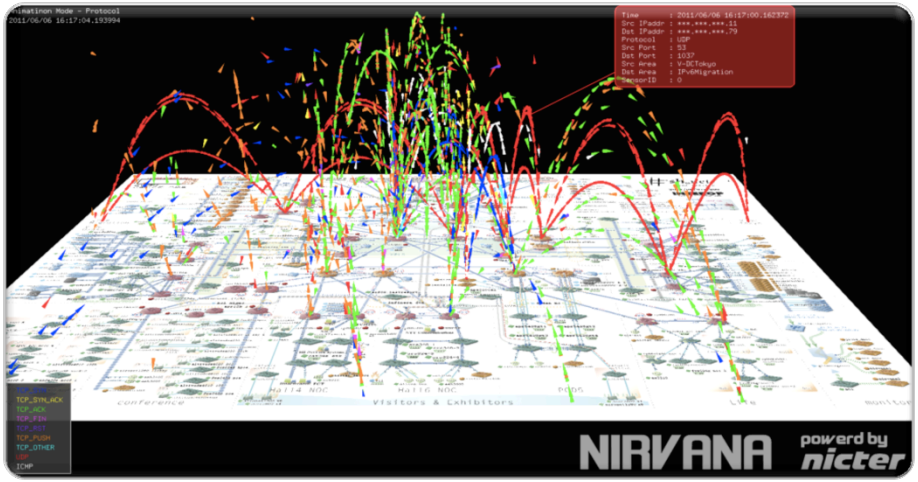
(nicter real-network visual analyzer)

