サイバー攻撃と最近の対策
―安心・安全なサイバー空間の利活用に向けて―

中尾 康二
独立行政法人情報通信研究機構（NICT）
KDDI株式会社 情報セキュリティフェロー

本日のトピック

最近のセキュリティ脅威（攻撃）の紹介

1）これまでの脅威（ボットネット中心）

2）不正ホップアップマルウェア

3）APTによる攻撃

4）最近のDNSアンプ攻撃、ZeroAccessボット

脅威に対抗するための対策の動向

5）ボットネット対策（日本、韓国、台湾、ドイツ）

6）APTによる攻撃の対策

7）NICTにおける研究活動（対策への活用）

まとめ

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**

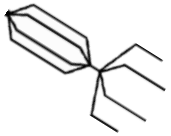
＋

Anonymous

- **2010年代：示威活動（Hacktivism）**
  諜報活動（Cyber Espionage）

マルウェアの感染形態に着目した分類

- **ウイルス（狭義のウイルス）**
  - ✓ 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
  - ✓ ブートセクタ感染型：ハードディスクなどのシステム領域に感染
  - ✓ ファイル感染型：実行可能ファイルを主な感染対象

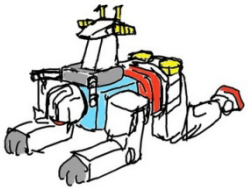


ウイルス

- **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
  - ✓ 電子メールやリムーバブルメディア（USBメモリ等）を媒体とするもの
  - ✓ Windowsのファイル共有やメッセージング機能を利用するもの
  - ✓ OSやアプリケーションの脆弱性に対する攻撃コードを用いるもの

ワーム

- **トロイの木馬**
  - ✓ 有用なプログラムやファイルに偽装
  - ✓ ユーザ自身によるシステムへのインストールや起動を誘う
  - ✓ 感染機能を持たないものが多い

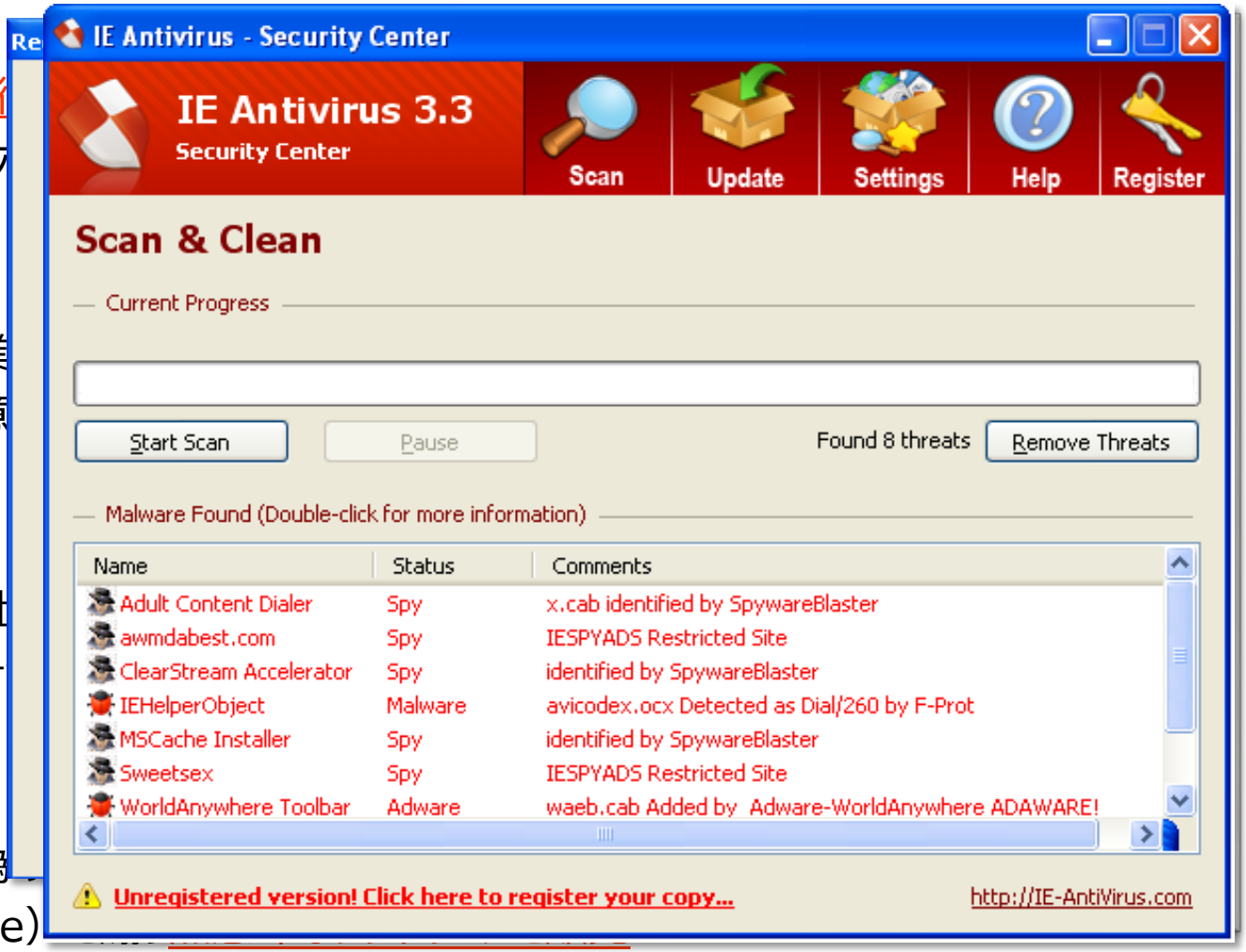


トロイの木馬

出典：GIZMODE Japan

マルウェアの目的に着目した分類

- **スパイウェア**
  - ✓ 個人情報や
  - ✓ ユーザのキー
- **アドウェア**
  - ✓ ユーザに企業
  - ✓ ユーザの同意
- **ランサムウェア**
  - ✓ ユーザのPC上
  - ✓ データの復号
- **スケアウェア**
  - ✓ ユーザに虚偽
  - ✓ 不安（scare）



1）これまでの脅威（ボットネット中心）：マルウェアの変遷

危険度

メールから感染
から感染

ネットワークから感染

ウェブサイトなど

営利犯
金儲けの道具

愉快犯
自己顕示欲

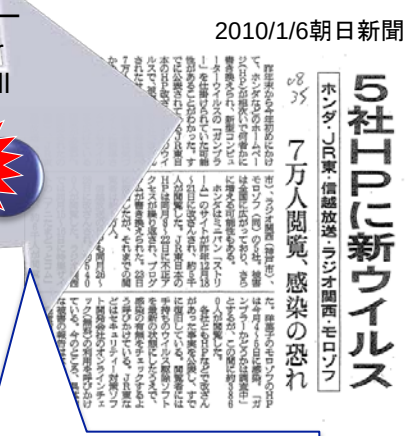
トロイの木馬
TROJ_AGENT.EH

ワーム
MS-Blaster
Slammer

ボット（BOT）
ロボットの略から命名
Agobot
ForBot

ガンブラー
Gumblar
Nine-Ball

2010/1/6朝日新聞



大量通信でネットワーク混乱（03年1月韓国ではネットが数時間利用不可）

感染したPCは遠隔操作される（迷惑メール、攻撃の踏み台など）

ウェブからPCにマルウェアを送り込まれる（：情報の抜き取り等）

W32/CIH(チェルノブイリ)、
Happy99

★目立つ→駆除しやすい

★目立たない→駆除されにくい

感染ユーザは「少し調子がおかしいかな？」程度で、特段の不具合を感じない

2000年　2005年　2010年

高機能

【関係機関の取り組み】

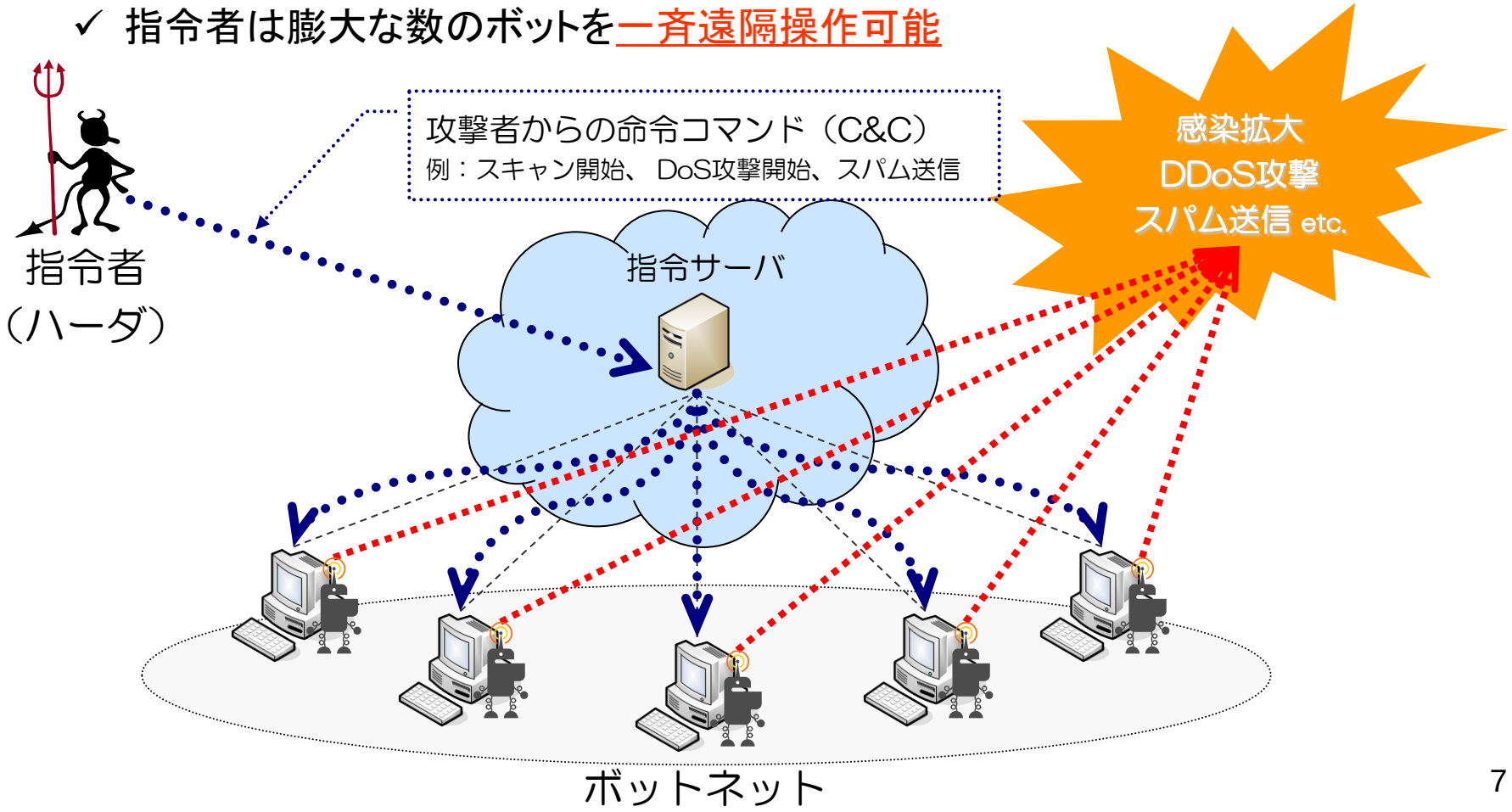
総務省関連　→　インターネット接続事業者（ISP）によるセキュリティ情報の共有・分析体制（T-ISAC）の整備（2003年～）

経済産業省関連　→　ソフトウェアの脆弱性情報の収集・共有体制（IPA, JP-CERT）の整備（2004年～）

ISP、ソフトウェア業界や総務省・経産省が連携して、ボット対策プロジェクトを開始　（2006年～）

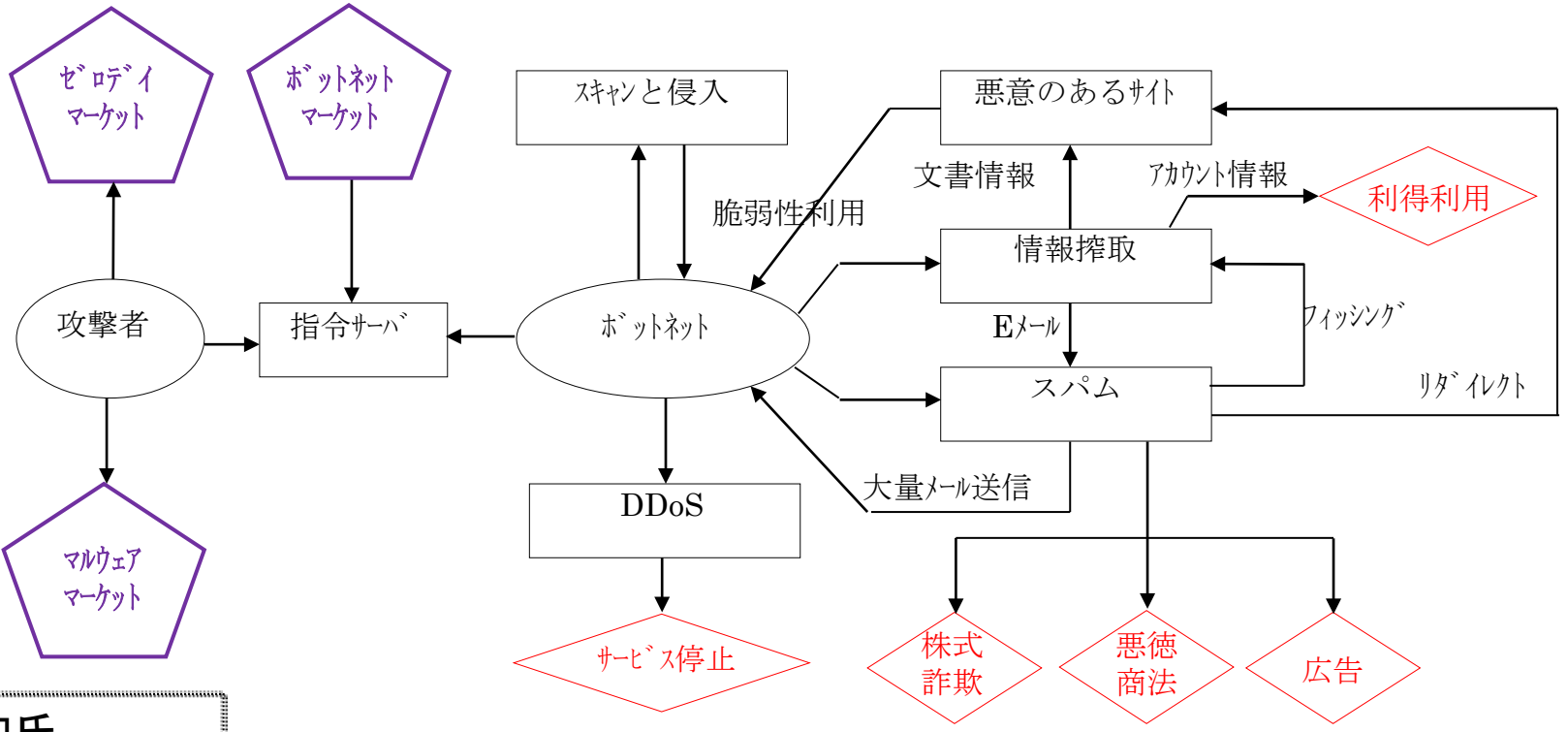
単独攻撃から連携攻撃(ボット)へ

- ボットの出現
  - ✓ 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オーバレイネットワークを形成（数百～一千万台規模）
  - ✓ 初期のボット(Sdbot, Agobot, Rbotなど)は感染形態としてはワーム
  - ✓ 指令者は膨大な数のボットを一斉遠隔操作可能



