平成28年2月17日

情報通信研究機構における ネットワークセキュリティ研究の 最前線

国立研究開発法人 情報通信研究機構（NICT）
ネットワークセキュリティ研究所長

平　和昌

国立研究開発法人情報通信研究機構（NICT）

●役職員：理事長　坂内正夫
　　職員　1001名（非常勤職員を含む　平成27年10月1日現在）

●平成27年度予算：　２７３．９億円（運営費交付金）

●所在地：　本部　東京都小金井市
　　研究所　　神奈川県横須賀市、兵庫県神戸市、
　　京都府相楽郡精華町（けいはんな）
　　技術センター　茨城県鹿嶋市、石川県能美市　等

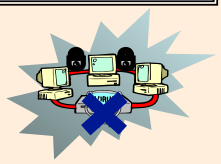
●主な業務：
- 情報通信分野の研究開発及び成果の普及
- 日本標準時の決定、標準電波の送信
- 電波の伝わり方の予報・警報
- 民間、大学等が行う情報通信分野の研究開発の支援　等

NICTが取り組む研究開発（第３期中長期計画：H23～H27）

ネットワーク基盤技術

情報量の増大、消費電力の低減等の要請に応える
安心・安全なネットワークを実現する

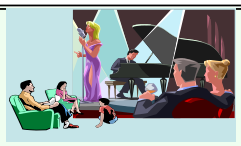




インターネットの次のNW（新世代NW）の研究開発
・光通信・ネットワーク技術、無線通信技術、情報セキュリティ技術

ユニバーサルコミュニケーション基盤技術

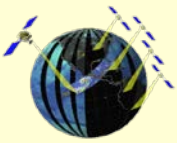
様々な壁を超えて人に優しい
コミュニケーションを実現する

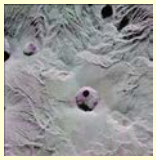


多言語間通訳技術、情報から知識に結びつける情報処理技術、立体映像等の臨場感あふれるコミュニケーション技術

電磁波センシング基盤技術

高精度な時刻情報や環境情報を
容易に安全に利用できるようにする

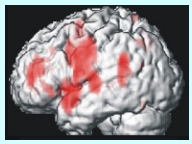
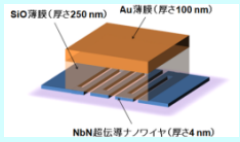




日本標準時・電波時計電波発射、レーダ等の地球センシング技術、宇宙天気技術、EMC電磁波影響評価技術

未来ICT基盤技術

未来の情報通信にパラダイムシフトをもたらす

脳情報融合技術、ナノ情報通信技術。量子通信技術、テラヘルツ帯利用技術

3

サイバー攻撃の現状

サイバー攻撃の変遷

- 20世紀：**愉快犯/自己顕示**
- 21世紀：**経済犯**
  示威活動（Hacktivism）
  諜報活動（Cyber Espionage）

Richard Skrenta
世界初のウイルス作成者（当時高校生）
(http://www.skrenta.com)

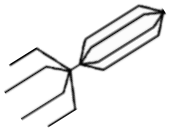
Anonymous
(Vincent Diamante - originally posted to Flickr as Anonymous at Scientology in Los Angeles)

- **ロンドン五輪で発生した事案※**
  - ✓ 23億5,000万件のセキュリティ・システム・メッセージ
  - ✓ 2億件の悪意のある接続要求
  - ✓ 構築時のウイルス検出　etc. etc…

※出典：“ LONDON 2012: CYBER SECURITY”
Oliver Hoare（英国 元GOEサイバーセキュリティ責任者）

サイバー攻撃の主役 『マルウェア』

- **Malware = Malicious(悪意のある)+ Software**
  - 情報漏えいやデータの破壊・改竄、他のコンピュータへの攻撃など、ユーザの望まない不正な活動を行うソフトウェアの総称



ウイルス

単体動作せず，自分自身を他のファイルやプログラムに寄生。

ワーム

単体で動作し自己増殖を行う。ウイルスに比べ高い感染力を有し，大規模感染を引き起こす。

ボット

指令者からの遠隔操作により多岐に渡る活動を行うマルウェア。
ボットネットと呼ばれるネットワークを形成し、それを活用して大規模に活動。

マルウェアの行動

- ✓ メールで送られてきて感染
- ✓ USBメモリ経由で感染
- ✓ インターネットからダウンロードしたファイルで感染
- ✓ OSやアプリの脆弱性を攻撃されて感染
- ✓ Webサイトを閲覧して感染

感染

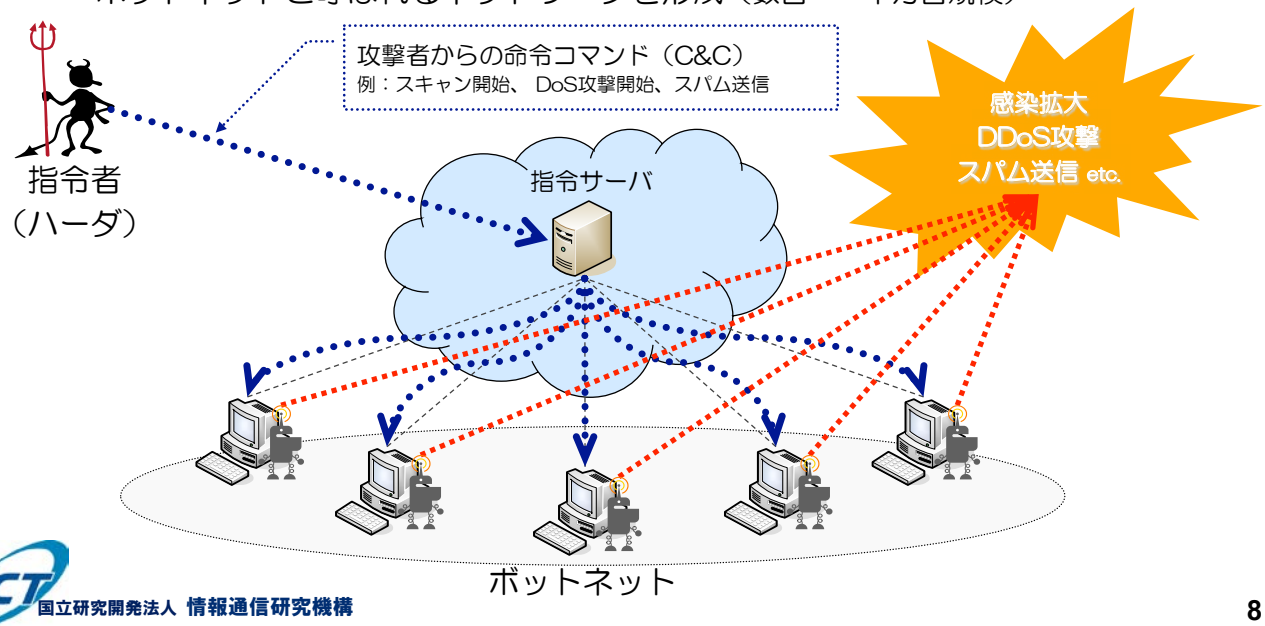
活動

- ✓ 他のPCへ感染を拡大する
- ✓ 内部のファイルを壊す・書き換える
- ✓ 内部の情報を外部へ送信する
- ✓ 内部のファイルを外部に送信する
- ✓ ネットワークで繋がっているPC内の情報を探すし、それらを外部へ送信する
- ✓ 外部のPCにアクションを仕掛ける