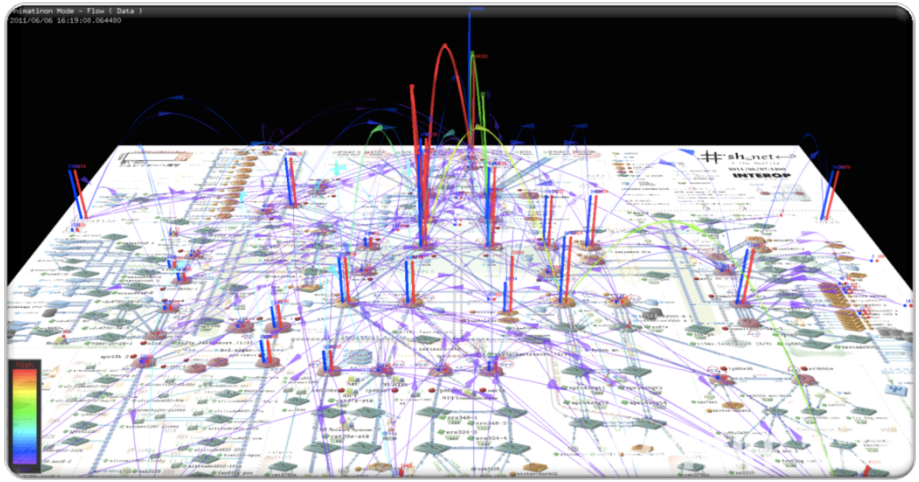
NIRVANA：目的

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）



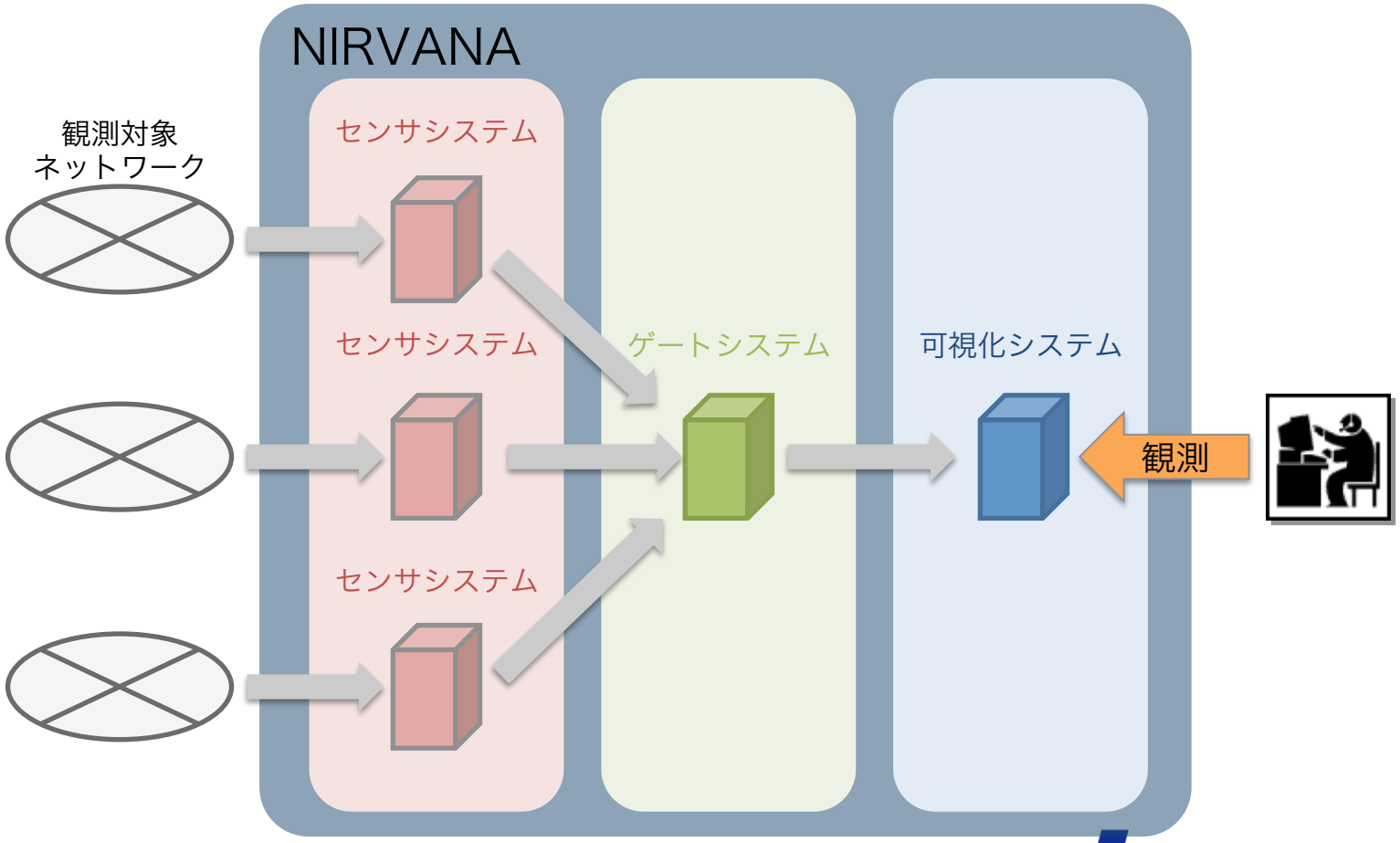


NICT

nicter
Network Incident Analysis Center for Tactical Emergency Response