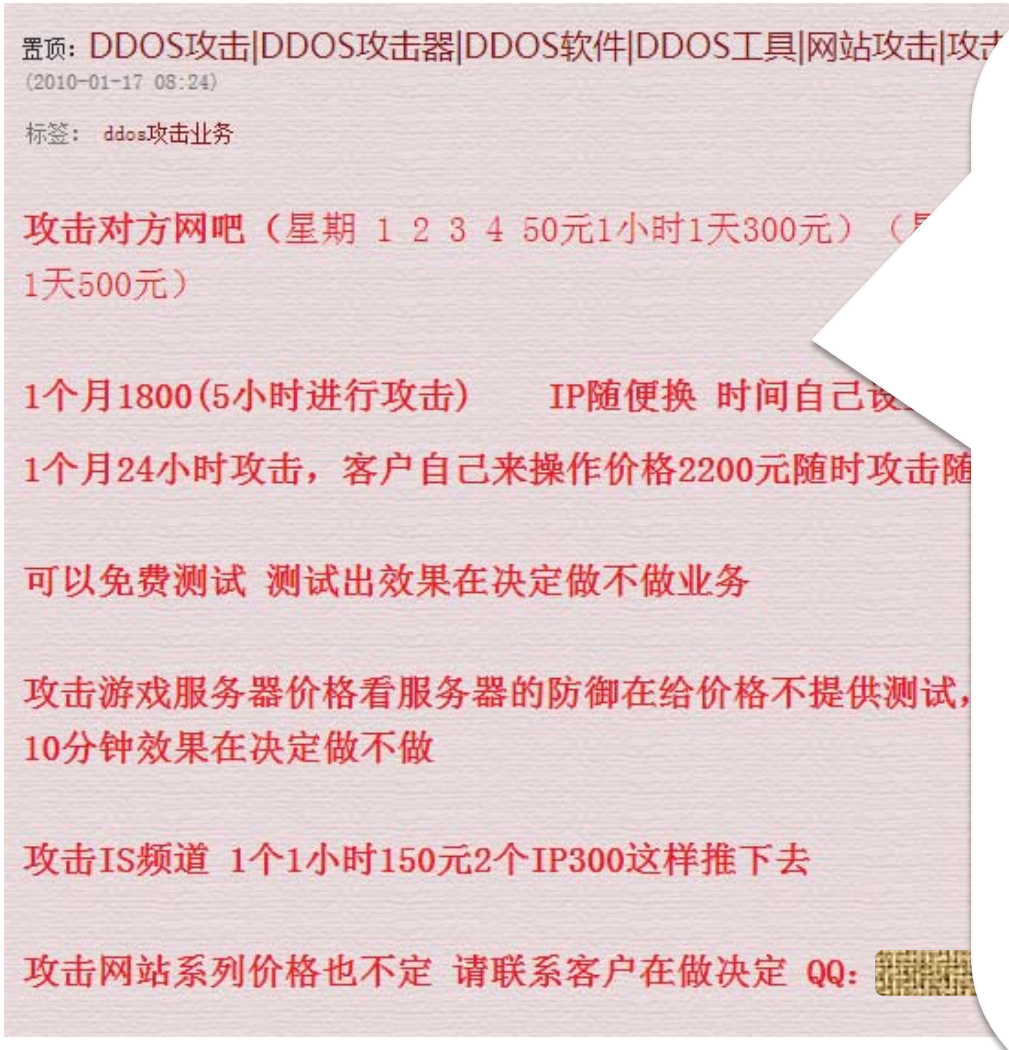
ボットネットに基づく悪のつながり

– 攻撃者が、競合他社等の「こちらにとって都合の良くない主体」に対するDDoS攻撃をすることによるサービス停止による営業妨害、不特定多数の人に対してスパムメールを送信することによる株式詐欺／悪徳商法／広告、そして、フィッシング詐欺サイトへの誘導によるアカウント情報の不正入手等をしていることを観測。



名和氏
Interop発表
資料より

ブラックマーケット(例)



インターネットカフェから攻撃
（**月曜-金曜** 50元1時間 300元1日：3700円程度）
（**土曜-日曜** 1時間100元 1日500元）

1ヶ月1800元（5時間攻撃）
IPアドレスは変更
時間はお客様が設定

1ヶ月24時間攻撃
2200元で、お客様の時間を任意に停止及び攻撃実施

テストは無料
テストは、意思決定のためであり、攻撃目的にしないでいただきたい

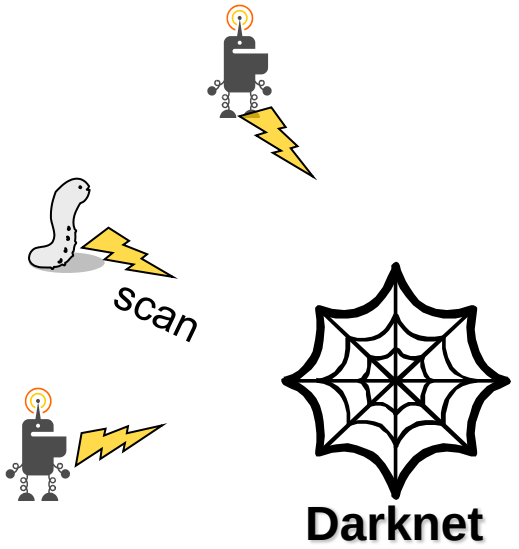
（以下、略）

名和氏 Interop発表 資料より

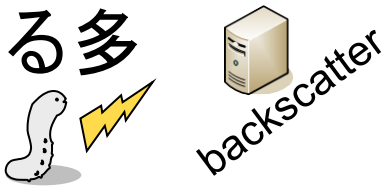
ダークネットを用いて攻撃確認を！

- ダークネット: 割り当てのないIPアドレス空間。実際のサーバ/PCなどは接続されていない。

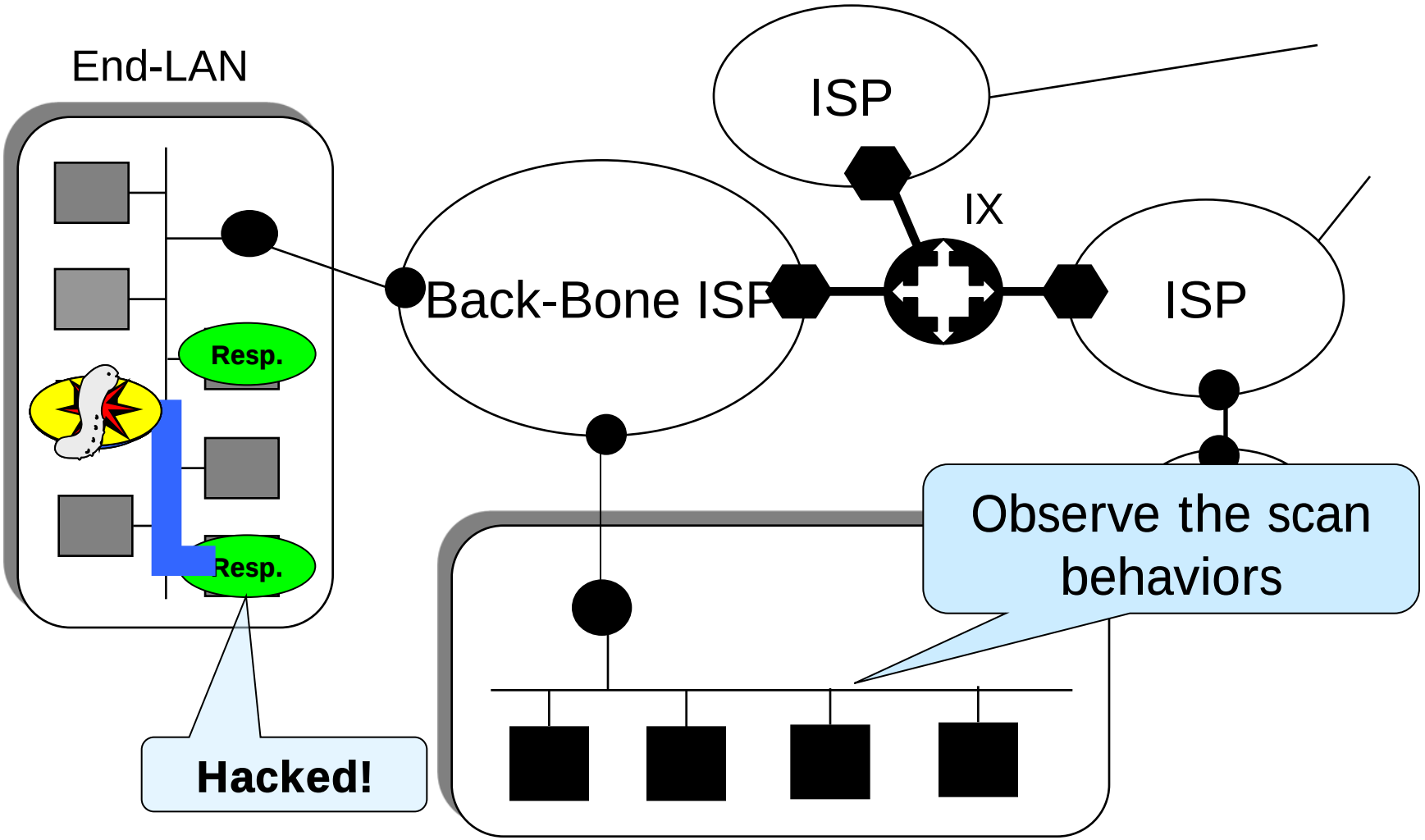
- ダークネットに飛来するパケット:
  - Scans by means of Malwares;
  - Malwares infection behaviors;
  - DDoS attacks by Backscatter;
  - Miss configurations/mistakes



- ダークネットは、インターネットにおける多くの挙動を解析するために効果的。



マルウェアの感染挙動とダークネットモニター



Dark-Net senser for Dark-Net

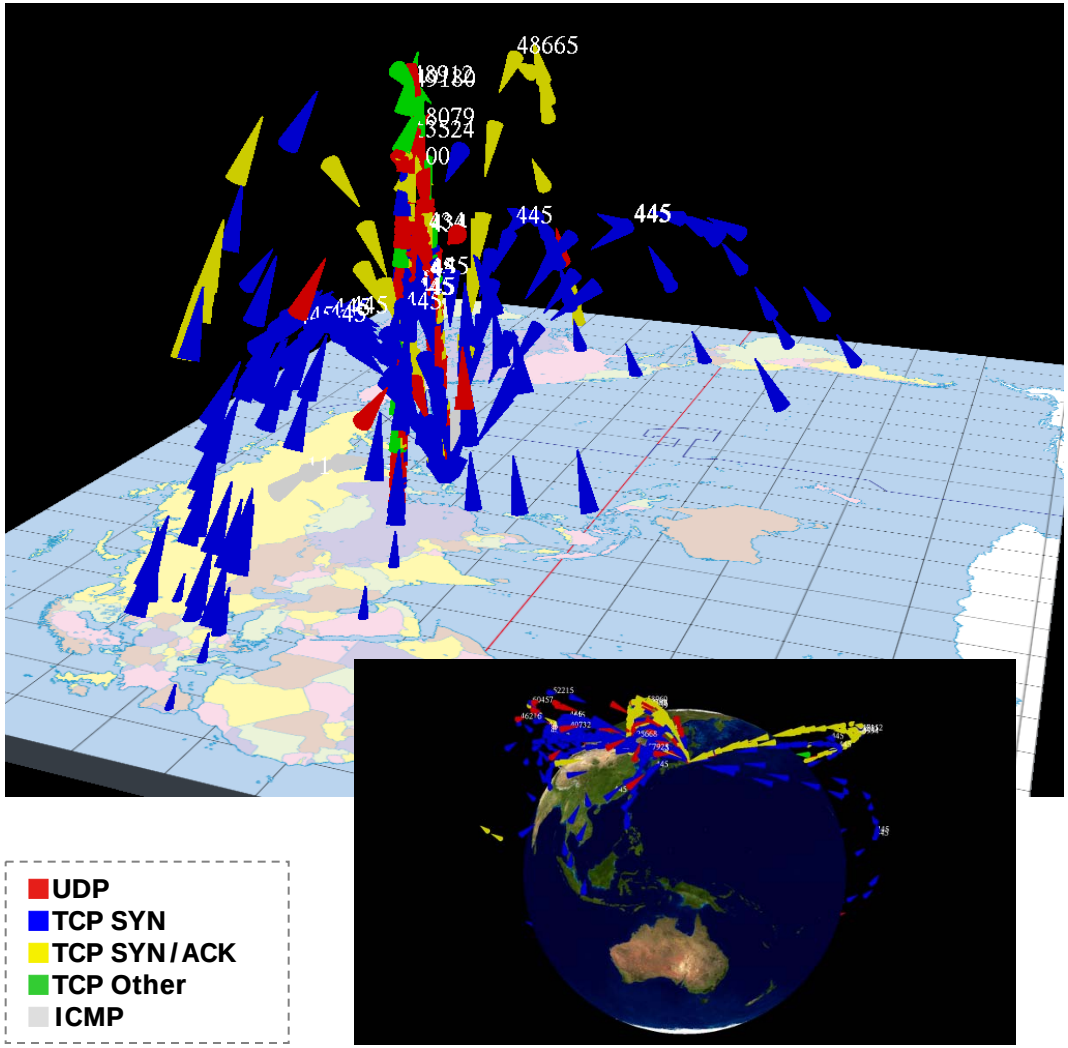
Atlas:実時間トラヒック可視化

- Shows geographical positions of a packet's src and dst from the IP addresses **in real-time**

- **Each packet** is represented by **a rocket** traversing from source to destination

- The **color** of the rocket indicates the type of packet

- The **altitude** of the rocket is in proportion to its dst port number

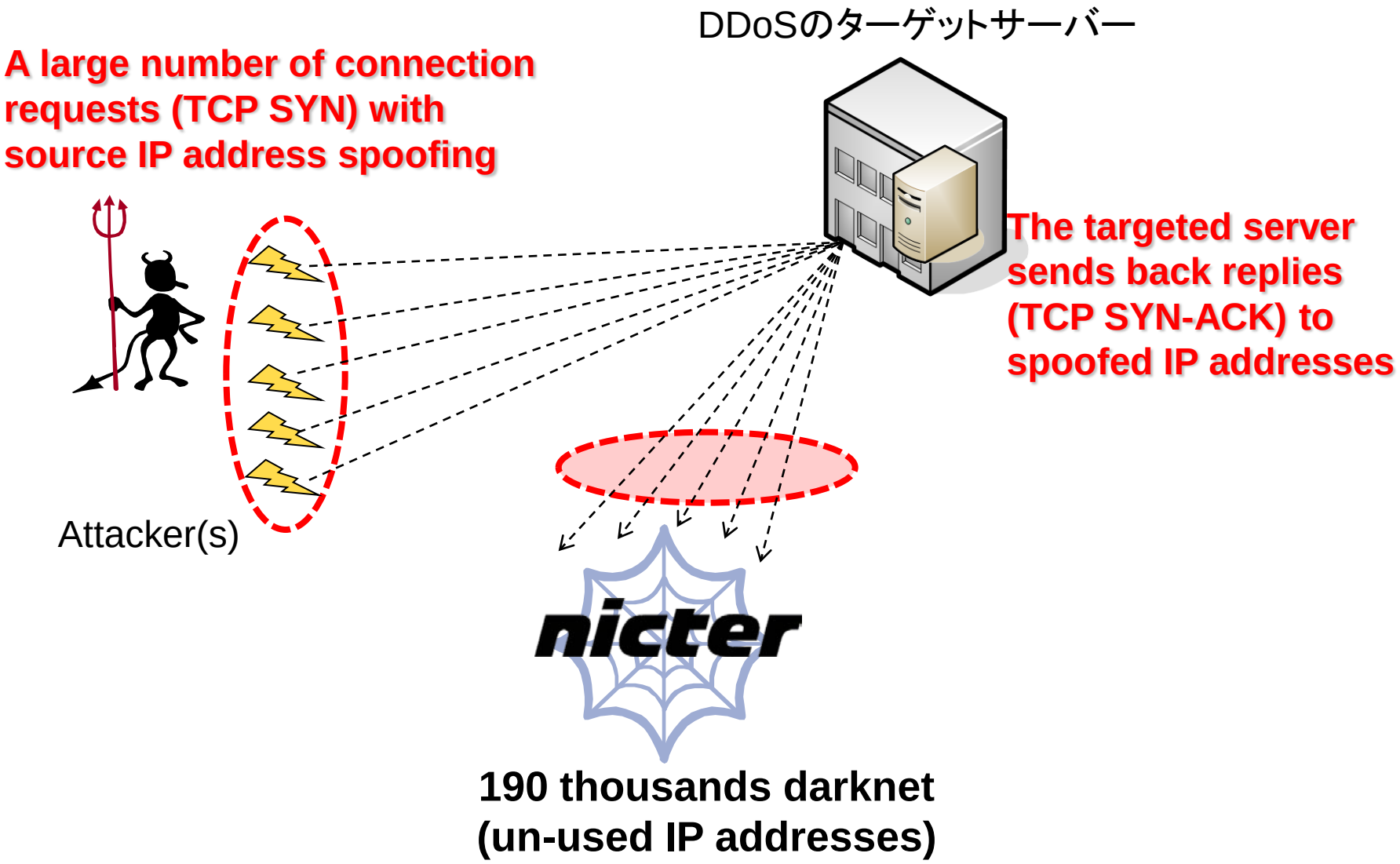


2012

Bot

US& China

Backscatter: DDoS Attack跳ね返り



大規模情報漏洩　事例　：ソニーの事例

- ソニーグループのオンラインサービスから合計1億件以上の個人情報が流出した可能性がある事件。ソニートップの経営責任の追及や、ソニーのタブレット端末などネットワーク製品戦略に与える悪影響への懸念など、史上最悪規模の個人情報流出事件のインパクトは大きい。