マルウェアの活動の具体例（1）

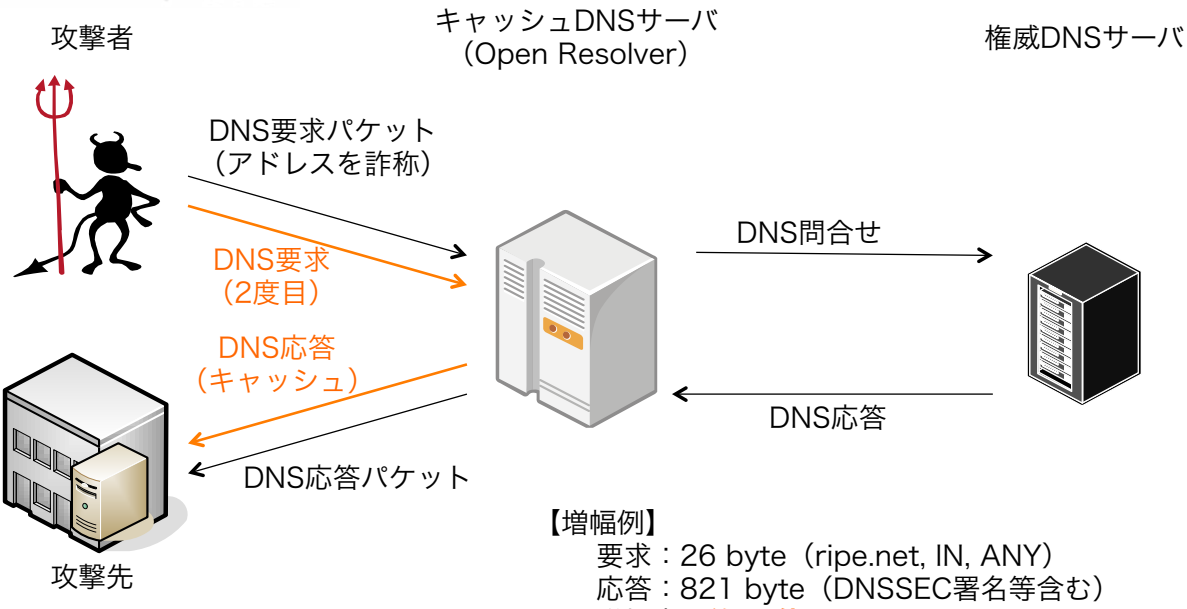
ボット

- ✓ 指令者からの遠隔操作により多岐に渡る活動を行うマルウェア
- ✓ ボットネットと呼ばれるネットワークを形成（数百～一千万台規模）



マルウェアの活動の具体例（2）

DNS amp攻撃

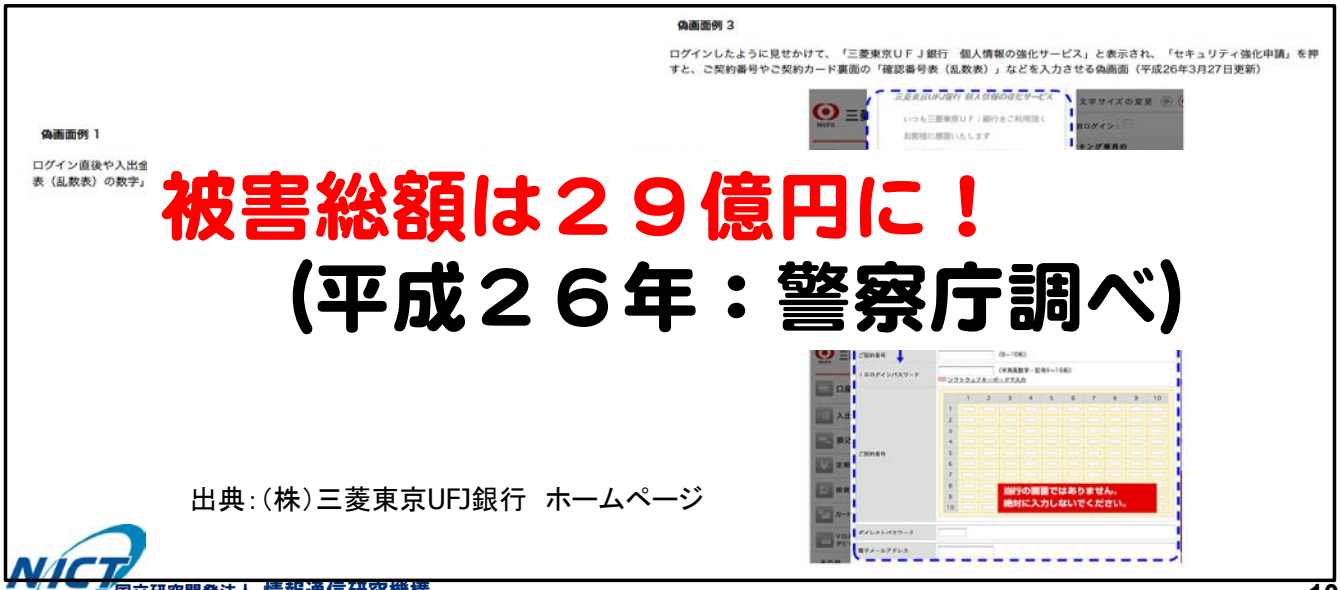


【増幅例】
要求：26 byte（ripe.net, IN, ANY）
応答：821 byte（DNSSEC署名等含む）
増幅率：**約32倍**

マルウェアの活動の具体例（3）

ネットバンキングにおける不正送金被害

- ✓ ユーザに画面が表示される前にマルウェアが通信内容を改竄
- ✓ ポップアップ画面などによりパスワードや乱数表を入力させる



インシデント分析センター

NICTER

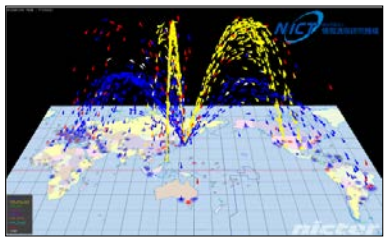
(Network Incident analysis Center
for Tactical Emergency Response)

