講演2

平成27年3月11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

独立行政法人 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

独立行政法人情報通信研究機構（NICT）

●役職員：理事長　坂内正夫　（前 国立情報学研究所長）
職員　９３７名（非常勤職員を含む　平成２６年４月１日現在）

●平成２６年度予算：　一般会計　２８０．７億円（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

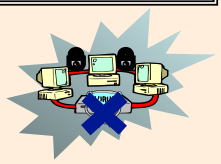
●主な業務：
・情報通信分野の研究開発及び成果の普及
・日本標準時の決定、標準電波の送信
・電波の伝わり方の予報・警報
・民間、大学等が行う情報通信分野の研究開発の支援　等

NICTが取り組む研究開発（第3期中期計画）

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

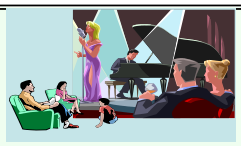




インターネットの次のNW（新世代NW）の研究開発
・光通信・ネットワーク技術、無線通信技術、情報セキュリティ技術

ユニバーサルコミュニケーション基盤技術

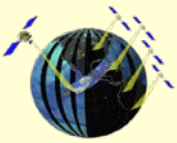
様々な壁を超えて人に優しい
コミュニケーションを実現する

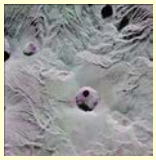


多言語間通訳技術、情報から知識に結びつける情報処理技術、立体映像等の臨場感あふれるコミュニケーション技術

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

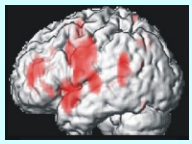
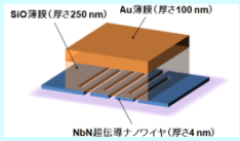