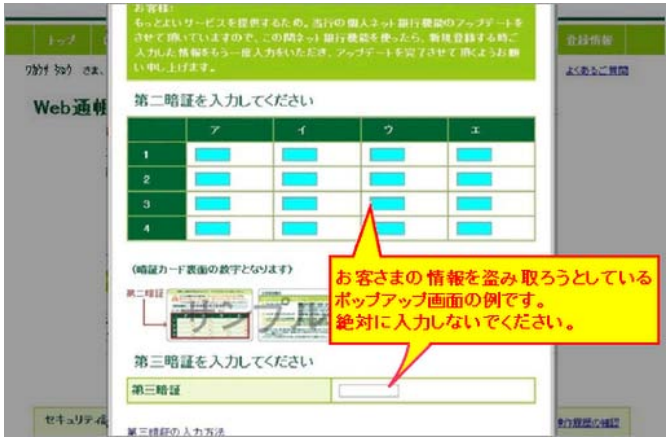
SONYからのバックスキャッター

Anonymous

2）不正ポップアップマルウェア(1/2)

出典：ゆうちょ銀行

出典：楽天銀行



出典：三井住友銀行

出典：三菱東京UFJ銀行

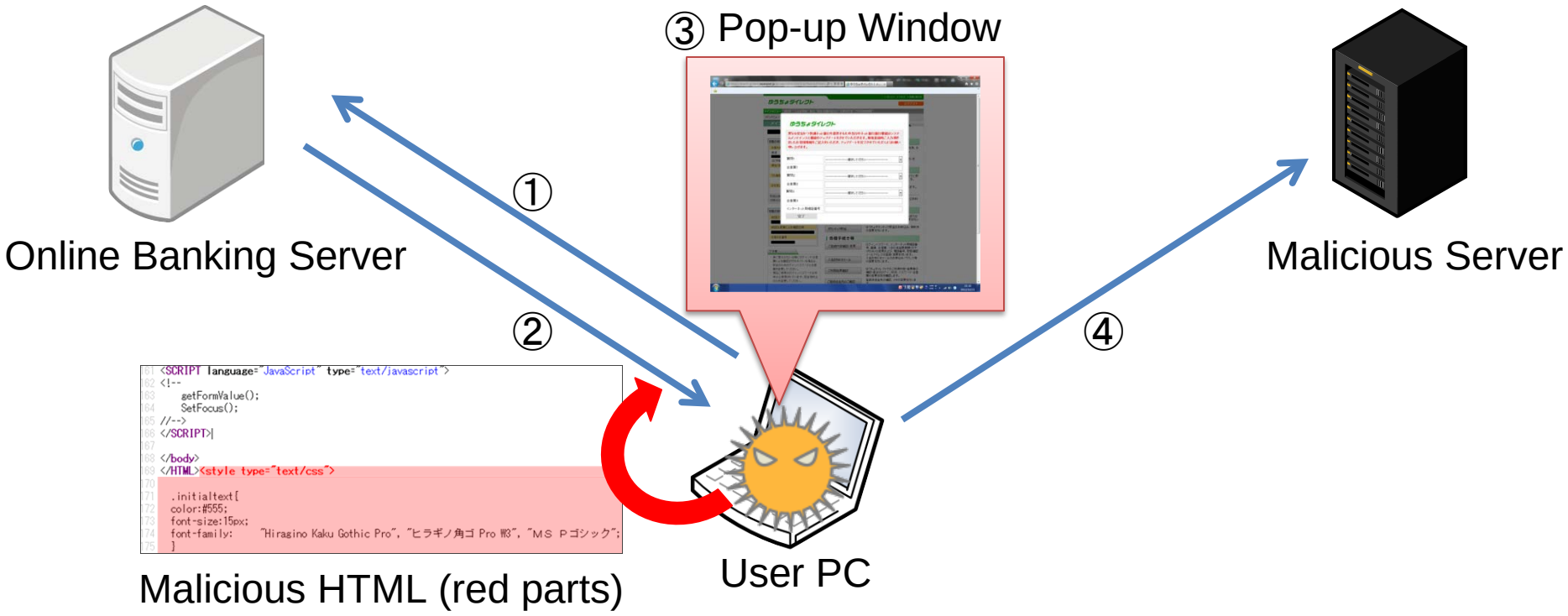
2）不正ポップアップマルウェア(2/2)

① マルウェア感染PCが正規サイトにアクセス

② 正規コンテンツにマルウェアが不正なHTMLを追記

③ ユーザの画面上に不正なポップアップが表示される

④ ユーザが入力を完了すると外部サーバに情報送付



出典：セキュアブレイン「インターネットバンキング利用者を狙ったマルウェアの挙動を解析」 2012-11-08

３）APTによる攻撃の現状

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

- APTによる攻撃の定義

  APTによる攻撃とは、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って継続するサイバー攻撃のこと。

JASA　APT研究会より

これまでのAPTによる攻撃の事例

公表時期	標的	攻撃の概要
2010年1月	米グーグルなど30数社	これは米国のグーグルなど33社がInternet Explorerのゼロデイぜい弱性を突く攻撃を受け、各企業が保有するソフトウェアのソースコード等の知的財産などが狙われたとされる。グーグルではメールサービス「Gmail」のアカウントやパスワードの一部が漏えいするなどの被害が確認された。
2010年11月	イランの核施設	ウラン濃縮用の遠心分離機の論理制御装置を乗っ取り、回転数を通常よりも過大に設定して、遠心分離機を意図的に故障させたといわれる。Windowsなどの複数のぜい弱性を突く、Stuxnetウイルスが使われた。
2011年2月	世界の石油・ガス関連企業5社	2009年11月以降、世界の石油・ガス関連企業の油田・ガス生産システムや現地調査入札関連の情報が盗み出された。中国のハッカー集団「ナイト・ドラゴン」によるものとされる。
2011年3月	米EMC	米国EMCの2要素認証製品であるSecureIDのワンタイムパスワードの生成に関する技術情報が流出。その後、米国ロッキード・マーチンへのサイバー攻撃にSecureIDのパスワード生成の情報が利用され、同社のシステムに不正侵入されたことが同年5月に明らかに。
2011年8月	世界70以上の企業や政府機関	2006年から2010年9月にかけて、重工業からエレクトロニクス企業、IT企業、オリンピック委員会など（日本は2組織）世界の70以上の企業や政府機関のコンピュータにRAT（Remote Administration Tool / Remote Access Trojan）が組み込まれ、情報が窃取された。
2011年8月	オランダ認証局のデジノター	オランダ・デジノターのSSL認証局システムが不正侵入されていたことが2011年7月に明らかになり、続いてGmailを含む多数のサイト向けのSSL証明書が不正に発行されていたことが同年8月に判明。
2011年9月	三菱重工ほかイスラエル、インド、米国の防衛産業	Flash PlayerやAdobe Readerのぜい弱性を突いた攻撃を受けた。PDFファイル付きメールを開けたPCがウイルスに感染、ネットワーク構成やファイルの所在を特定された上で、一部の端末にRATを組み込まれた。
2011年10月	外務省在外公館	日本の国外9ヶ国にある外務省在外公館の職員が使用するコンピュータ等が、情報窃取を目的とする不正プログラムに感染。不正プログラムは外務省のネットワークシステムを標的にした特殊なものとされる。
2011年10月	衆議院	情報窃取を目的とする不正プログラムに感染し、11月には全衆議院議員のID・パスワードが流出、最大15日間にわたってメールが盗聴されていたおそれがあることが判明。
2011年11月	参議院	メールに添付されたウイルスによって参議院のサーバが感染し、全参議院議員・秘書の計約千件のパスワードが流出した可能性が判明、その一部は実際の流出が確認された。

APTによる攻撃の特徴的な行動

- **ローカルPCの特権の獲得**
  - ✓ レジストリー情報の取得
    - System hiv; システム起動、デバイスドライバ、サービスに関する情報
    - Security hiv; ローカルセキュリティとユーザ特権に関する情報　など
- **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

APTによる攻撃と従来の攻撃の相違

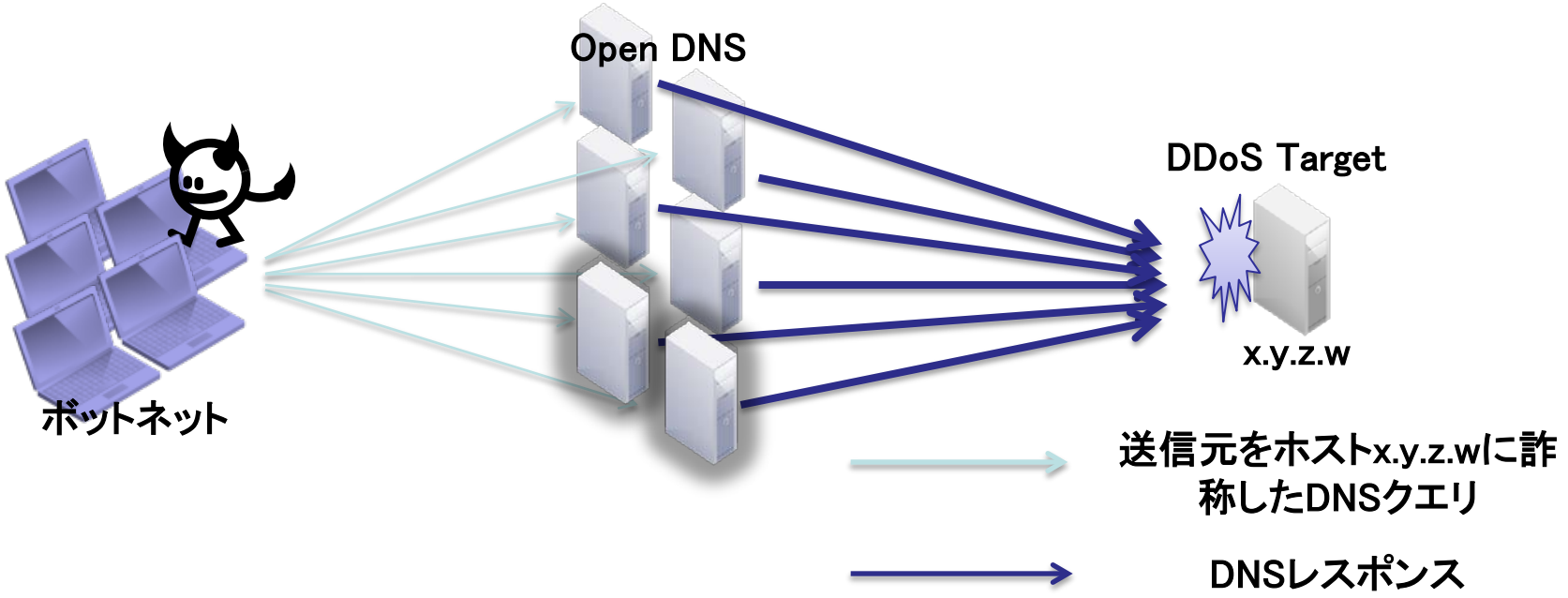
	APTによる攻撃（発見が困難）	従来の攻撃
攻撃目的	情報の収奪（スパイ行為）	多様な目的
	情報を盗むことを目的とする。動機は軍事・政治目的や経済目的など様々。	政治目的・経済目的等に加えて、いやがらせや自身が目立つためという目的もある
攻撃の重要な拠点	対象システムの内部	対象システムの外部
	目的を達成するために、対象とするコンピュータシステムの中に拠点を作り、そこから本格的な攻撃に取り掛かる	ボットネットなどを用いて、主に外部から攻撃する
攻撃ツール	特別仕様・手動ツール	標準的ツール・既成ウイルス
	目的に合わせ手作り。マニュアル（手動）操作も用いる	出来合いのツールを使う。ウイルスも闇で市販されているものが多い。
攻撃の手順	段階的で変幻自在	直線的で定型的
	対象システムの情報を入手し、それにあわせて手口を変える	標準ツール等で攻略できる範囲しか行わない
攻撃の痕跡の改ざん・消去	偽装・改ざん（痕跡なし）	痕跡にこだわらない
	発覚を遅くするために、痕跡を残さないようにする	自ら攻撃成功を誇ることがなるなど、発覚に問題がない為、頓着しない

発見の困難さ

APTによる攻撃	発見の困難さ
情報の収奪（スパイ行為）	目的を達成するまで、長期に行われるので、日々の変化が小さく、異常が目立たない
対象システムの内部	正当な行為に紛れ込むため、発見が難しい また、境界での検知の有効性が低い
特別仕様・手動ツール	パターンマッチングを行う仕組み（一般のウイルス検知ソフトなど）では発見が難しい
段階的で変幻自在	攻撃対象のシステムや権限行使状況などの情報を入手し、その分析を踏まえて次の手を行うなど、手口が複雑で分かりにくいので、発見が難しい
偽装・改ざん	正当な権利者や正当な通信に偽装する。また、目的を達成するまでの発覚を恐れて、痕跡を改ざんすることが少なくない。このため、発見が難しい

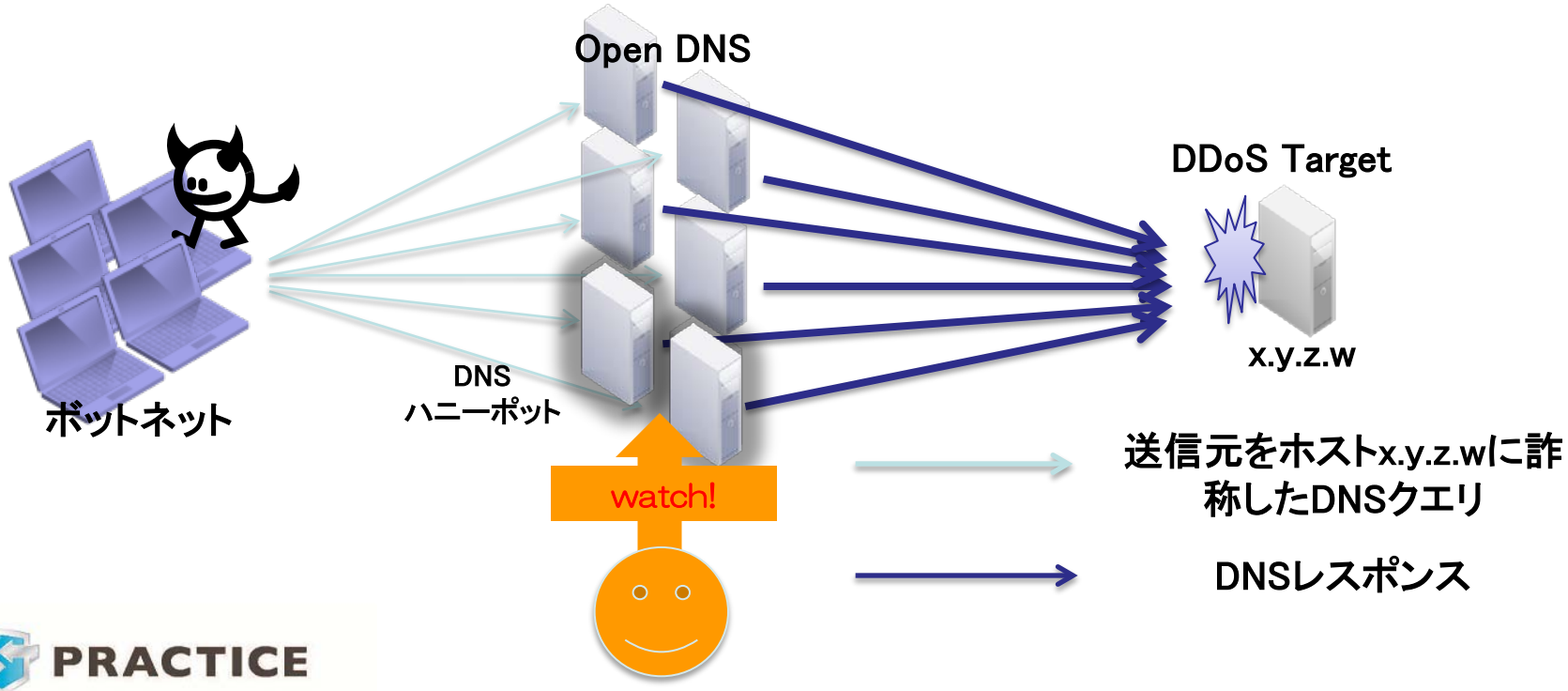
4）DNSアンプ攻撃とは

- 送信元を偽装した（スプーフ）DNS問い合わせによる攻撃
- ターゲット（偽装先）のアクセス回線帯域を溢れさせる目的
- 反射板 (リフレクター: オープンリゾルバ) を利用して攻撃を行う
- リフレクター（オープンリゾルバ）でパケットサイズを増幅させる。応答パケットは、問い合わせパケットサイズの数十倍以上。