インシデント分析センター NICTER

Network Incident analysis Center for Tactical Emergency Response

目的

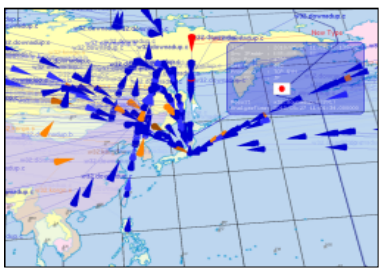
ネットワークにおけるセキュリティインシデントの迅速な状況把握、原因究明、対策を導出すること



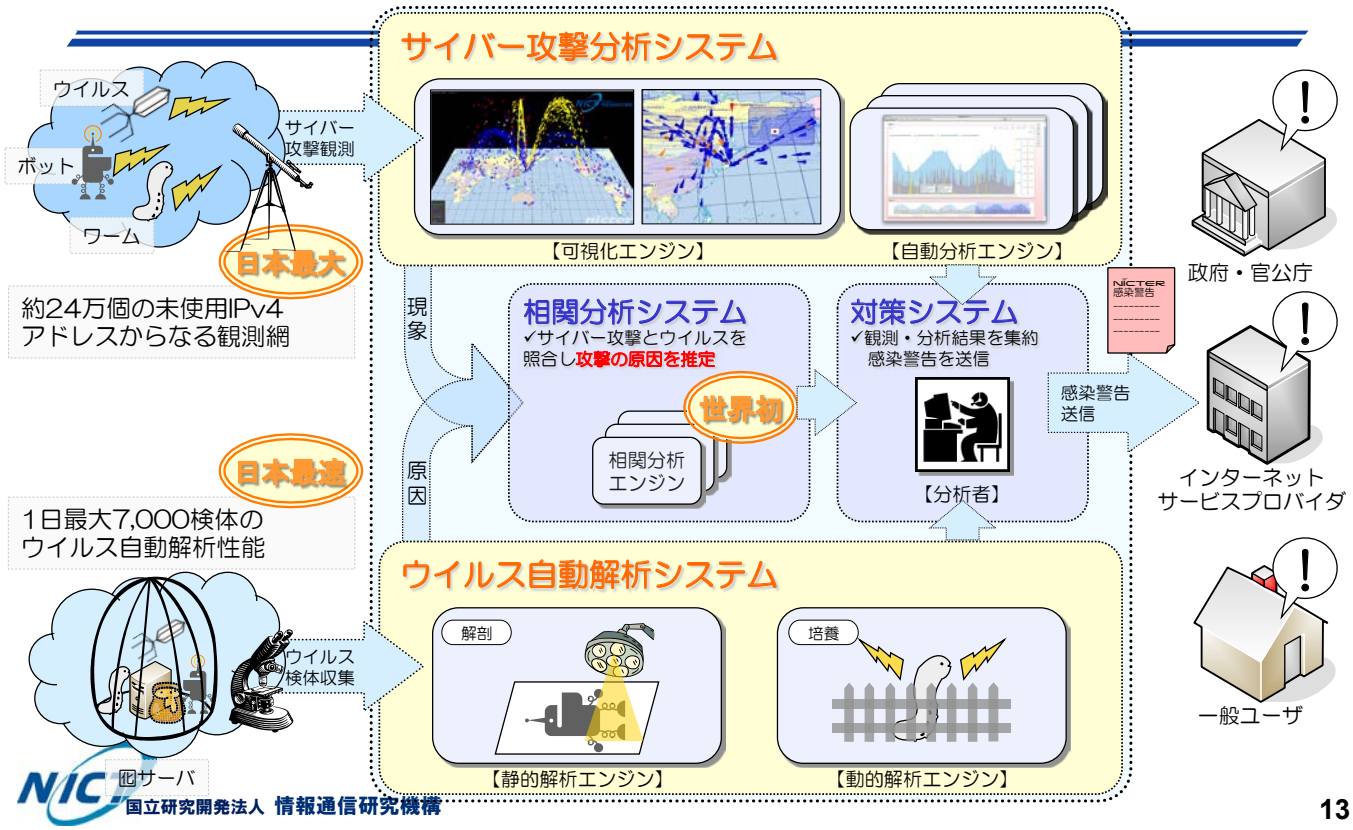
NICTERにより可能となること

- 世界のどの地域でマルウェア感染が広がっているのかの把握
- 個々の攻撃はどのマルウェアによって起きているのかの把握

⇒ サイバー攻撃のトレンドを迅速に把握して対策に役立てる



NICTERの全体像

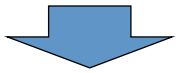


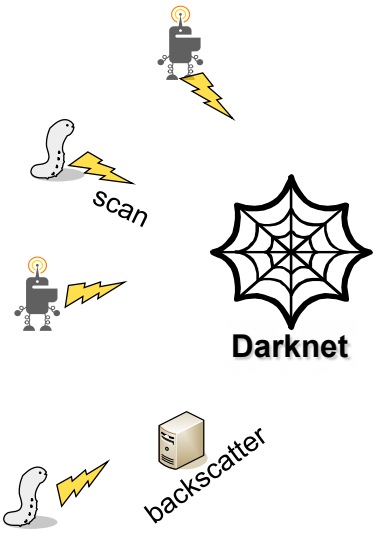
ダークネット（Darknet）

- コンピュータが接続されていない未使用のIPアドレス（ブロック）

- ダークネットに届くパケットは
  - マルウェアが感染対象を探す行為（スキャン）
  - マルウェア本体を含むパケットを送りつける行為
  - DDoS攻撃による影響（バックスキャッタ）
  - 設定ミス