日本標準時・電波時計電波発射、レーダ等の地球センシング技術、宇宙天気技術、EMC電磁波影響評価技術

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

サイバー攻撃の変遷

- **20世紀：愉快犯/自己顕示**

Richard Skrenta
世界初のウイルスElk Clonerの
作者（当時高校生）

- **21世紀：経済犯**

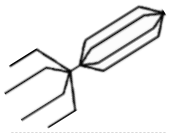
＋

示威活動（Hacktivism）
諜報活動（Cyber Espionage）

Anonymous

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

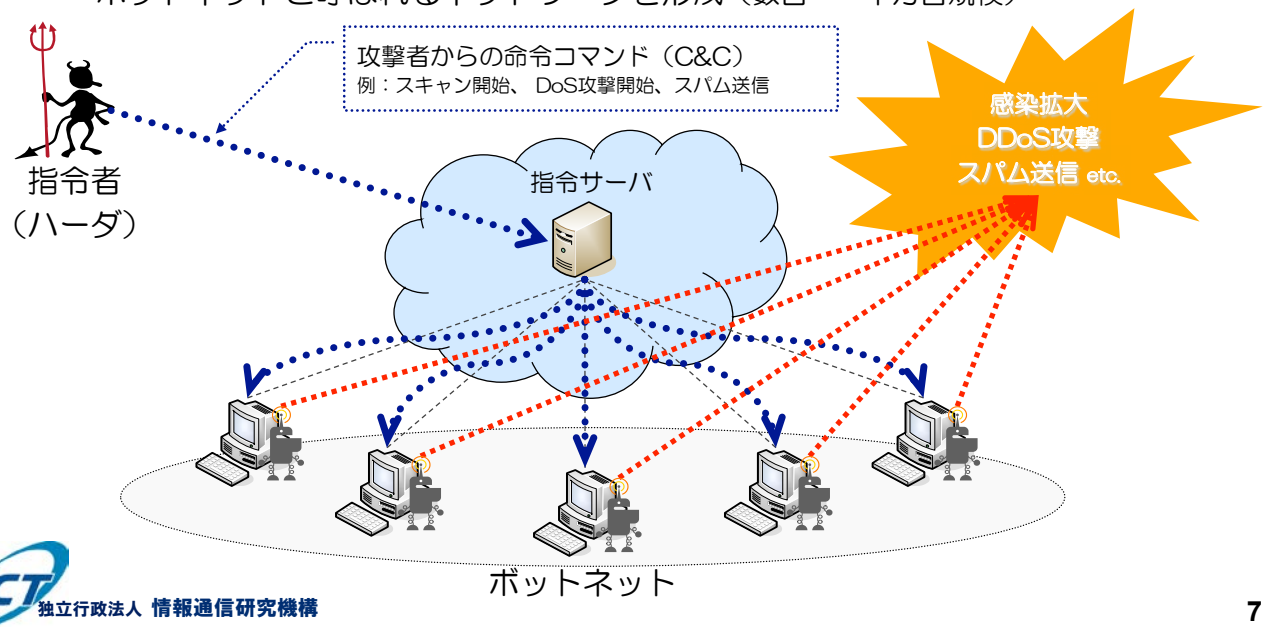
- ✓ 他のPCへ感染を拡大する

- ✓ 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）

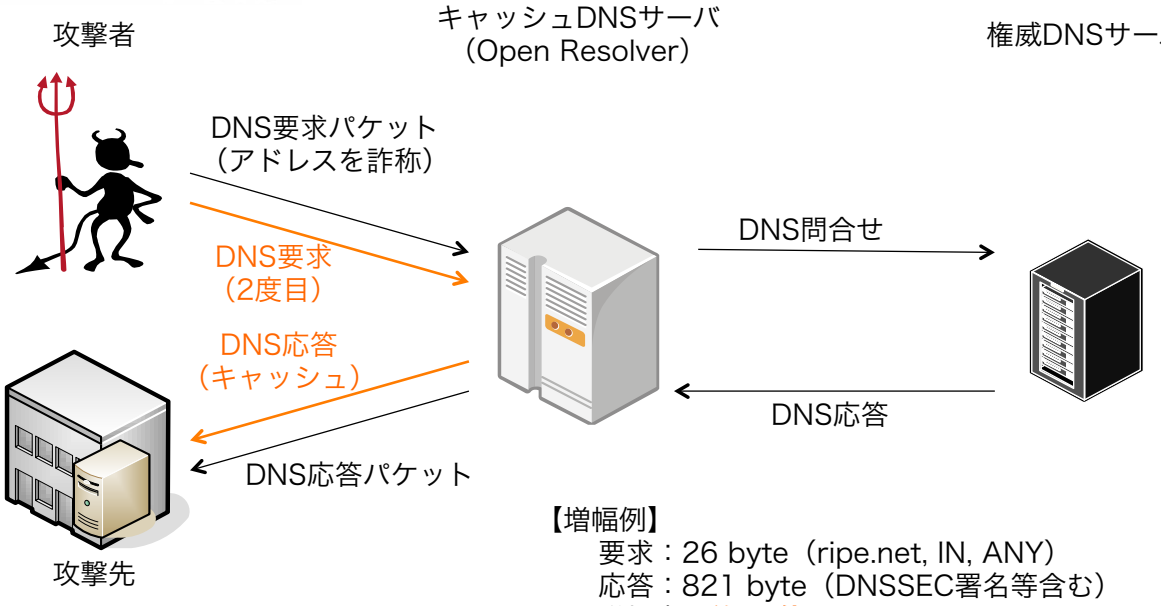
ボット

- ✓ 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）

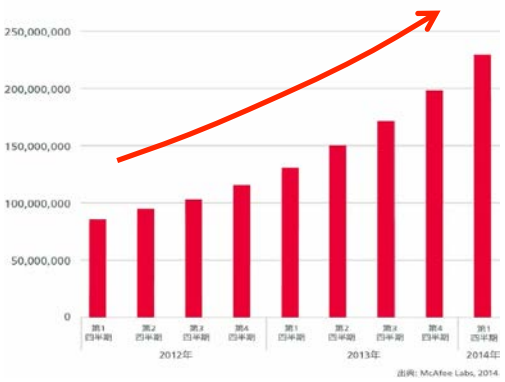
DNS amp攻撃



【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**

セキュリティ脅威の増大

マルウェアの総数



マカフィーにおいて、１四半期で3,000万超の新種マルウェアを確認しており、これまでデータベース上登録されたマルウェア数は２億件を突破

政府機関・重要インフラへの脅威件数等

24時間365日
（１分に１０回）

	2010年度	2011年度	2012年度	2013年度
センサー監視等による脅威件数※	約48万	約66万	約108万	約508万
センサー監視等による通報件数	１８１	１３９	１７５	139
不審メールに関する注意喚起の件数	118	209	415	381

	2013年度（括弧内は昨年度の数字）	主な内訳
重要インフラ分野からの情報連絡件数	153（110）	不正アクセス、DoS攻撃 １２１ ウイルスへの感染 7 その他の意図的要因 5

※ GSOC（政府機関・情報セキュリティ横断監視・即応調整チーム）により各府省等に置かれたセンサーが検知等したイベントのうち、正常なアクセス・通信とは認められなかった件数

インシデント分析センター

NICTER

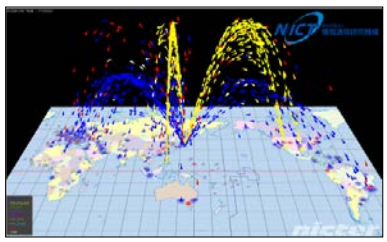
(Network Incident analysis Center
for Tactical Emergency Response)