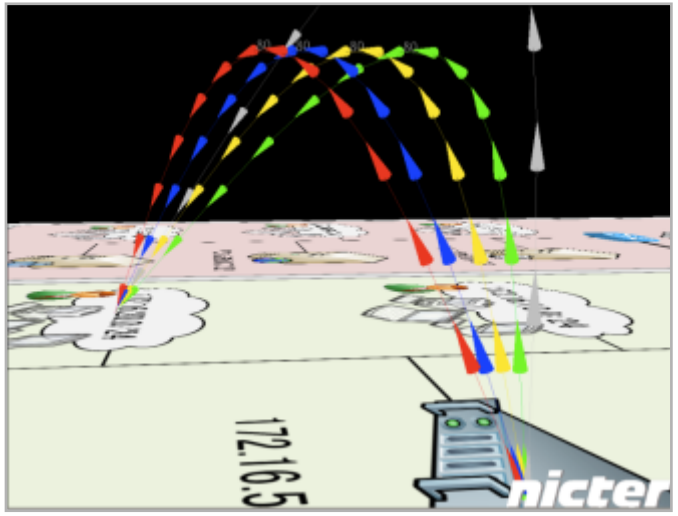
NIRVANA：システム構成

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

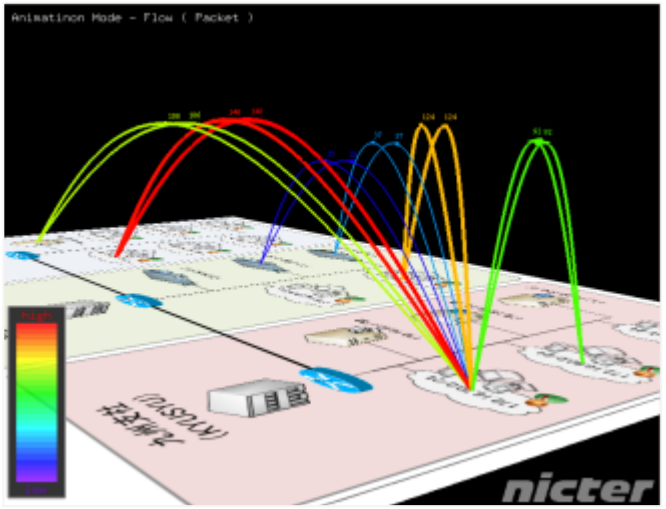


NIRVANA：トラフィック表示方法

- **パケットモード**
  - ✓ トラフィックをパケット単位で描画。
  - ✓ プロトコルやポート番号等に応じてパケット表示色を設定可能。
  - ✓ パケットをクリックし詳細情報表示。