DNSアンプ攻撃の観測
（PRACTICEプロジェクトにて（後述））

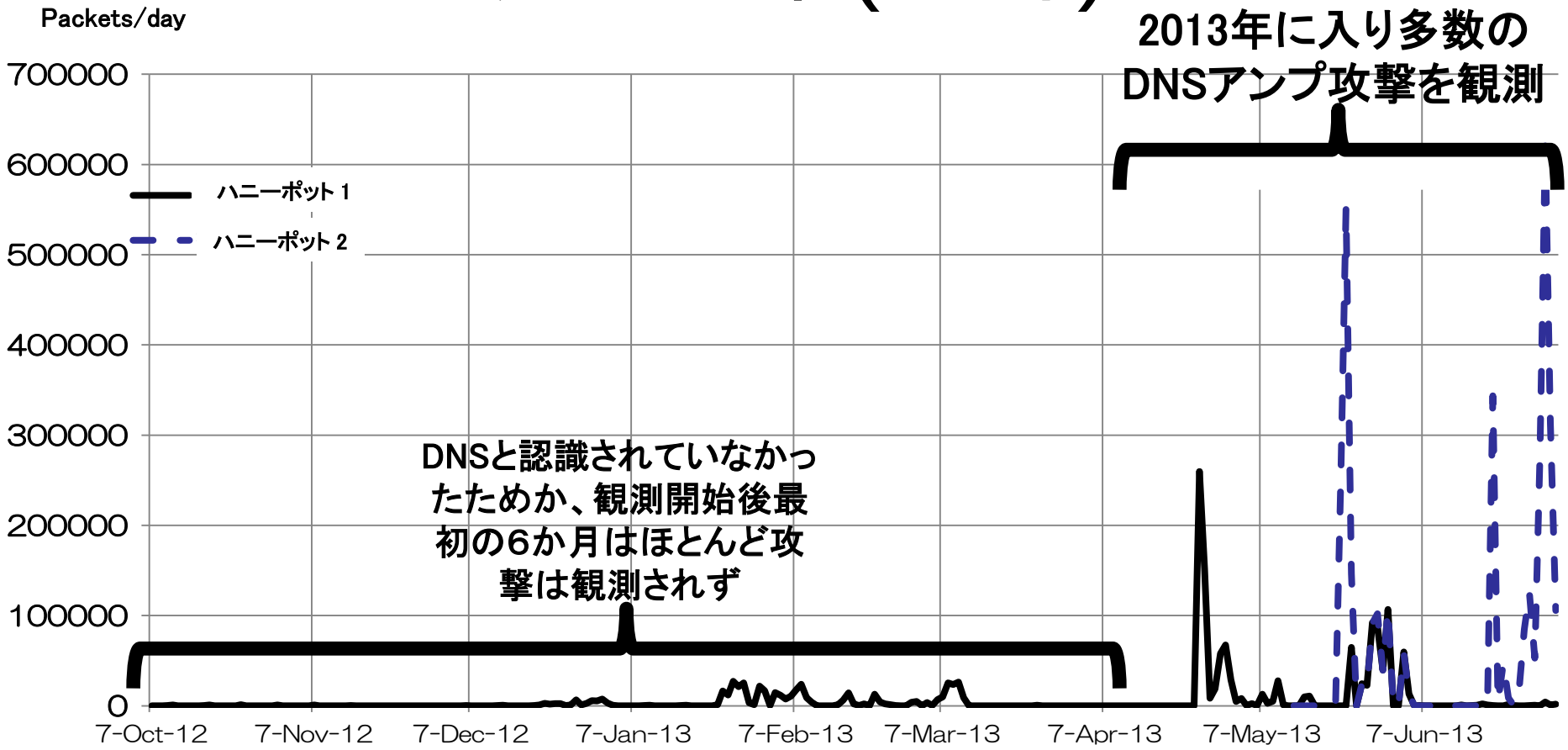
- 帯域制限のあるオープンリゾルバをDNSハニーポットとして複数台設置し、DNSアンプ攻撃の観測を実施。
- パッシブ観測(ダークネット)に比べて(1IPアドレス当り)1万倍以上のDNSクエリを観測できることが分かった。



PRACTICE

PRACTICE

観測結果(抜粋)



	honeypot1 (390days)	honeypot2 (165days)
全クエリ数	24,600,390	22,169,789
送信元IPアドレス	16,546	8,145
ドメイン数	1,363	174

PRACTICE

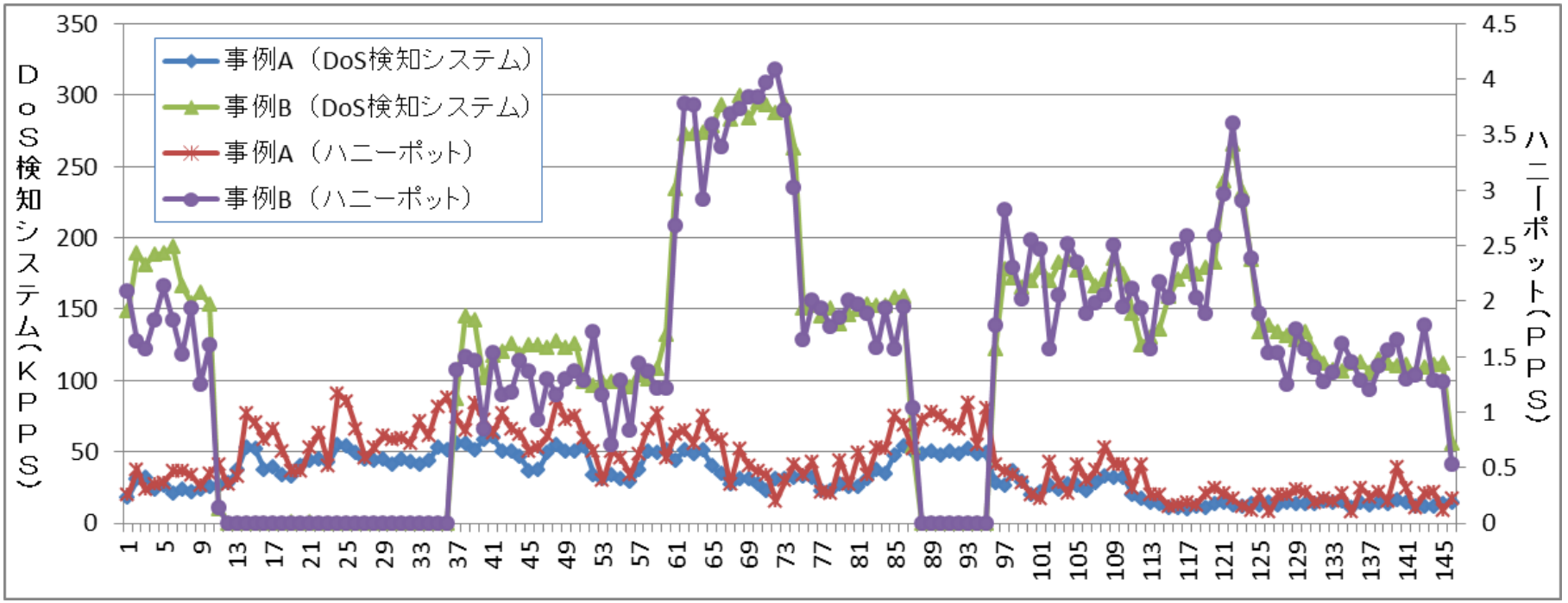
日本への攻撃例

– DNS アンプ攻撃の一部の事例 –

- 118.109.108.163 (AS2518 NEC BIGLOBE, Ltd.)
  - ホスト名：FL1-118-109-108-163.tky.mesh.ad.jp
  - 時刻(JST)：　2013-09-02 01:10:42 ～ 03:10:36（7194秒）
  - 受信パケット数：　58,359
  - 平均PPS，最大PPS：　8 pps, 10 pps
  - ドメイン名／型：　anonsc.com / ANY

- 182.23.211.158 (AS38638 Ip Core Corporation)
  - ホスト名：なし
  - 時刻(JST)：　2013-09-02 00:00:02 ～ 00:57:42（3460秒）
  - 受信パケット数：　31,627
  - 平均PPS，最大PPS：　9 pps, 12 pps
  - ドメイン名／型：　anonsc.com / ANY

DNSハニーポットとISPバックボーンのトラヒックの相関（例）

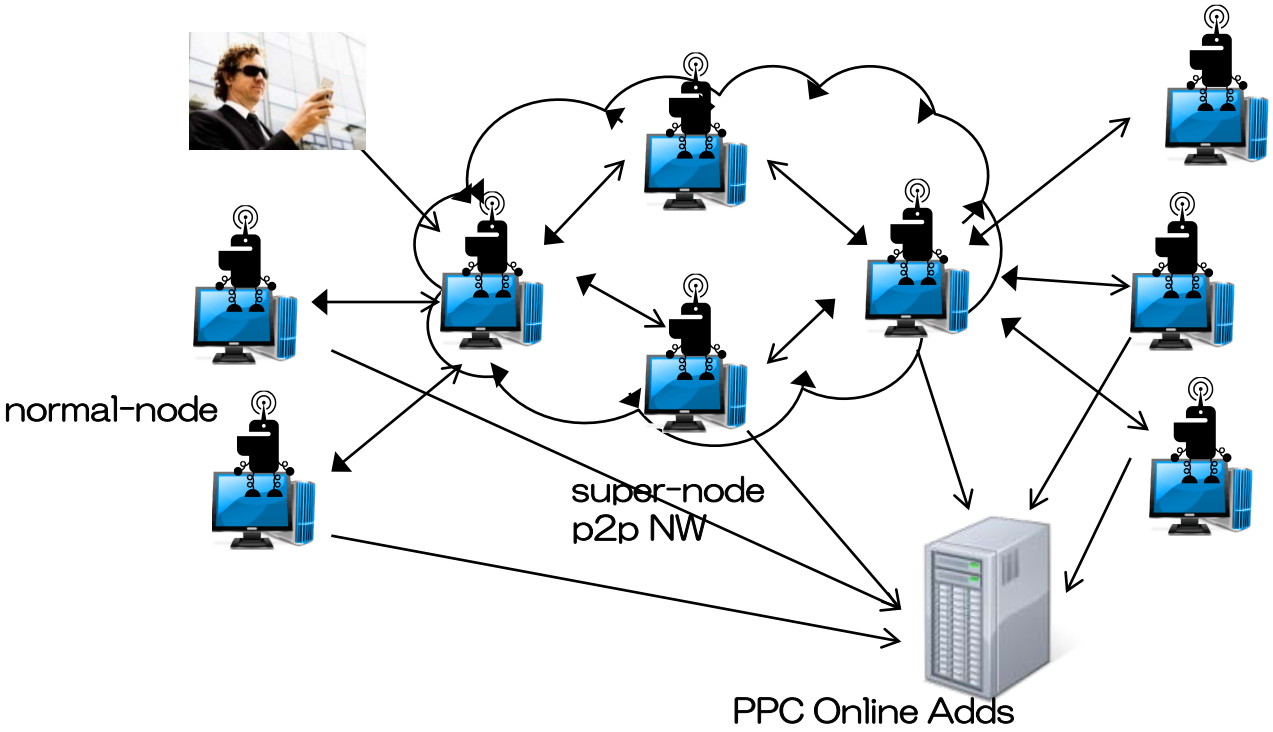


- ハニーポットとバックボーンでのトラヒック変動が同期していることを確認

- ハニーポットの検知後数分間のppsと攻撃ピーク時のppsに相関を確認
  - ハニーポット：　事例A：**0.36pps**、事例B：**1.85pps**
  - バックボーン：　事例A：**60kpps**、　事例B：**300kpps**

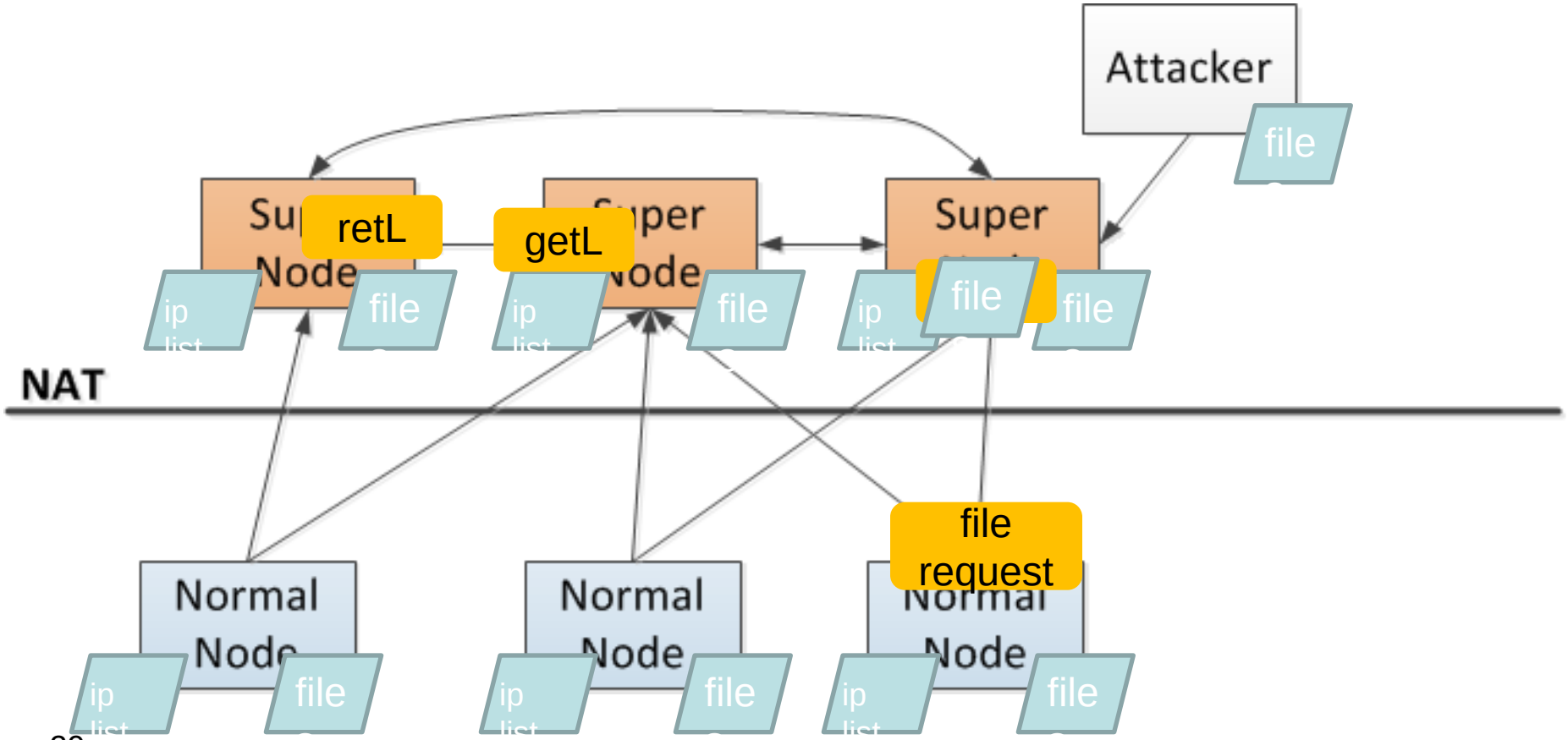
4）Zero Access: 大規模 P2P ボットネット

- 数百万の感染ホストを世界にもつ、Ｐ２Ｐベースの大規模なボットネット。
- そのＰ２Ｐネットワークを利用して、感染ＩＰアドレスや plug-in ファイルを交換する。
- RSA会議(2013）によると、140M ad-clicks/day, $0.1M/day の稼ぎが報告されている。