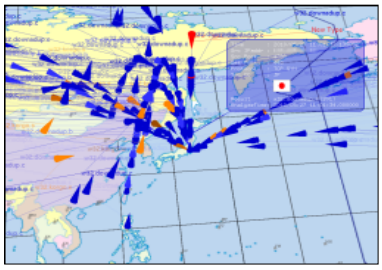
インシデント分析センター NICTER

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

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



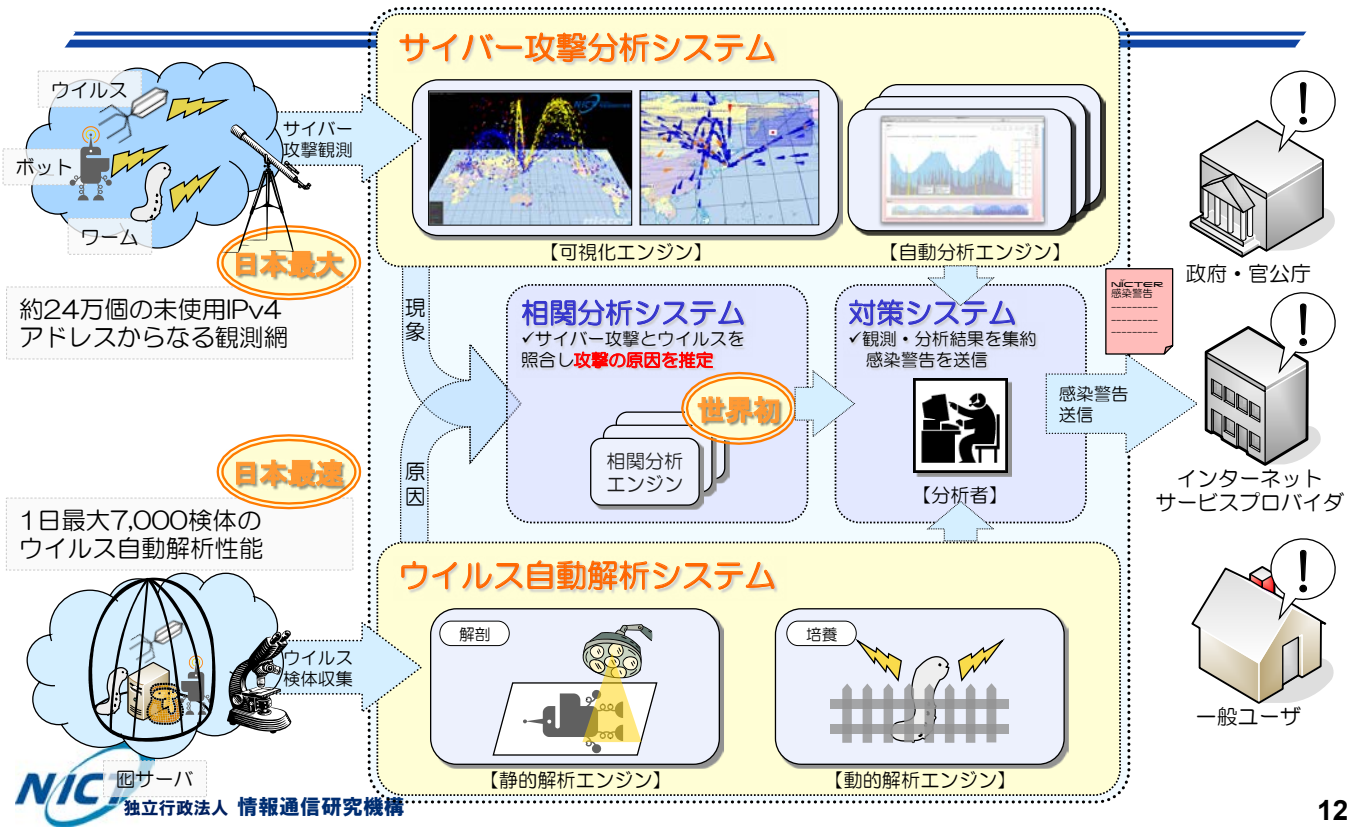


NICTERにより可能となること

- 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

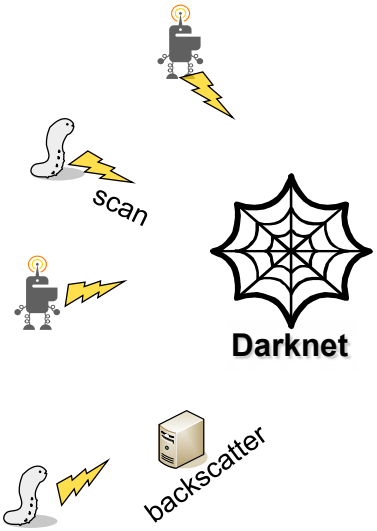


ダークネット（Darknet）

- 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

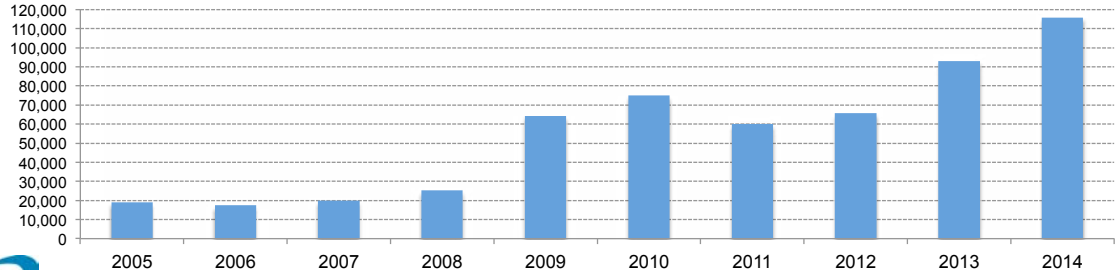