  などが原因。



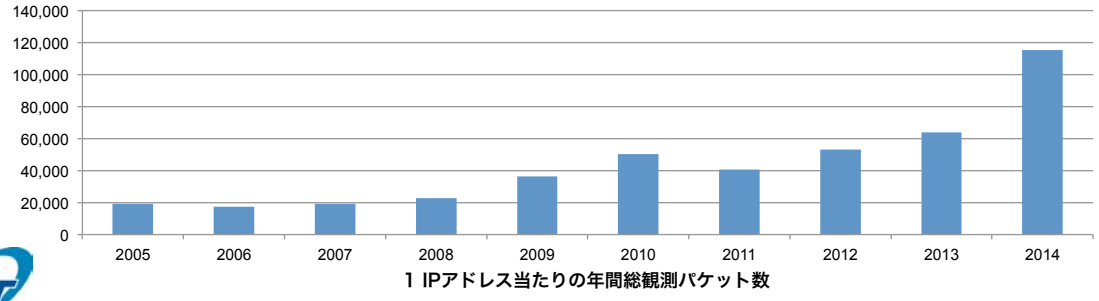


✓すべてのパケットを不正なものと見なして分析することができる

✓攻撃特性の把握やマルウェアの捕獲が可能

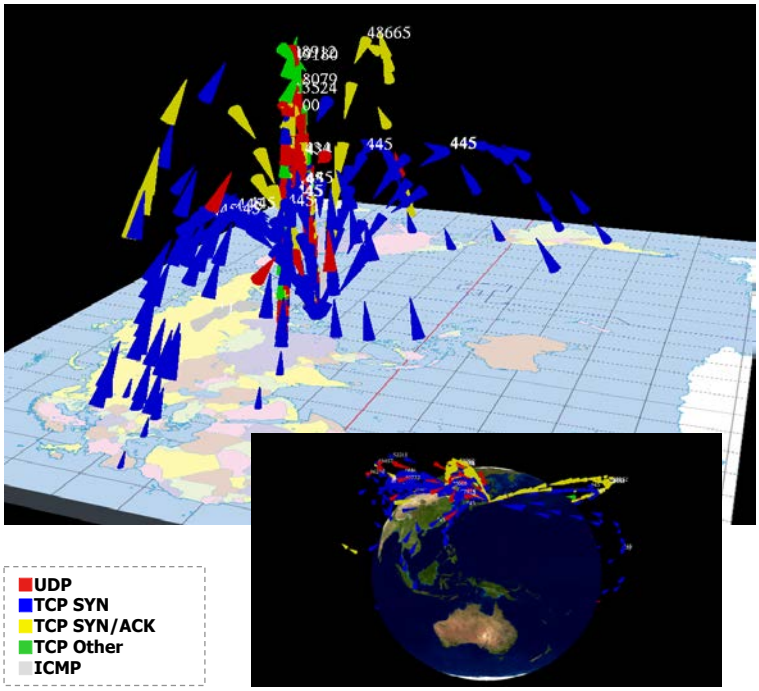
NICTERダークネット観測統計

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**

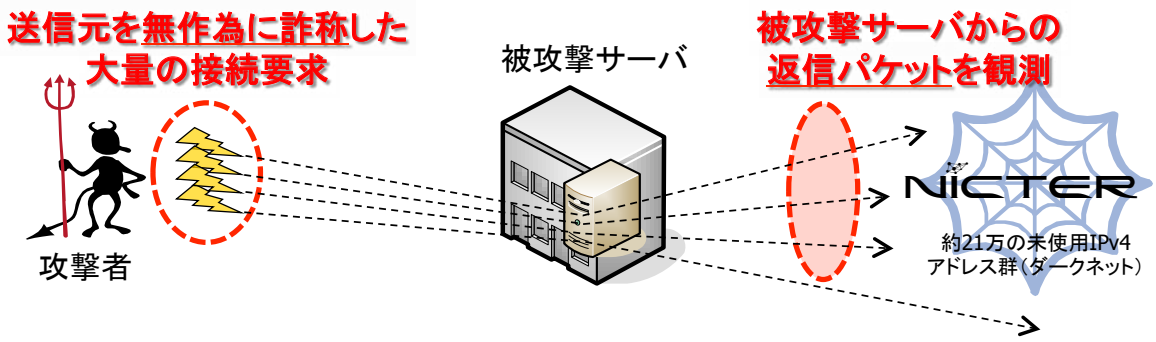


世界地図上での可視化エンジン「Atlas」

- ダークネットに飛来するパケットの発信元アドレスをもとに、世界地図上でリアルタイムに可視化
- 色：プロトコルやタイプを表現
- 高度：ポート番号に比例（対数軸）