ZeroAccessのP2P通信モデル

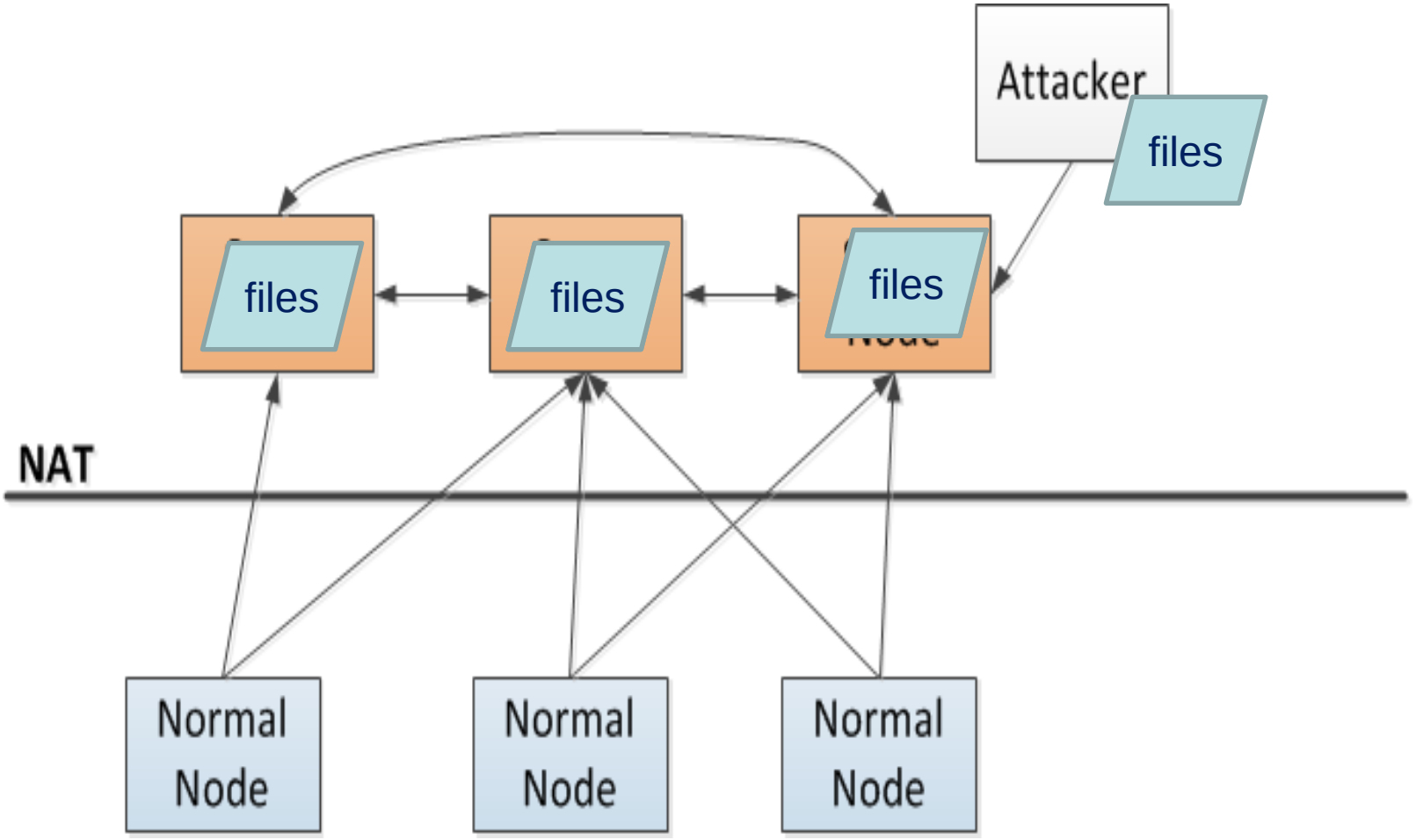
- P2P通信により感染ホスト間で通信を行い、通信先ノード情報や自身の更新のためのファイルを交換する。



29

プラグイン伝搬

攻撃者がいくつかのスーパーノードに新規のプラグインをリリースすると、P2Pネットワークを介して、当該プラグインが感染ホスト間を伝搬する。



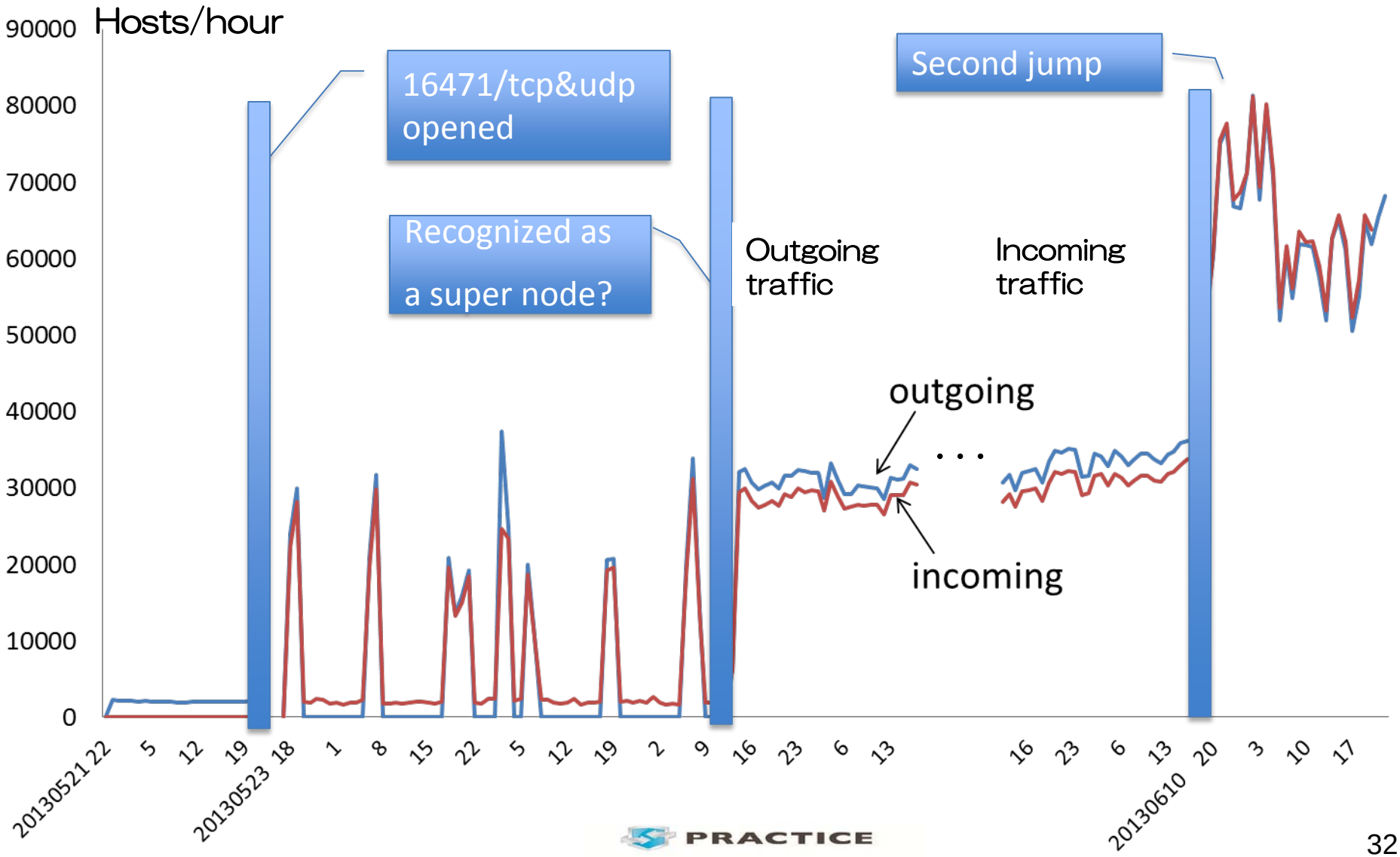
ZeroAccess検体観測結果
（PRACTICE プロジェクトにて）

- 以下の検体を長期間解析

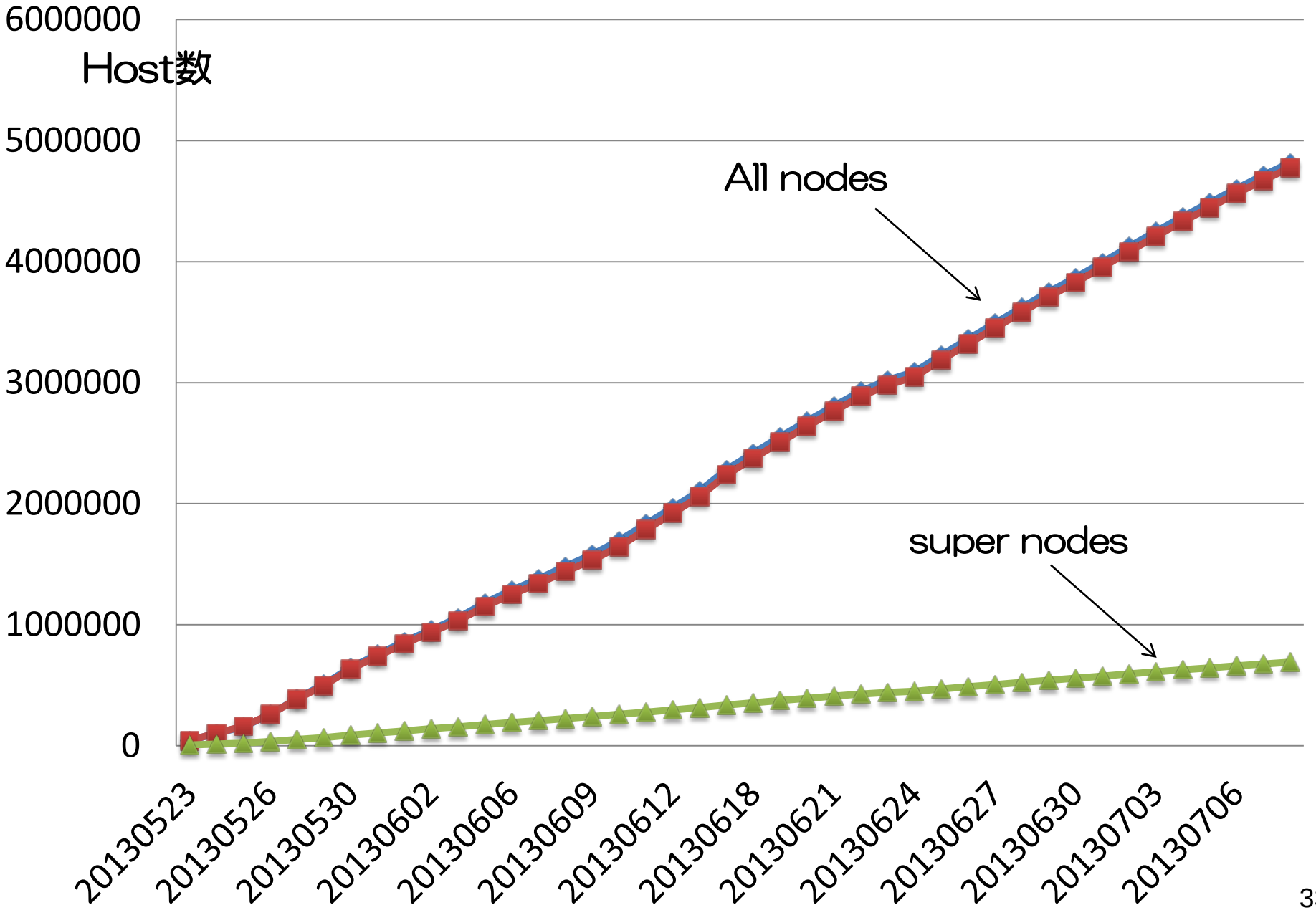
検体名	ZeroAccess.ib（McAfee）
MD5値	cd10050574974a441cc89d1a5a41ba59
解析期間	2013/5/21～現在 (断続的な解析停止あり)
待ち受けポート	16471/tcp,16471/udp

PRACTICE

単位時間当たりの接続ホスト数の推移



接続先ホストの累計


6000000
Host数
5000000
4000000
3000000
2000000
1000000
0
All nodes
super nodes
20130523
20130526
20130530
20130602
20130606
20130609
20130612
20130618
20130621
20130624
20130627
20130630
20130703
20130706

ZeroAccess感染情報

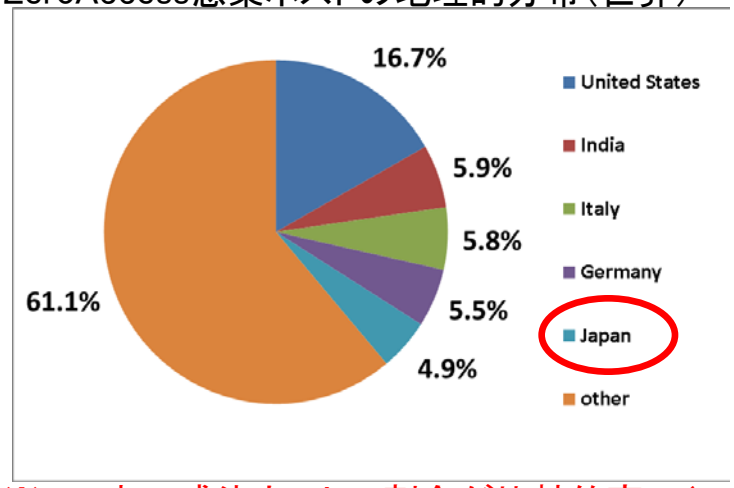
PRACTICE（後述）のサンドボックス環境から得られた感染ホス情報を連携先へアウトプット

PRACTICE連携先における感染ホスト台数

ZeroAccess感染ホスト（台数）
Malaysia : N（54,020台）, S（876台）
Thailand : N（78,578台）, S（1,687台）
Indonesia : N（66,287台）, S（2,170台）
Singapore : N（17,239台）, S（2,530台）
Philippine : N（41,051台）, S（2,464台）

※ ”N”はNormal node, “S”はSupernodeの件数

ZeroAccess感染ホストの地理的分布（世界）



※ 日本の感染ホストの割合が比較的高い（4位、5%）

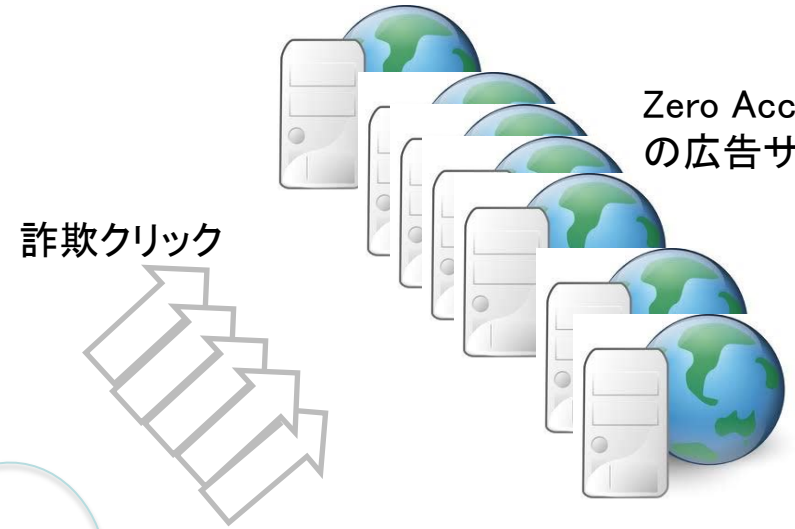
以下期間を対象：2013/05/23 ～ 2013/06/17、2013/07/17 ～ 2013/09/25、2013/10/06 ～ 2013/10/22

ZeroAccessの感染ホストリスト(一部事例のみ抜粋)

Source IP	Source Country	Netname / descr	Oraganization	Reverse lookup result
58.9.88.169	Thailand	Internet Service Provider Co., Ltd.	ISP	ppp-58-9-88-169.revip2.asianet.co.th.
218.186.85.108	Singapore	StarHub Cable Vision Ltd SGCABLEVISION-SG	ISP	cm108.omega85.maxonline.com.sg.
60.50.92.253	Malaysia	TMNST ADSL-STREAMYX	ISP	253.92.50.60.cbj05-home.tm.net.my.