  などが原因。



✓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

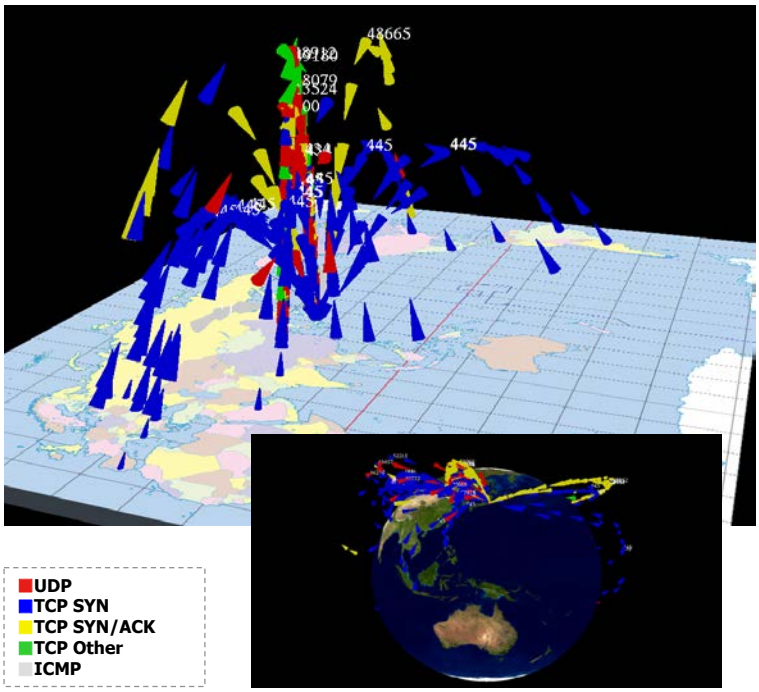
年	年間 総観測パケット数	観測IPアドレス数	1IPアドレス当たりの 年間総観測パケット数
2005	約　3.1億	約1.6万	約19,066
2006	約　8.1億	約10万	約17,404
2007	約　19.9億	約10万	約19,855
2008	約　22.9億	約12万	約25,242
2009	約　35.7億	約12万	約64,304
2010	約　56.5億	約12万	約74,952
2011	約　45.4億	約12万	約59,987
2012	約　77.9億	約19万	約65,614
2013	約128.8億	約21万	約92,835
2014	約241.8億	約24万	約115,782