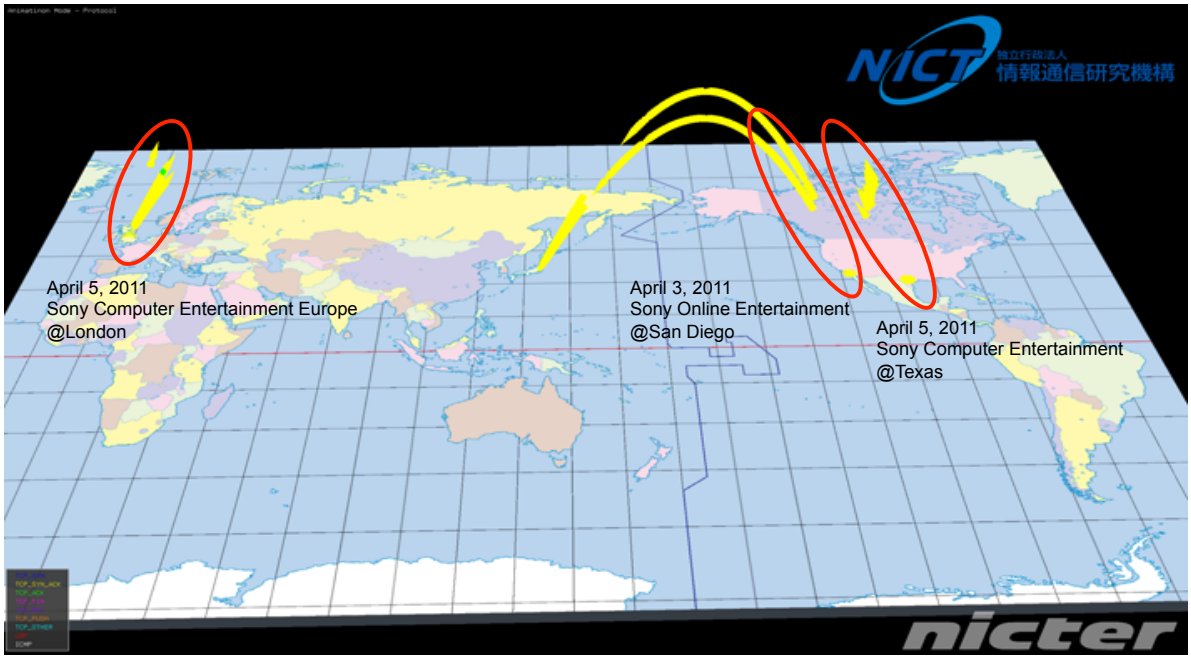


バックスキャッタ観測の仕組み

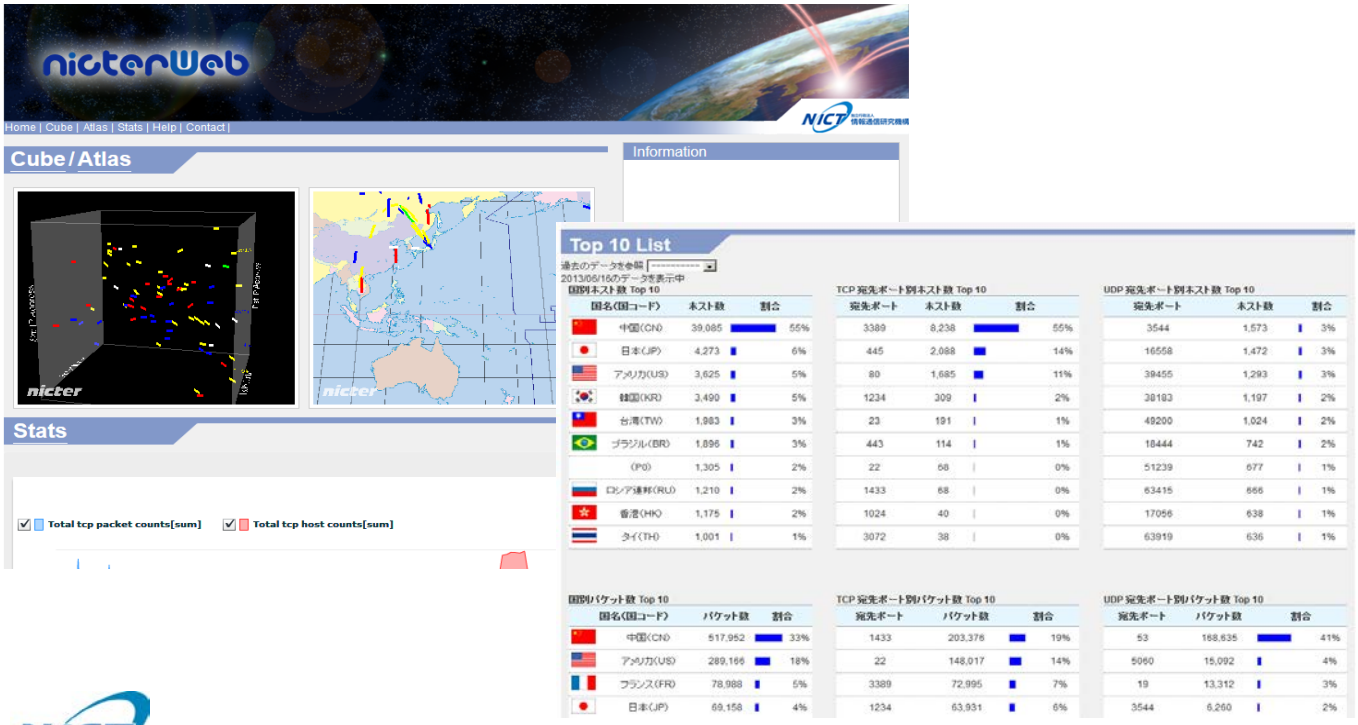


SONY DDoS攻撃時の観測状況

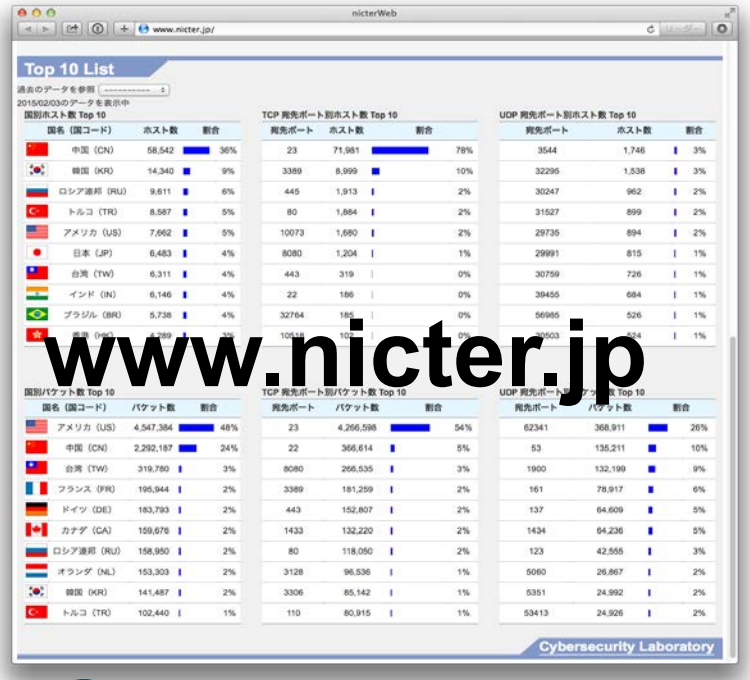
～ 被攻撃サイトから跳ね返りの通信（バックスキャッタ）を観測 ～



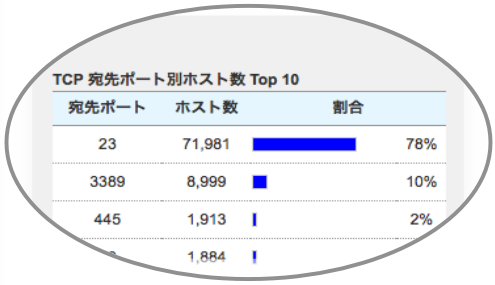
nicterWeb (www.nicter.jp)