12月5日の前後の状況の変化

12/5にMSがPPC(Pay-Per-Click)などに関連するサイトのTake Downを実施。



12月5日より前

幾つかの広告用ドメインやIPが減少

12月5日より後

PRACTICE

本日のトピック

最近のセキュリティ脅威（攻撃）の紹介

1）これまでの脅威（ボットネット中心）

2）不正ホップアップマルウェア

3）APTによる攻撃

4）最近のDNSアンプ攻撃、ZeroAccessボット

脅威に対抗するための対策の動向

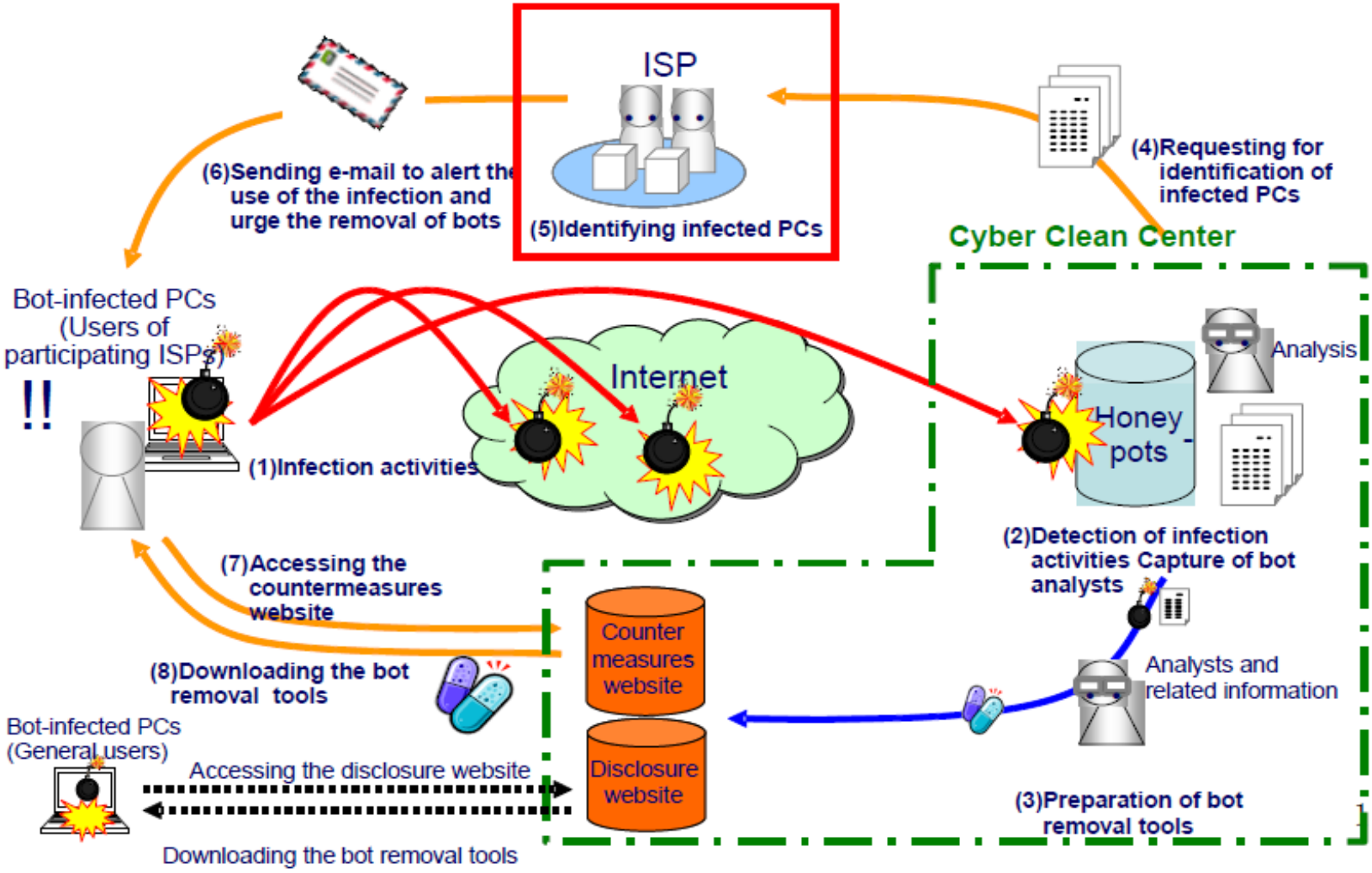
5）ボットネット対策（日本、韓国、台湾、ドイツ）

6）APTによる攻撃の対策

7）NICTにおける研究活動（対策への活用）

まとめ

ボットネット対策(1):CCC の旧枠組み(日本)



総務省、経済産業省の連携プロジェクト

Figure 2 – Workflow of bots detection and response in CCC

ボットネット対策（2）DNS sinkhole scheme （韓国）

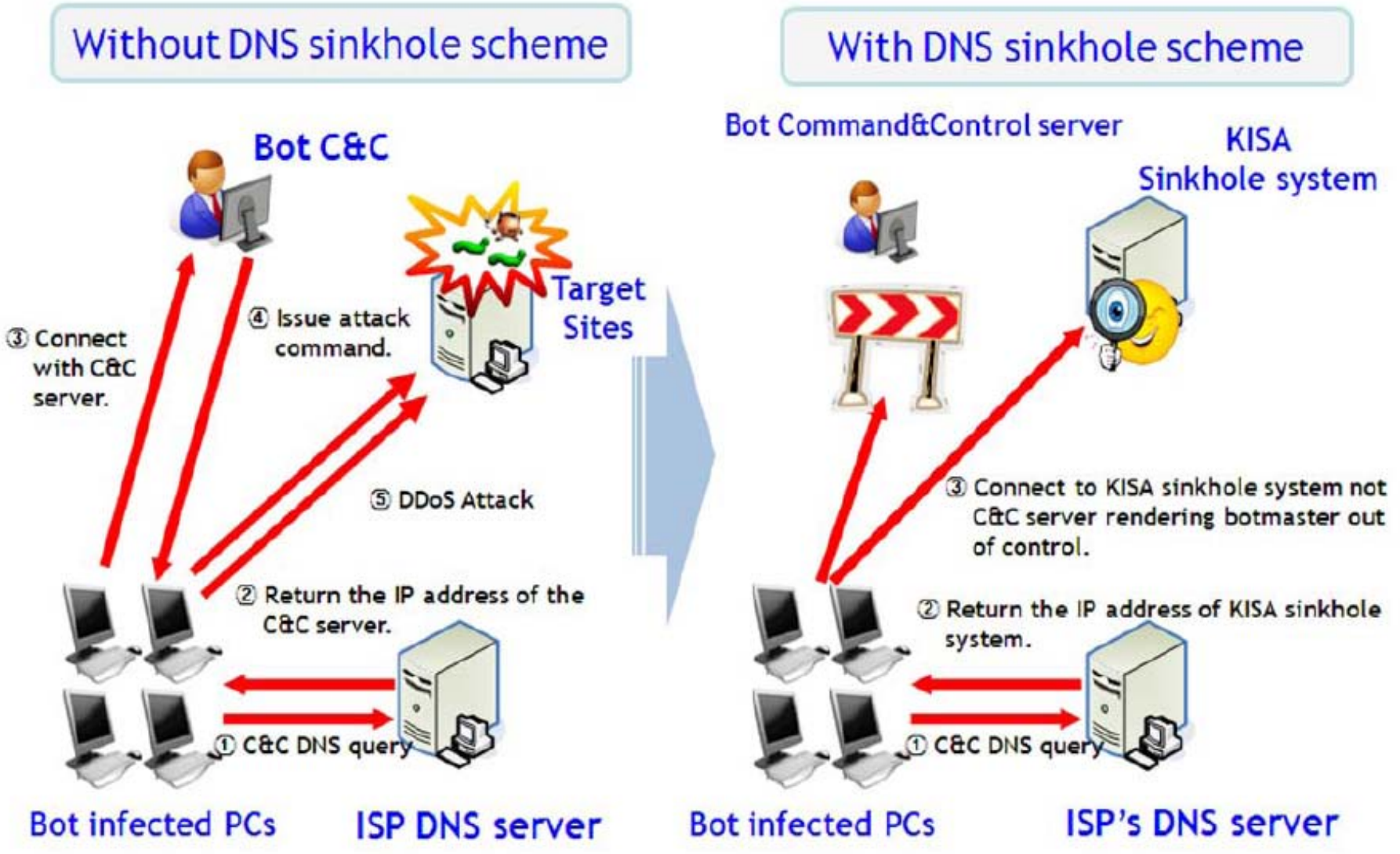
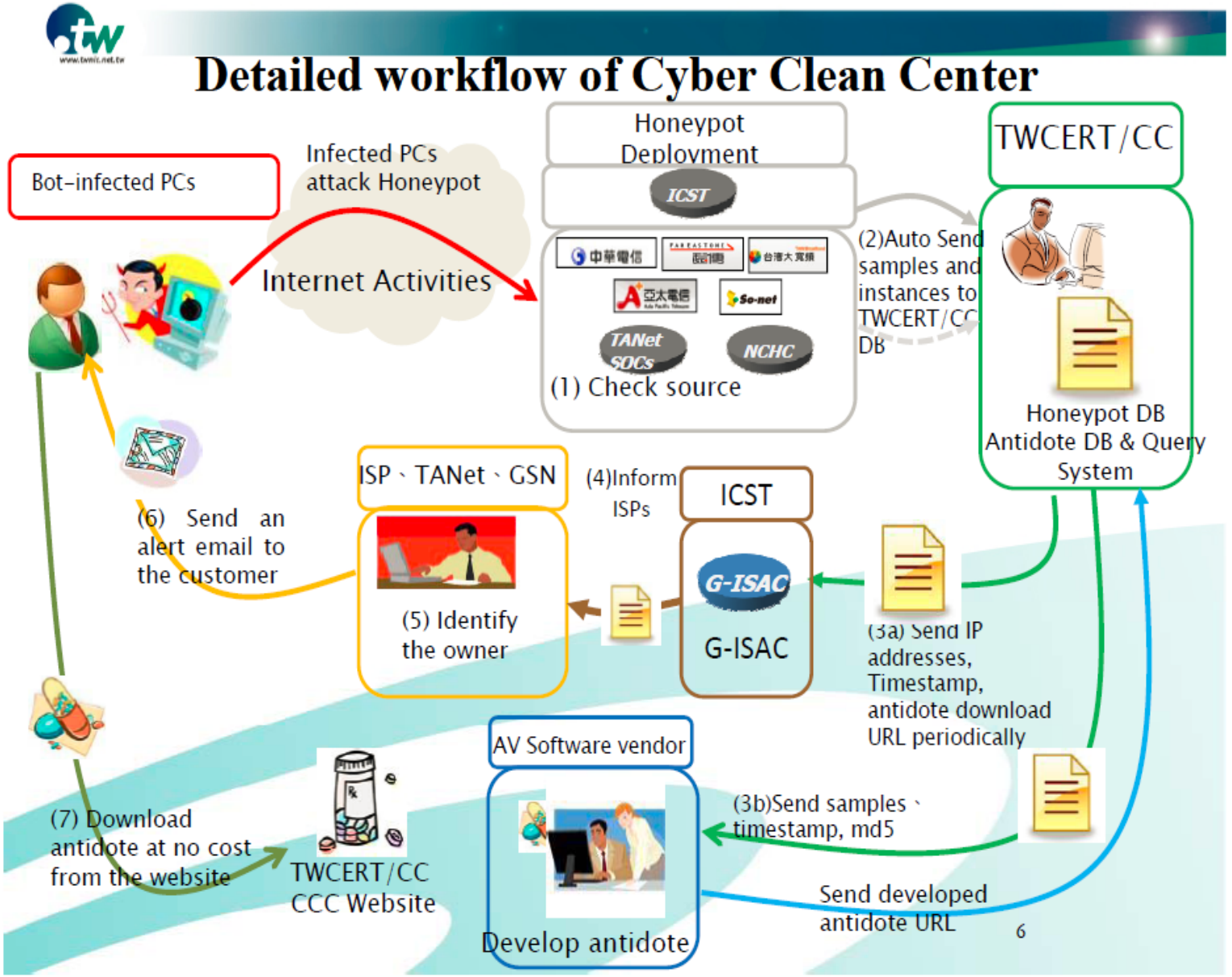
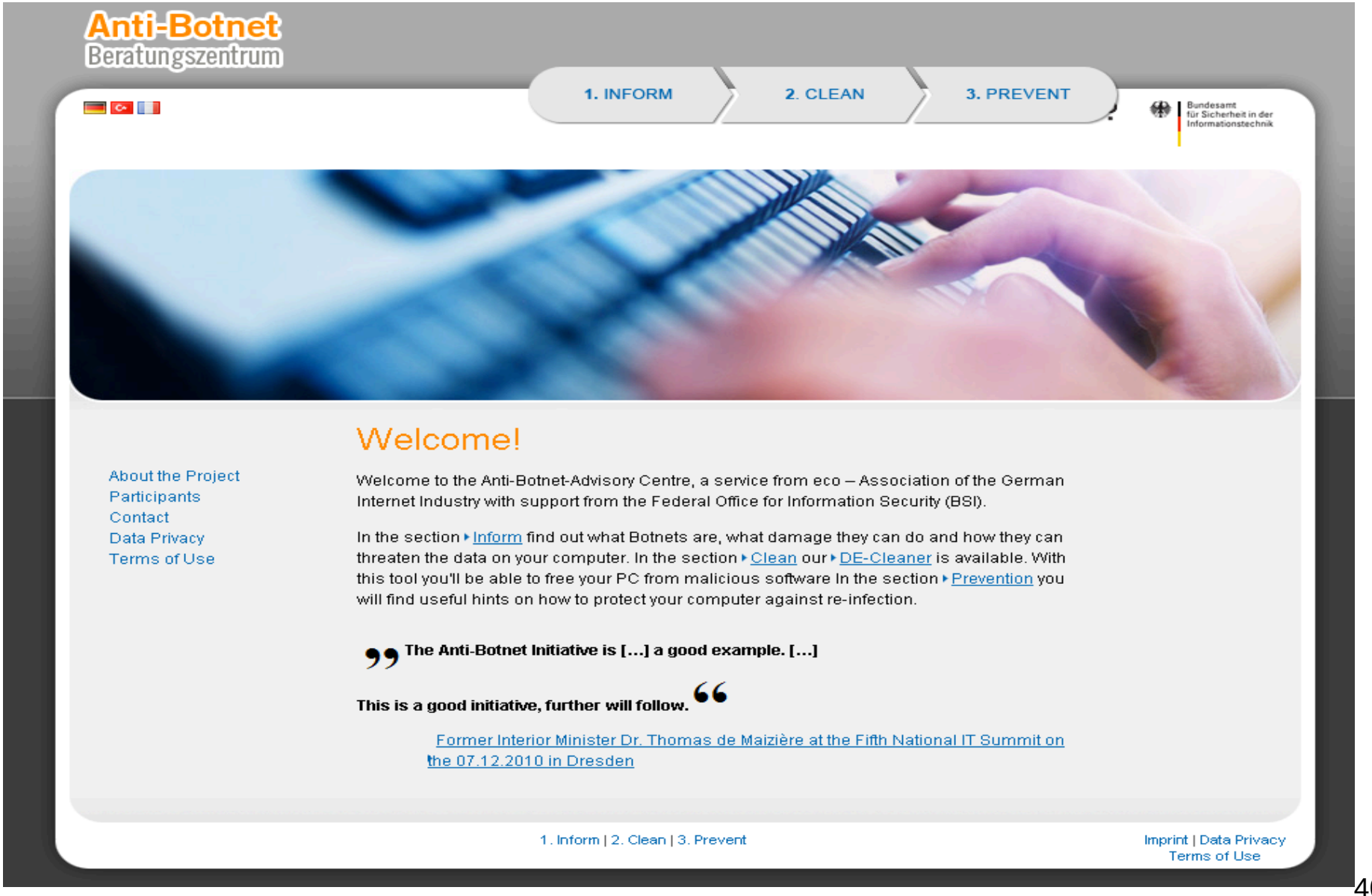