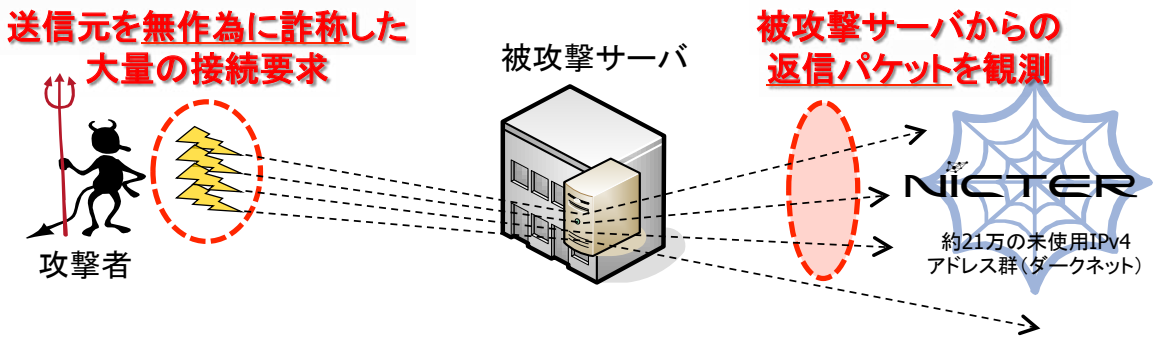
1IPアドレス当たりの年間総観測パケット数

世界地図上での可視化エンジン「Atlas」

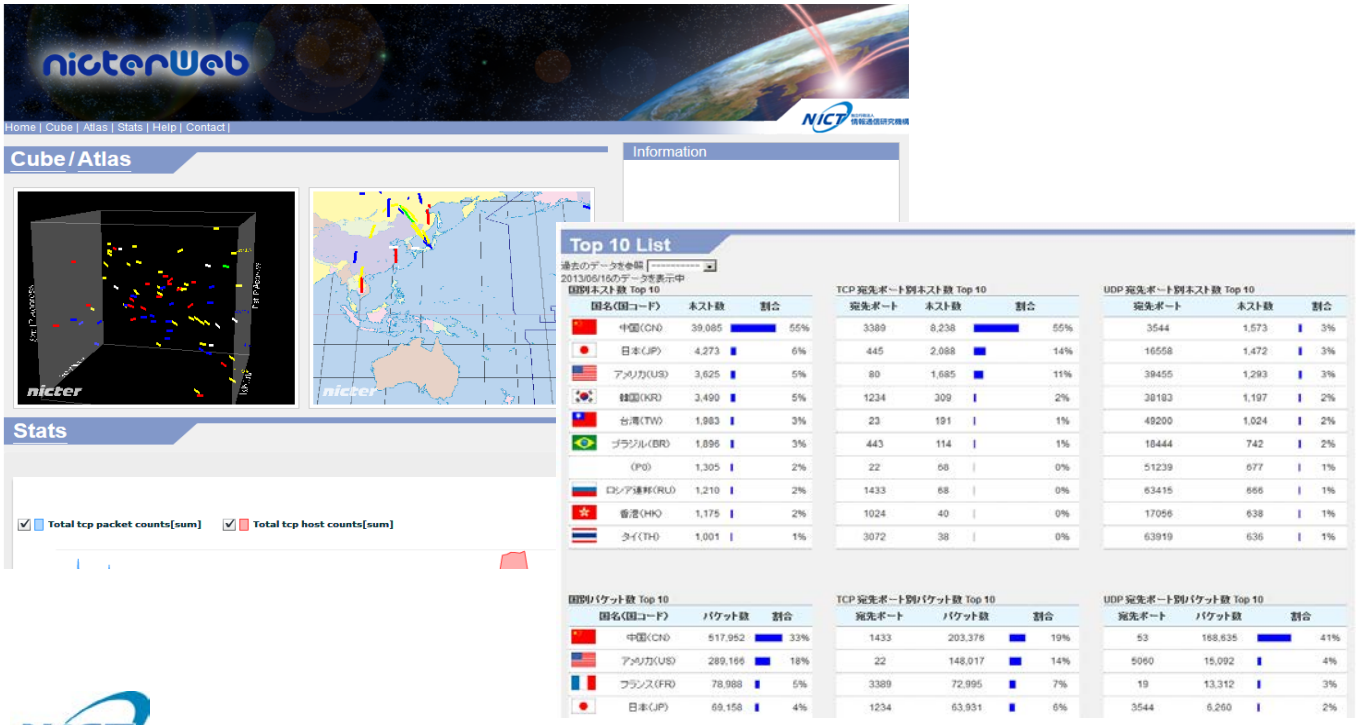
- ダークネットに飛来するパケットの発信元アドレスをもとに、世界地図上でリアルタイムに可視化
- 色：プロトコルやタイプを表現
- 高度：ポート番号に比例（対数軸）



バックスキャッタ観測の仕組み



nicterWeb (www.nicter.jp)