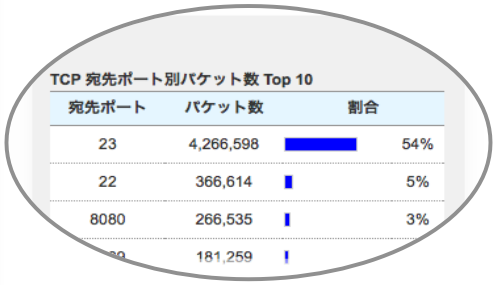


ダークネットトラフィック急増の原因



www.nicter.jp





対サイバー攻撃アラートシステム

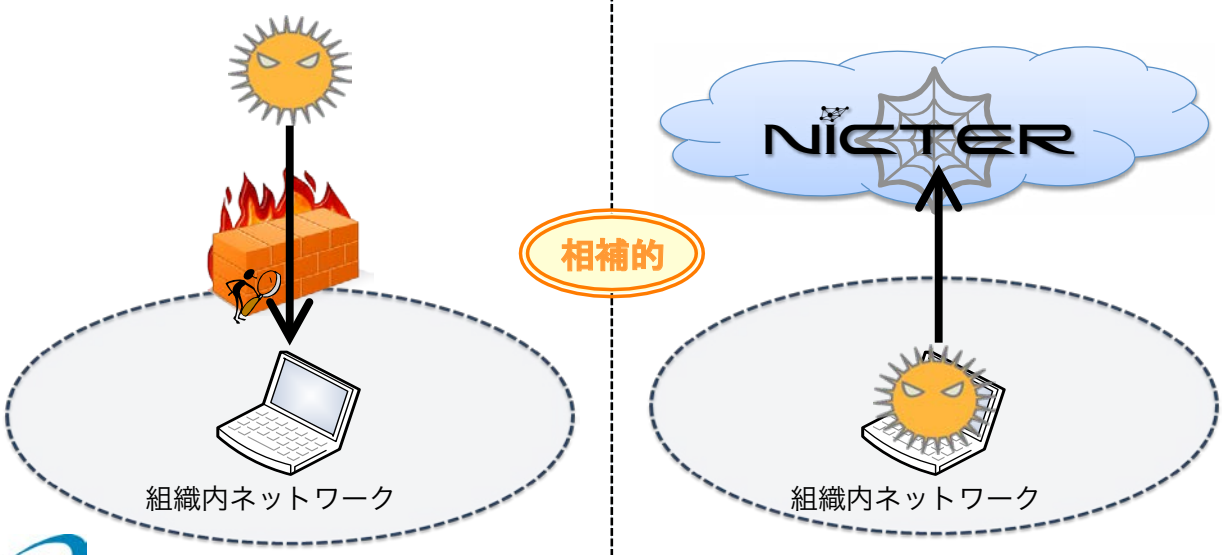
DAEDALUS

(**D**irect **A**lert **E**nvironment for
Darknet **A**nd **L**ivenet **U**nified **S**ecurity)

GOOD DESIGN AWARD 2013

境界防御技術とDAEDALUS

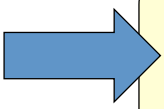
境界防御技術	DAEDALUS
組織外からの攻撃をネットワーク境界で検出	組織内からの攻撃をネットワーク広域で検出



DAEDALUS
対サイバー攻撃アラートシステム

Direct **A**lert **E**nvironment
for **D**arknet **A**nd **L**ivenet **U**nified **S**ecurity

- nicterの大規模ダークネット観測を応用し、サイバー攻撃に対してアラートを発するシステム
- 組織内のマルウェア感染や、組織外への攻撃、組織外からのDoS攻撃などを迅速に検知してアラートを送信

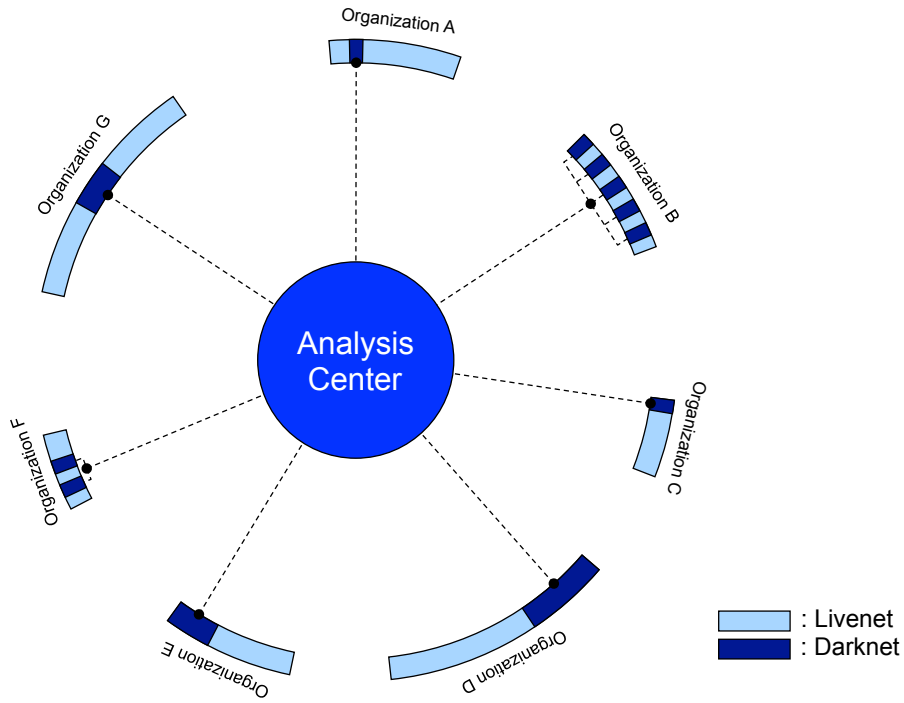


ダークネットを用いて
ライブネットの安全を強化する！

基本アイデア

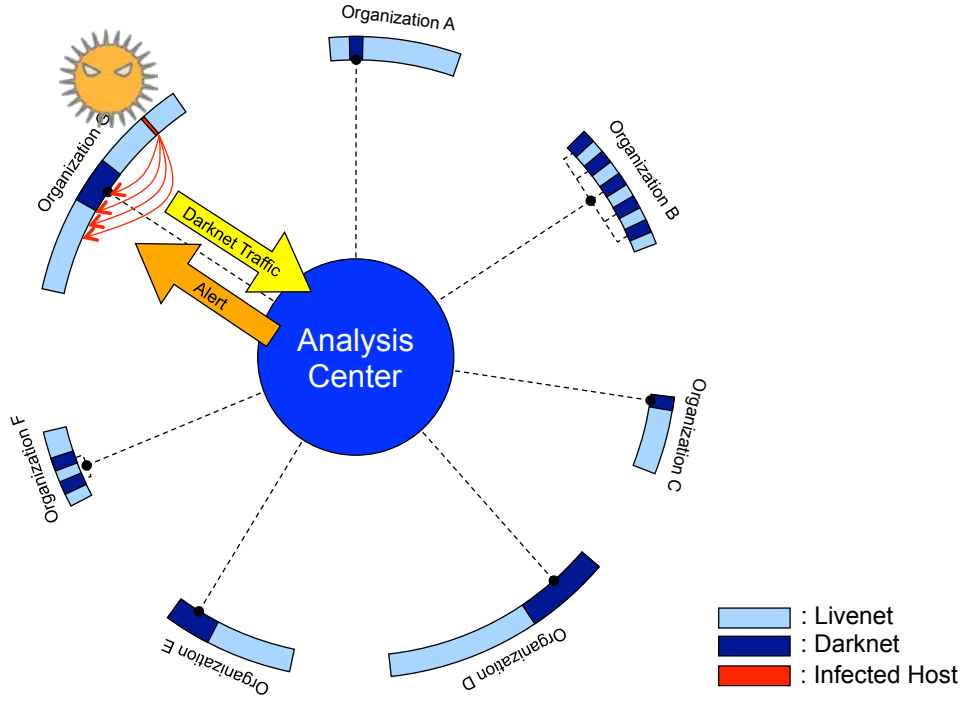
登録されたIPアドレスから
NICTERの
ダークネットセンサに
パケットが飛んできたら
アラート！