Figure 4 – Effectiveness of the DNS sinkhole scheme

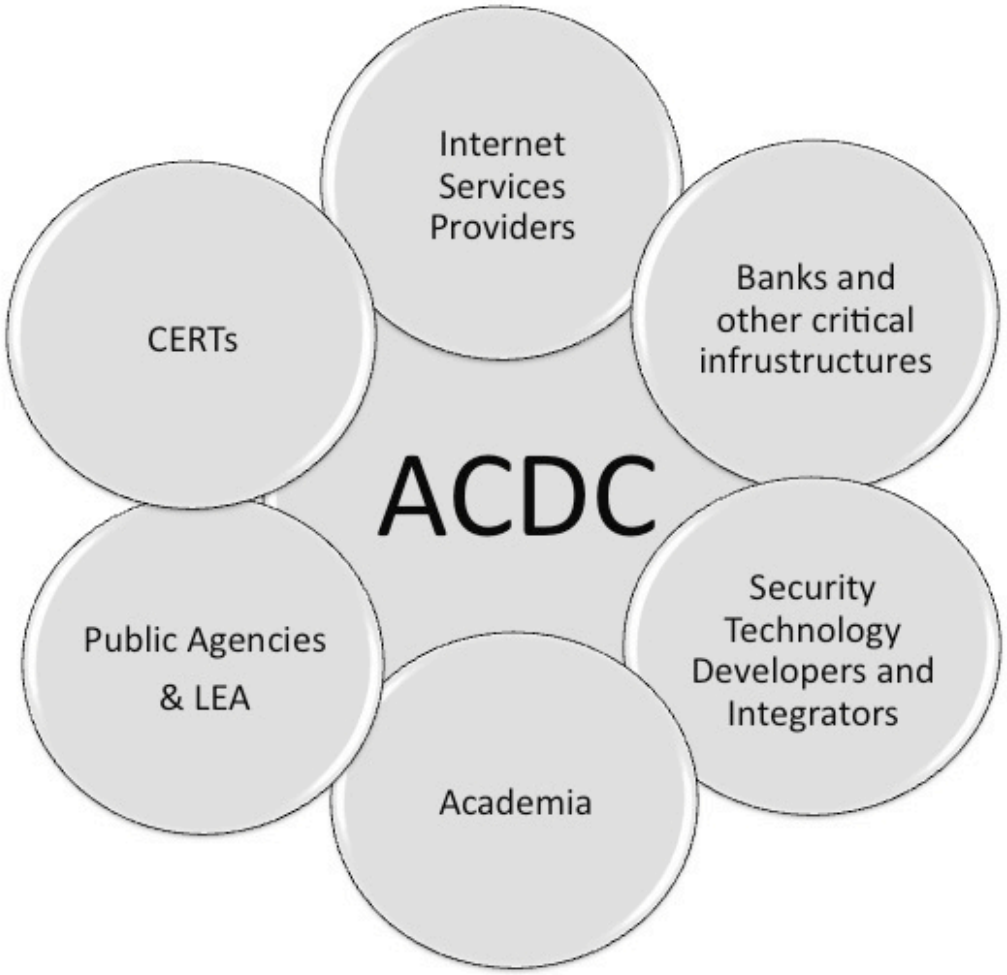
(参考)国外におけるサイバー攻撃に関連する取組事例調査
台湾:サイバークリーンセンター



ボットネット対策（3）:ドイツにおけるボット対策（ECO）



ACDC – Advanced Cyber Defence Center – Consortium Structure



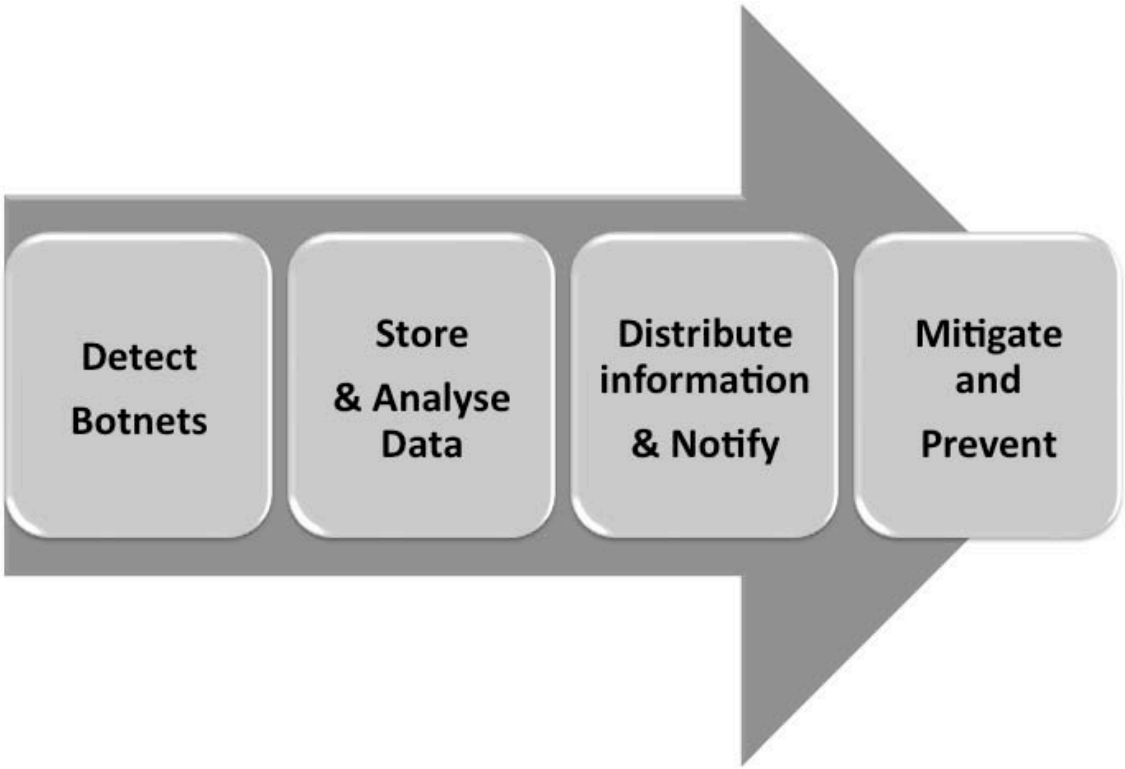
28 partners – 14 member countries

- ECO Association of the German Internet Industry
- Technikon Forschungs- und Planungsgesellschaft mbH
- Atos Spain S.A
- Bulgarian Posts PLC
- Croatian Academic and Research Network - CARNet and Croatian National CERT
- Romanian National Computer Emergency Response Team - CERT-RO & Romanian Partners
- Cognitive Security s.r.o.
- Cassidian (EADS Company)
- CyberDefcon
- DE-CIX
- DFN CERT Services GmbH
- Engineering Ingegneria Informatica
- FCCN - Foundation for National Scientific Computing

- Fraunhofer FKIE
- G Data Software AG
- Institute for Internet Security, Gelsenkirchen University of Applied Sciences
- INTECO - National Institute of Communication Technologies
- KU Leuven
- LSEC - Leaders in Security
- Microsoft EMEA
- SignalSpam
- Telecom Italia
- Telefonica I+D
- University of Technology - Delft
- XLAB Razvoj programske opreme in svetovanje d.o.o.
- Fundació Privada Barcelona Digital Centre Tecnològic
- Istituto Superiore Delle Comunicazioni e delle Tecnologie dell'Informazione
- Montimage

ACDC – Approach

From Detection to Protection



総務省におけるボット対策

総務省における官民連携事業（施策）　～これまでとこれから～

マルウェアの変遷

より高度で多様なマルウェア

より高度で多様なマルウェアが次々と出現。

Webを見ただけで感染するWeb感染型マルウェアが台頭。

Drive-by-download

ボット

インターネットにつないだだけで、インターネット利用者の知らない間に感染するボットが主流。

国際的な連携体制を構築。
海外からのサイバー攻撃情報を収集し、攻撃の予兆を捕捉。

ACTIVE
Advanced Cyber Threats response InitiatiVE
2013~2017

マルウェア感染防止・駆除の取組

PRACTICE 2011~2015

国際連携によるサイバー攻撃予知・即応システムの実証実験

RDB 2009~2011

マルウェア配布等危害サイト回避システムの実証実験

ボット感染率が大幅に低下。
2.5%(2005年)
→ 0.6%(2011年)

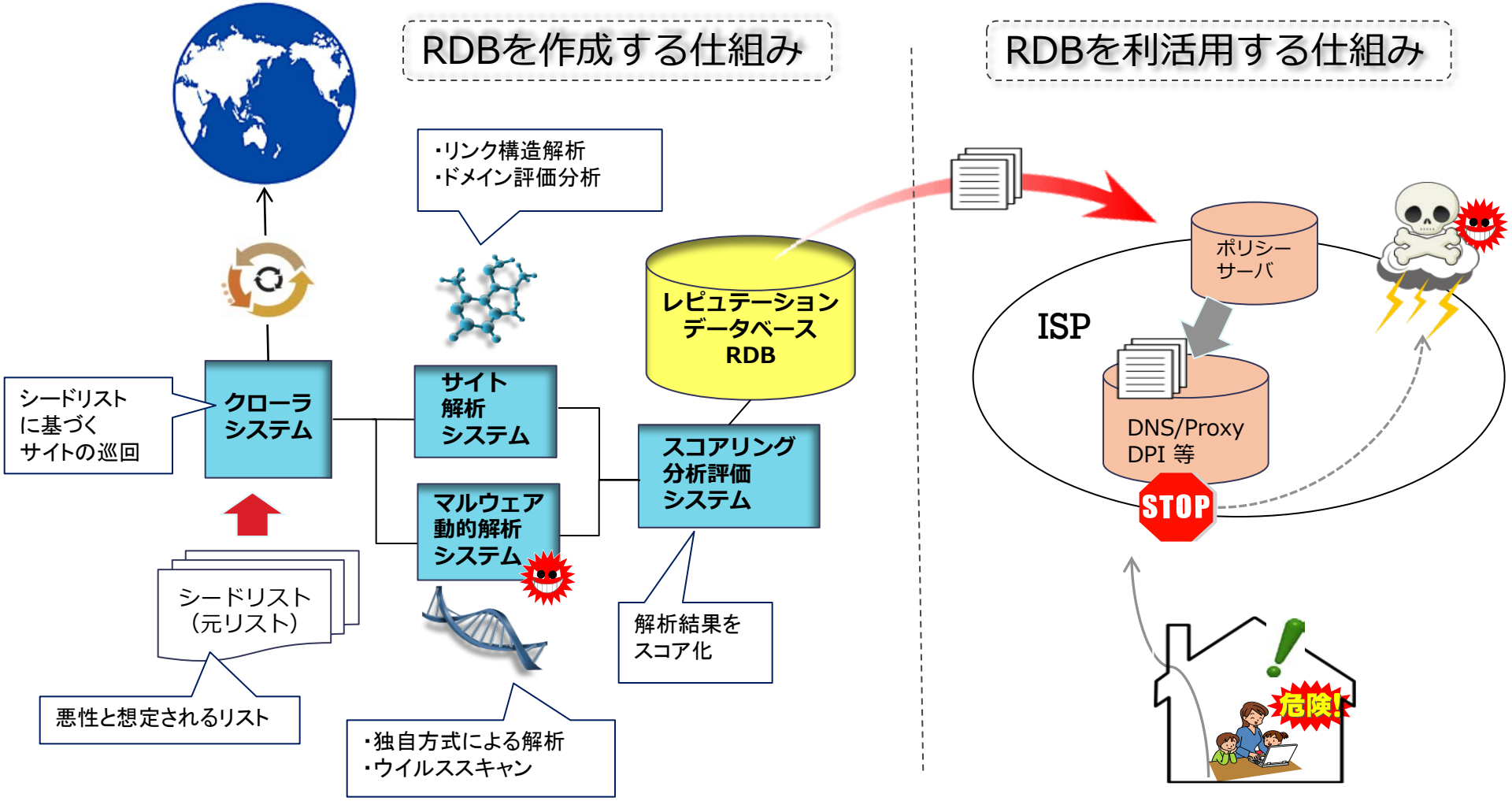
Cyber Clean Center

Cyber Clean Center 2006~2010

ボット対策プロジェクト（総務省＋経済産業省）

総務省プロジェクト：「マルウェア配布等危害サイト回避システム」の活用（RDB: Reputation DataBase)

Webアクセスによりマルウェアに感染するサイトを特定してデータベース化し、その情報をISPへ提供することによって、ユーザをWeb感染から守れるようにするための基盤となる実証



PRACTICEプロジェクト
―研究開発の目的・目標―

目的

サイバー攻撃（マルウェアの感染活動、分散型業務妨害攻撃等）に関する情報収集ネットワーク及び連携体制を国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等から受けるリスクを軽減する。

研究開発目標

国際的なサイバー攻撃への速やかな対処を行うためには、その脅威を正確かつ速やかに察知することが必要不可欠である。本研究開発は、国際連携により各地のサイバー攻撃情報（ダークネット観測により取得したスキャンやシェルコード等の攻撃パケット情報、Web型も含めたマルウェア感染活動情報等）を収集し、それを実時間で分析することにより、サイバー攻撃の脅威を速やかに把握する技術及び高度分析による将来のサイバー攻撃状況の推移を予測する基盤技術の確立を目指す。

PRACTICE

Proactive **R**esponse **A**gainst **C**yber-attacks **T**hrough **I**nternational **C**ollaborative **E**xchange

研究開発の概要：サイバー攻撃予兆のための前提、アプローチ、目標

前提

サイバー攻撃が行われる前には、ボットネットを用いた攻撃インフラにおいて、何らかの予兆(攻撃者による準備行動等)が現出する

アプローチ

予兆を捉える ＝「ボットネットの活動を把握する」
予兆把握の仕組みを構築し、早期対策に役立てる

予兆警報として目指すもの（目標）：
①今後急激な増加が見込まれるマルウェアに起因するスキャン攻撃を検知、及び、今後急激な増加が見込まれるマルウェアを捕獲量の視点で検知すること。これらの結果は、マルウェア駆除の活動として、ACTIVEや関連ベンダーと連携する予定。
② Sandbox上で飼育するDNSハニーポット/マルウェア、及びnicter ダークネットを用いて、「DNSアンプ攻撃」や「ZeroAccess新Plug-in（機能追加）」などの警報を発動する。結果、PRACTICE実証実験及び、ISPとの連携により即応などの対応が必要。（事例ベースのアプローチとなる）
③ Sandbox上で飼育するボット系検体を観測することにより、C&CやDNSとのやり取りを監視し、C&Cリスト、ボット攻撃命令などが把握できた場合は、ボット挙動警報を発出する。PRACTICE実証実験及び、ISPとの連携を想定。同時に、ACTIVEとの連携と必要。