対サイバー攻撃アラートシステム

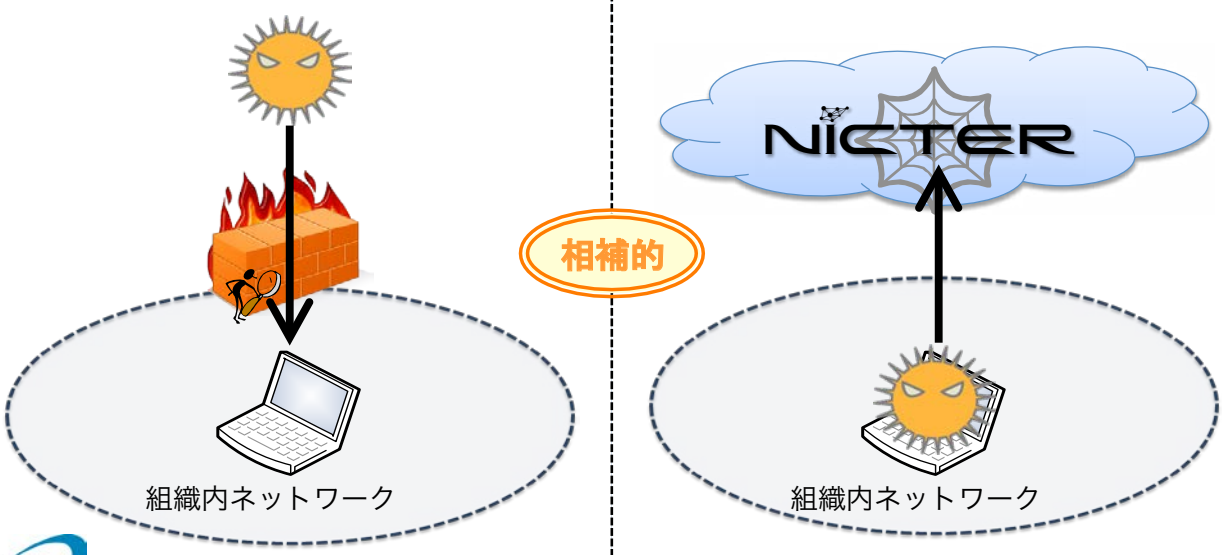
DAEDALUS

(**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

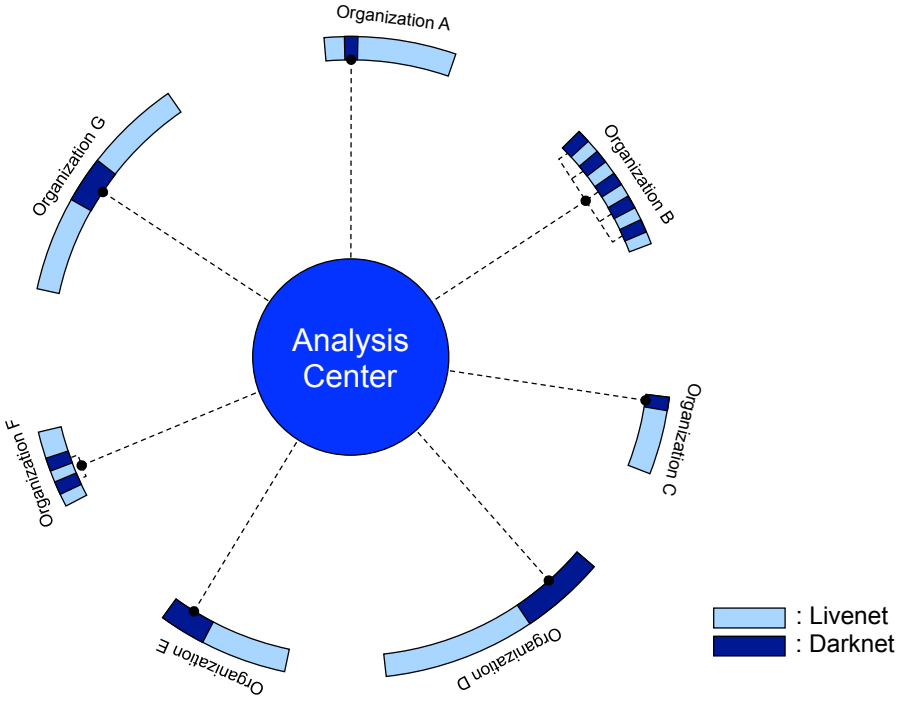
NICTERの

ダークネットセンサに

パケットが飛んできたら

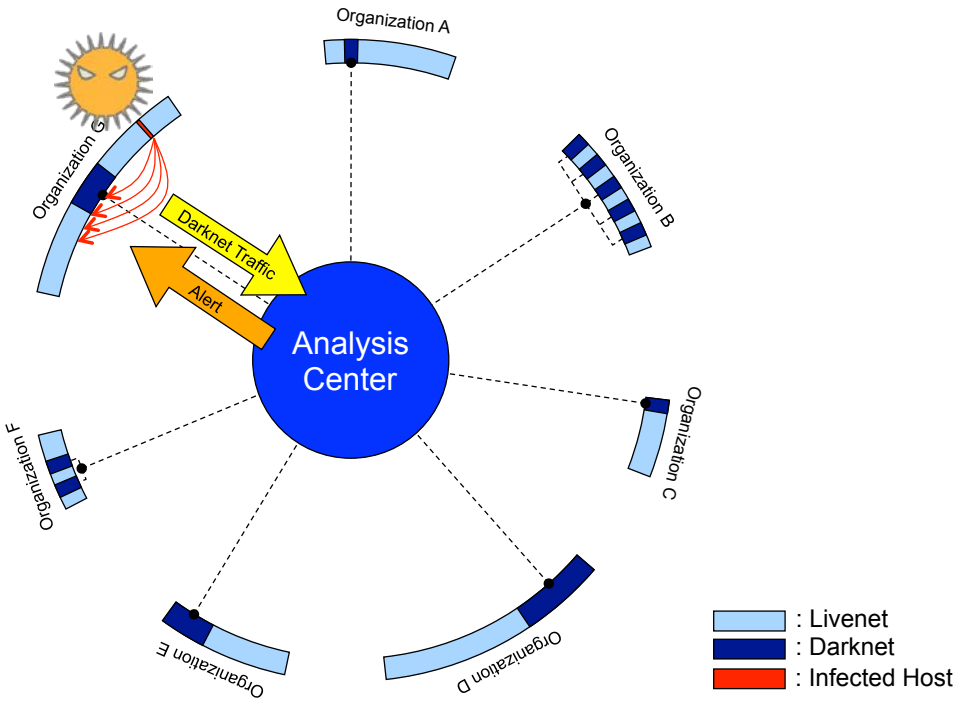
アラート！

想定環境



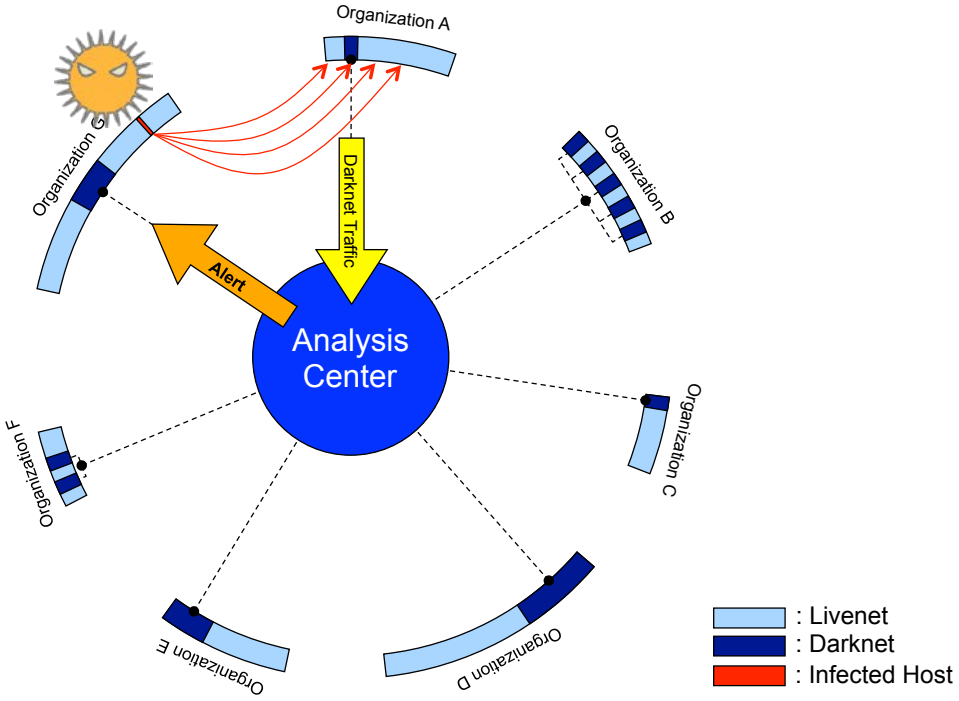
ケース1

内部ダークネットでの不正ホスト検出



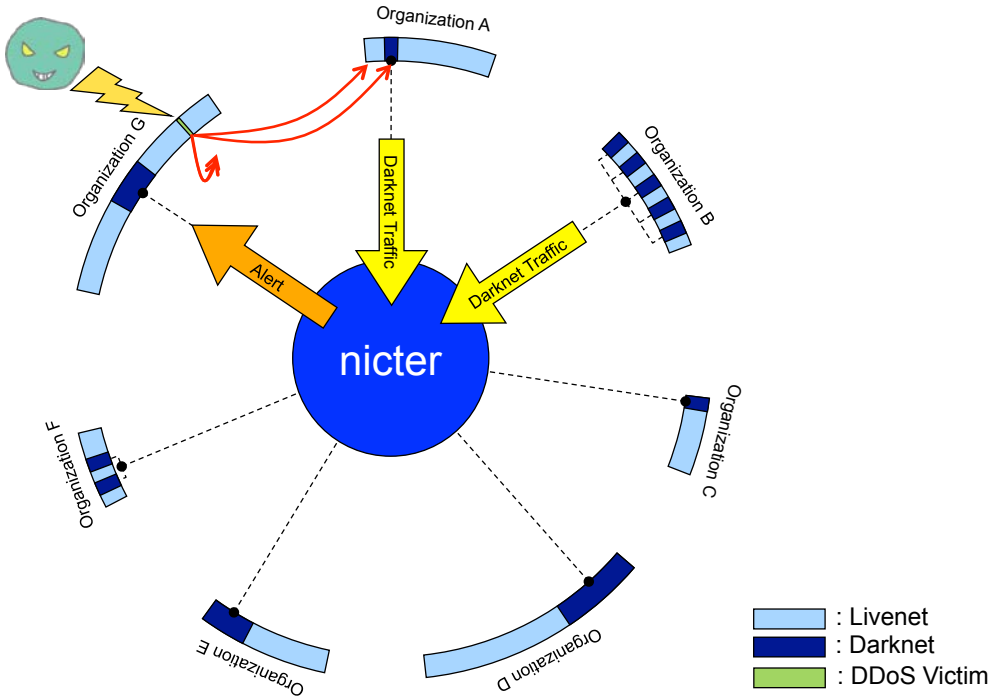
ケース2

外部ダークネットでの不正ホスト検出



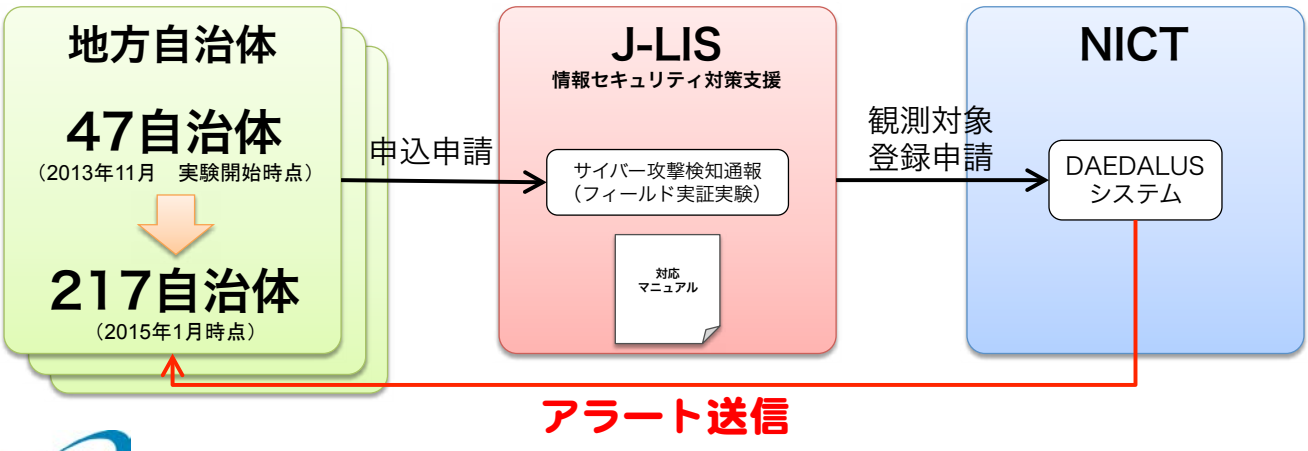
ケース3

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の送信