想定環境



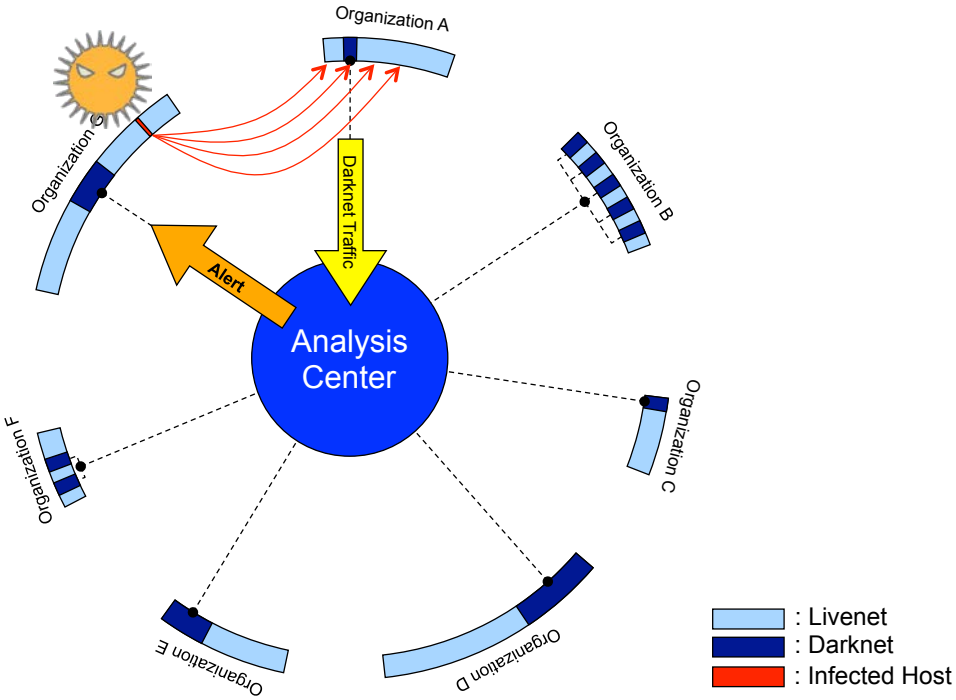
ケース1

内部ダークネットでの不正ホスト検出



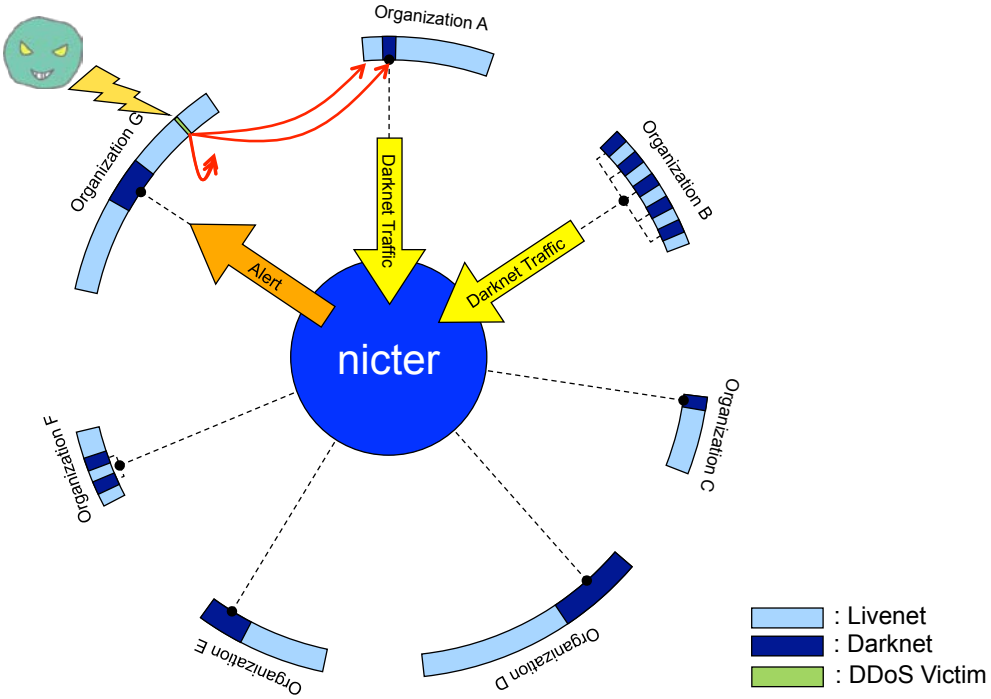
ケース2

外部ダークネットでの不正ホスト検出



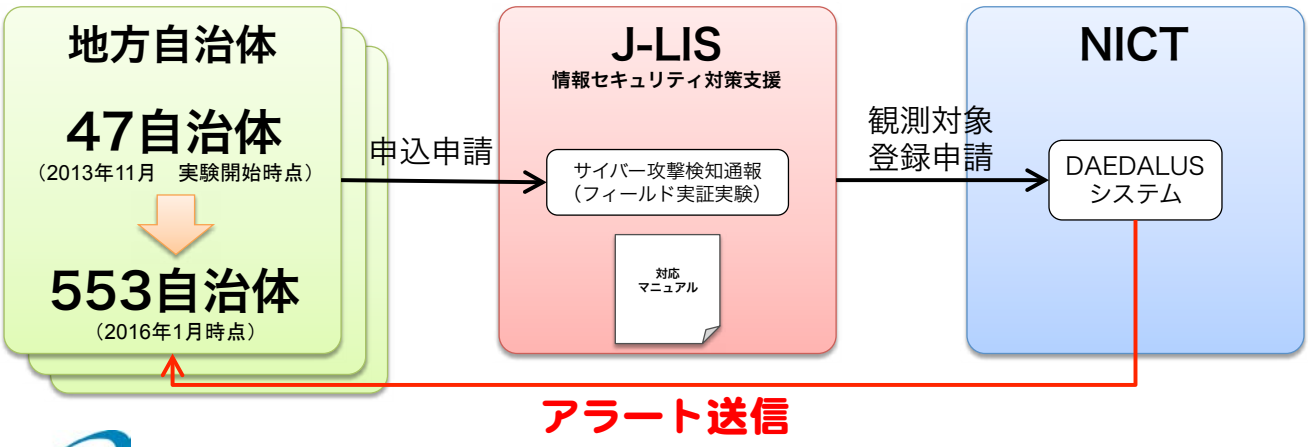
ケース3

DDoS攻撃の跳ね返り（バックスキャッタ）



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サイバー攻撃のアラート送信を開始（DAEDALUSの活用）**
  - 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



新たなタイプのサイバー攻撃「標的型攻撃」の脅威に対して

新たなサイバー攻撃の脅威に対して

➢ 標的型攻撃(APT)等の新たなサイバー攻撃の脅威が顕在化

Advanced --- 高度で
Persistent --- 執拗な
Threat: --- 脅威

- APTによる攻撃
  特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたり継続して行われるサイバー攻撃