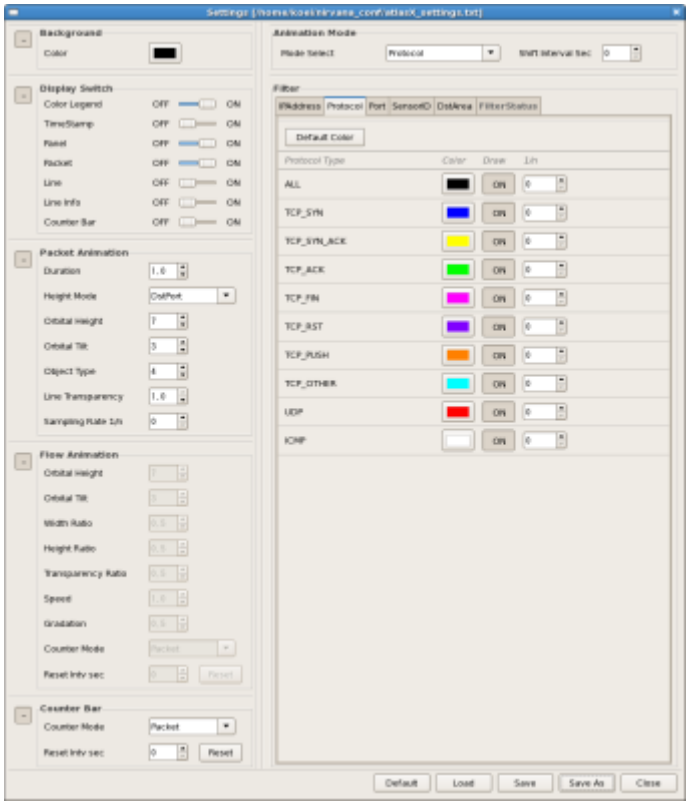


- **フローモード**
  - ✓ リボン状のフローの高低や色温度でトラフィック量を表現。
  - ✓ 大量のトラフィックを処理可能。



NIRVANA：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。

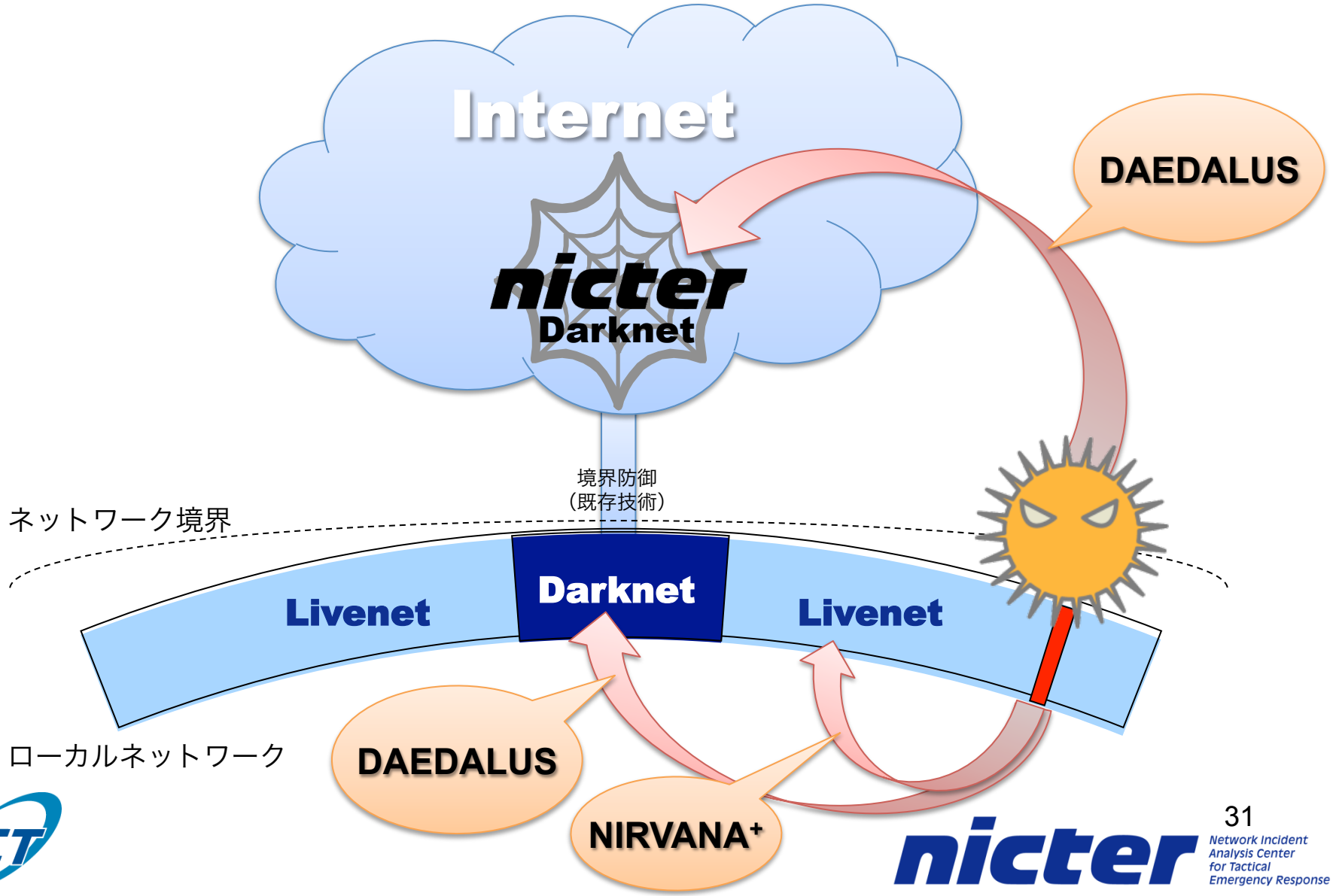


- **IPアドレス**
  - ✓ Src/Dst IPアドレスによる通信のフィルタリング。
- **プロトコル**
  - ✓ プロトコルの種類毎のフィルタリング。
- **ポート番号**
  - ✓ ポート番号毎のフィルタリング。
- **センサID**
  - ✓ センサID：センサに一意に割り当てられるID。
  - ✓ トラフィック取得地点毎のフィルタリング。
- **エリア**
  - ✓ エリア：Visioファイル内で定義する、各ネットワーク機器が属するグループ。
  - ✓ 営業拠点毎のエリア定義や建物のフロア毎のエリア定義などが可能。
  - ✓ 宛先エリア毎のフィルタリン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

サイバーセキュリティの新たな地平

nicter + DAEDALUS + NIRVANA+

nicter + DAEDALUS + NIRVANA+ による多層防御



NICT

nicter
Network Incident Analysis Center for Tactical Emergency Response

まとめ

- nicter：ダークネット観測によるグルーバルトレンド把握

+

- DAEDALUS：グローバルとローカルを繋ぐアラート機構

+

- NIRVANA+：ローカルの内側を守る新セキュリティ機構（開発中）

+

- ドライブ・バイ・ダウンロード対策技術（開発中）

+

- 境界防御（既存技術）

||

サイバーセキュリティの新たな地平