- **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

新たなタイプのサイバー攻撃

日本を襲った新たなタイプのサイバー攻撃（標的型攻撃）

- ✓ 2011年　9月：三菱重工
- ✓ 2011年10月：外務省在外公館
- ✓ 2011年10月：衆議院
- ✓ 2011年11月：参議院　　etc. etc...

しかし・・・

- ● 特定の組織を狙った攻撃であることから、被害を被った組織の多くは、被害状況や攻撃手法を外部に公開しない。
- ● そのため、標的型攻撃に対する実践的な解析手法や具体的な対策法の検討が実施できない。
- ● したがって、標的型攻撃に対する対策ツールなどが各組織において整備できない状態。

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

APTによる攻撃の特徴的な行動

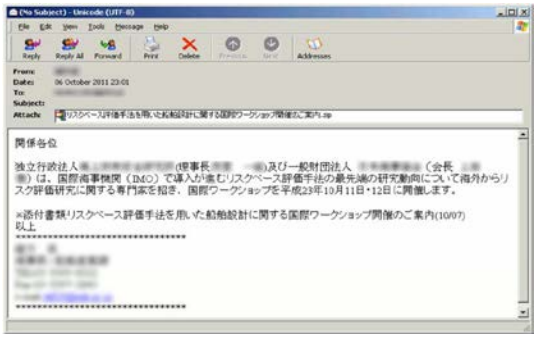
- **ローカルPCの特権の獲得**
  - ✓ 標的型メールによるマルウェア感染
  - ✓ リモート制御ツールのインストール
- **組織のネットワークを俯瞰できるホストの乗っ取り**
  - ✓ ネットワーク管理者のPC
  - ✓ ネットワーク監視系サーバ　など
- **目的とするサーバの乗っ取り**
  - ✓ ドメインコントローラ
  - ✓ ファイルサーバ　など
- **執拗な攻撃**
  - ✓ 少なくとも3カ月以上にわたる攻撃

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（境界防御）　出口（境界防御）

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

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

今後に向けて

誰もが安心・安全にコミュニケーションできる社会を実現するために、理論と実践の両側面からネットワークセキュリティ技術の研究開発を推進し、NICTの中立性を最大限に活用することにより、世界的な研究開発拠点となることを目指します。

ご清聴ありがとうございました