➢ 新たなサイバー攻撃は、
- 大規模観測網では発見できない
- 侵入の痕跡自体が削除される

など、発見・解析が極めて困難

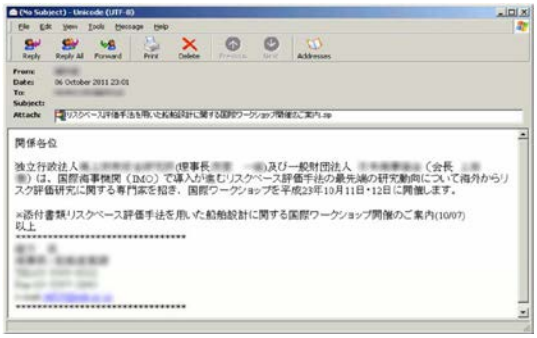
→ 革新的な対策手法の研究開発が必要

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

諜報 → 侵攻 → 潜伏 → 橋頭堡確保 → 索敵 → 浸透 → 占領 → 収奪 → 撤収



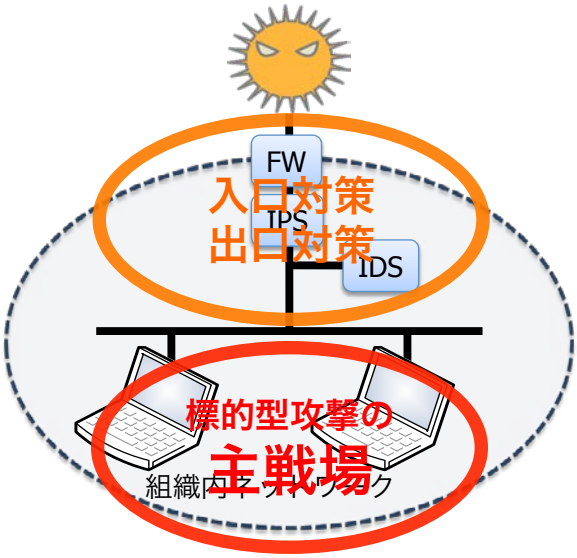
TECH.ASCII.jp「9.5社に1社が対象に！シマンテックが明かす日本の標的型攻撃」
http://ascii.jp/elem/000/000/652/652712/ （2011-11-30）

入口対策/出口対策

入口 → 諜報 → 侵攻 → 潜伏 → 橋頭堡確保 → 索敵 → 浸透 → 占領 → 出口 → 収奪 → 撤収

入口対策/出口対策 = 境界防御

- **FW**（ファイアウォール）
  - ✓ 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**（侵入検知システム）
  - ✓ 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**（侵入防止システム）
  - ✓ シグネチャで攻撃を<u>防止（遮断）</u>
  - ✓ インライン

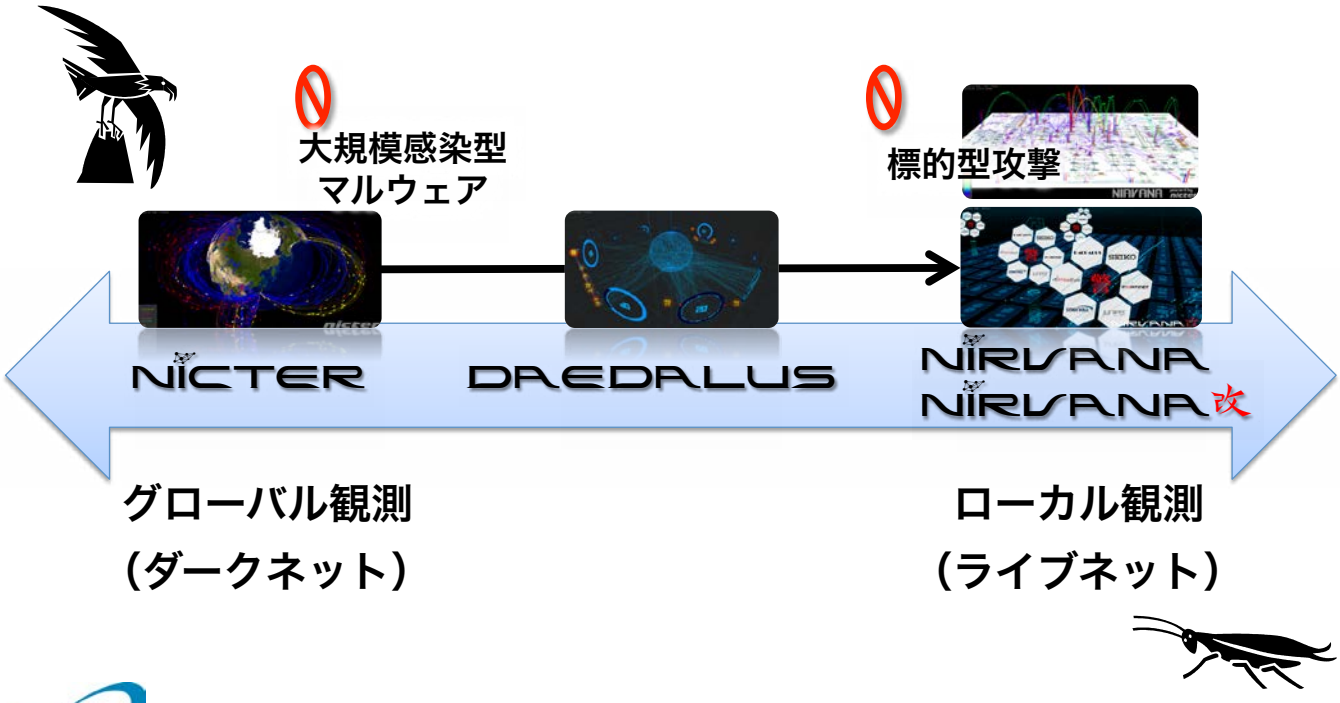


- サイバー攻撃統合分析プラットフォーム
  - – NIRVANA にセキュリティ機能を追加
  - – ライブネットトラフィック＋アラートの可視化
    → 統合的ネットワークオペレーションツールへ

なぜ止められない？標的型攻撃

- 単一のセキュリティ機器だけでは検出困難
  - 改 → 複数機器を連携させる統合分析プラットフォーム
- ネットワーク内部での攻撃に境界防御は無力
  - 改 → 組織の末端までセンサ設置しリアルタイム分析
- ネットワーク系とエンドホスト系対策の断絶
  - 改 → ネットワークからエンドホストへシームレスに没入
- 防御策実施までのタイムラグ
  - 改 → 相関分析結果に基づく防御策の自動展開

鳥の目/虫の目



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！