新プロジェクト
ACTIVE　概要説明

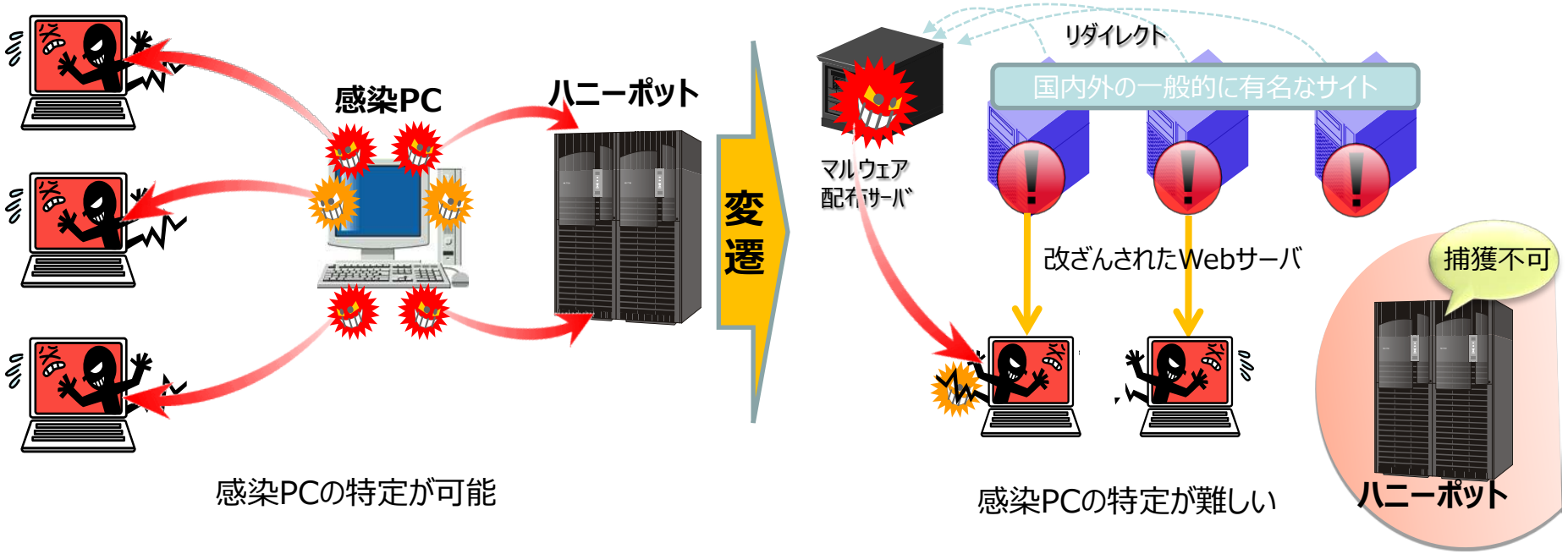
背景：マルウェア感染経路の変遷

ネットワーク感染型マルウェア

ネットワーク経由で感染するマルウェア。
ハニーポットにて捕獲可能であり、旧CCCの駆除対象。

Web感染型マルウェア

Webサイトへのアクセスにより感染するマルウェア。
ネットワーク感染型の他、こちらの脅威に対する対応も必要。



感染PCの特定が可能

感染PCの特定が難しい

カスペルスキー社のレポートによると…

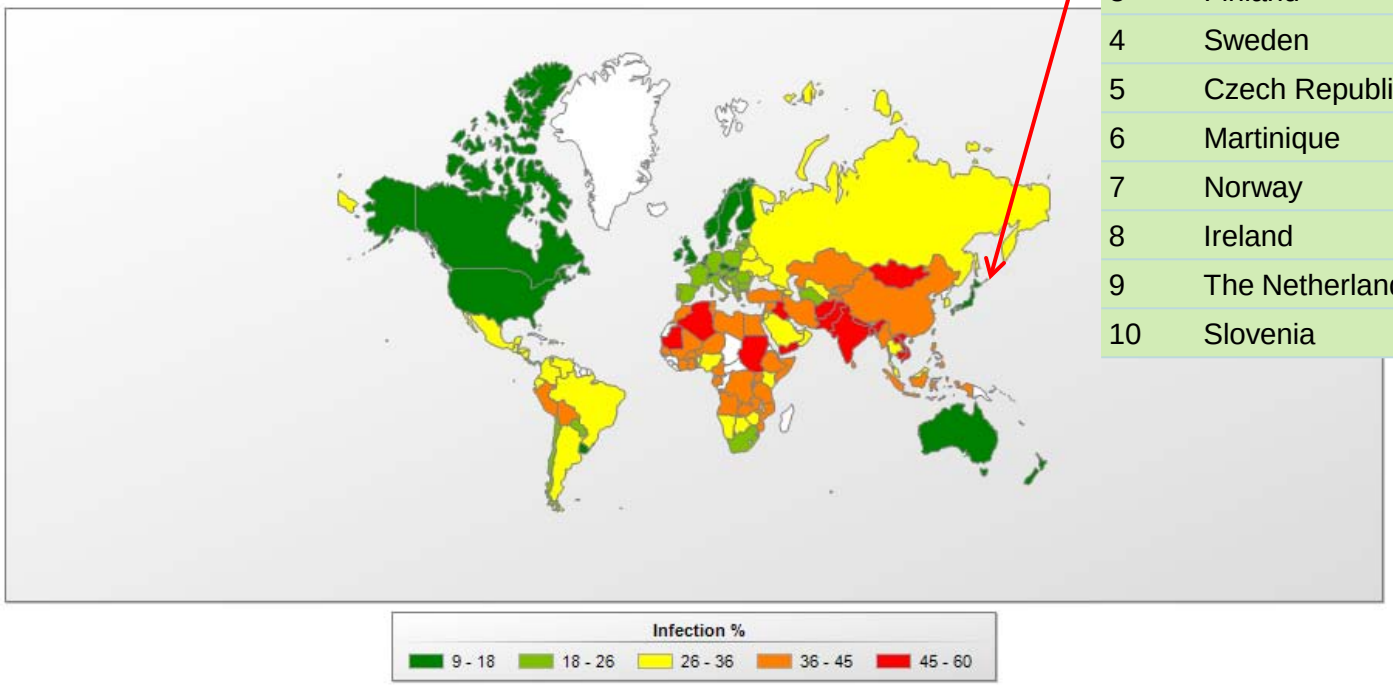
- **マルウェアの感染率は、日本が最低である。**

以下に、マルウェア感染率の低い順のトップ１０を示す。

IT Threat Evolution: Q2 2013

http://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013

Rank	Country	%
1	**Japan**	**9.01%**
2	Denmark	9.72%
3	Finland	11.83%
4	Sweden	12.10%
5	Czech Republic	12.78%
6	Martinique	13.94%
7	Norway	14.22%
8	Ireland	14.47%
9	The Netherlands	14.55%
10	Slovenia	14.70%



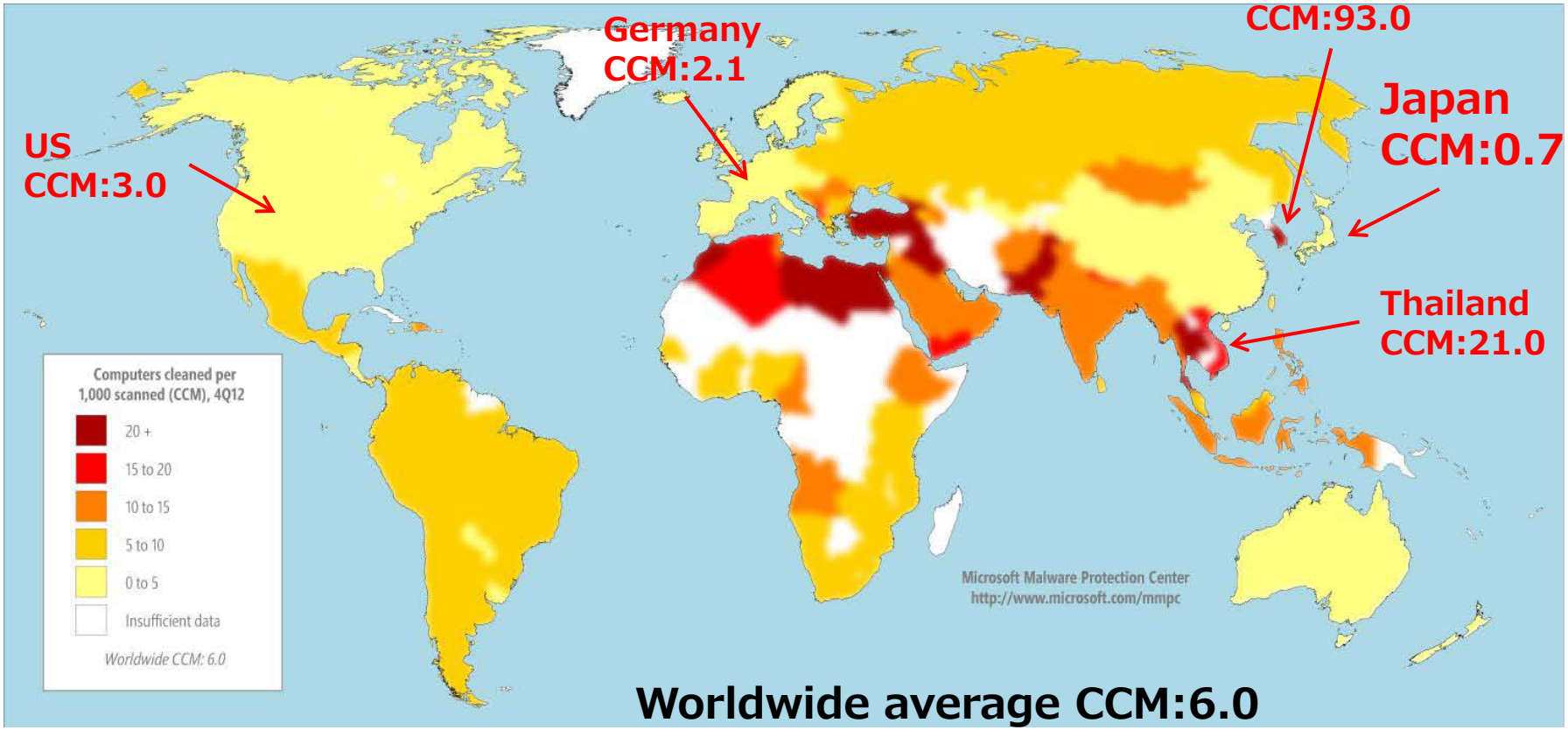
マイクルソフト社のレポートによると…

- **日本におけるマルウェアの感染率は、他国と比較して極端に低い…**

Microsoft Security Intelligence Report Volume 14

Infection rates by country/region in 4Q12 (bottom), by CCM

CCM is the number of computers cleaned for every 1,000 executions of MSRT.



しかし、日本に対する多くの攻撃もみられる…

- **日本には、実際は多くのマルウェアが潜伏しているのではないか？**

Citadel (online banking Trojan**) Makes a Comeback, Targets Japan Users**

<<TrendMicro 2013-09-02>>

http://blog.trendmicro.com/trendlabs-security-intelligence/citadel-makes-a-comeback-targets-japan-users/

Through investigation and collaboration between our researchers and engineers, we discovered a malicious online banking Trojan campaign targeting users in Japan, with the campaign itself ongoing since early June of this year. We've reported about such incidents in the past, including in our Q1 security roundup – and we believe this [illegible] attacks have been expanded

Alert regarding compromised websites

<<< JPCERT/CC Alert 2013-06-07 >>>

https://www.jpcert.or.jp/english/at/2013/at130027.html

JPCERT/CC has been receiving a large number of incident reports regarding compromised websites (
According to the reports, most of th
embedded iframes or obfuscated J
attack site. When a user visits a co
infected by malware.

CERT China claims Japan and US lead in attacks on Chinese internet sites <<<SOPHOS 2013-03-22>>>

http://nakedsecurity.sophos.com/2012/03/22/cert-china-claims-japan-and-us-lead-in-attacks-on-chinese-internet-sites/

The People's Daily Online reported Monday that the number of foreign attacks against Chinese internet infrastructure "remain severe." China's CERT stated that a total of 47,000 foreign IP addresses were involved in attacks against 8.9 million Chinese computers last year.

They claim that **most of these attacks originate from Japan**, the United States and the Republic of Korea (South Korea)

ACTIVE施策の背景

多種多様なマルウェア感染経路が存在

- ネットワーク感染(bot型)
- Web経由の感染
- メール経由の感染
- USB経由の感染　など

マルウェア感染時にはさまざまな脅威が存在

- 不正アクセスインシデント
- 他人のPCを踏み台にしたサイバー攻撃
- フィッシング、SPAMメール
- PCの破壊活動　など

ISP等 ＝ 顧客対応、インシデント対応の観点から**マルウェアの感染率の低下**を実施する必要性がある

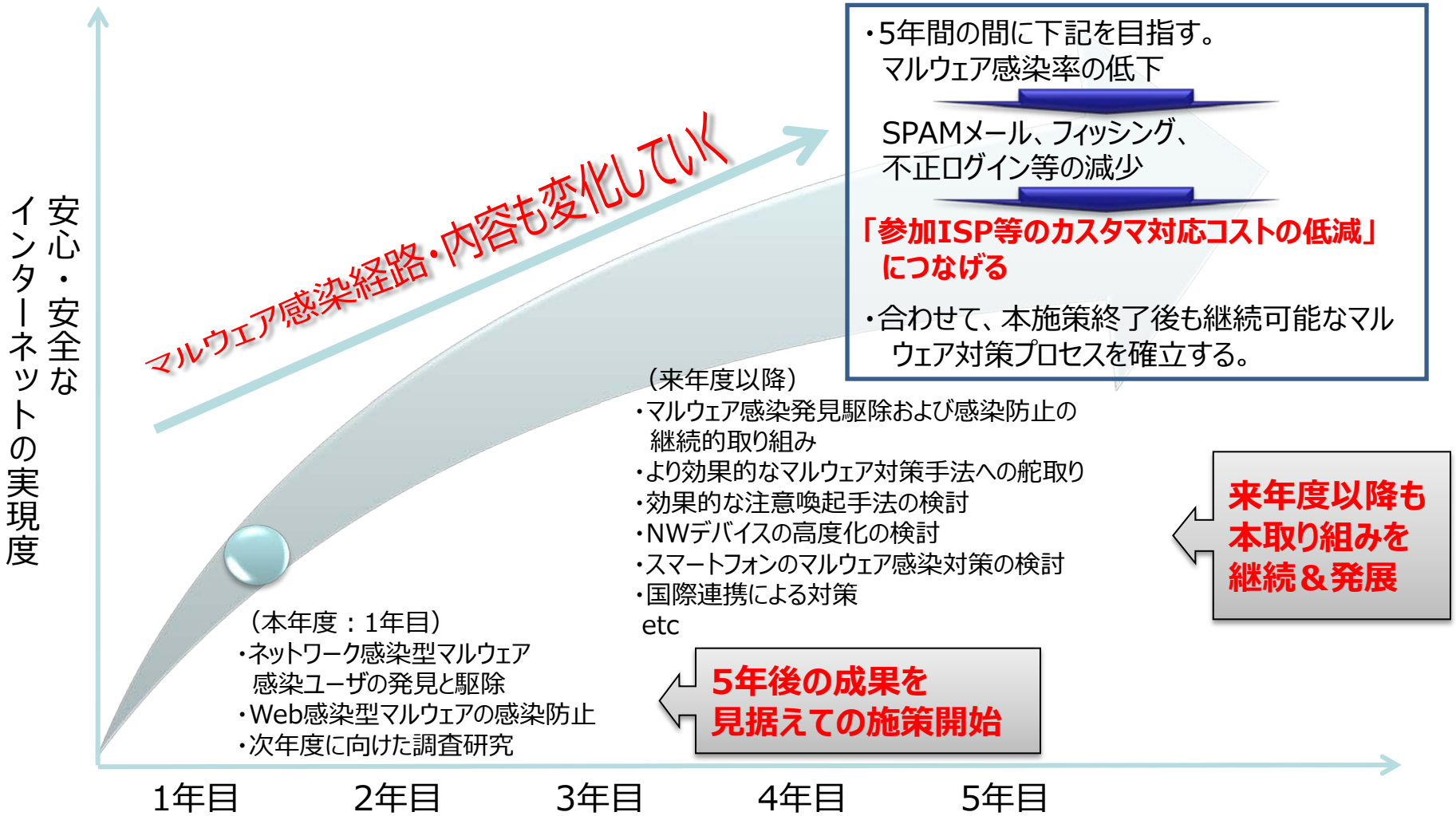
行政 ＝ 安心・安全なインターネットの利用環境の向上、維持の観点から**マルウェアの感染率の低下**が望まれる

サイバーセキュリティ戦略（P.31）　http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf

「ネットワーク型のボットウイルス感染対策として、ＩＳＰの協力を得て実施された官民連携プロジェクトであるＣＣＣでは、一般利用者に注意喚起等を行う取組が行われてきた。今後、マルウェアを配布する等の悪性サイト情報を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする一般利用者に対する注意喚起等を、ＩＳＰ等により実施するための仕組みを構築し、悪性サイトの検知機能の強化などデータベースの機能の高度化を推進する。」

ACTIVE施策の目的

施策の目的： ACTIVE（Advanced Cyber Threats response InitiatiVE）とは総務省の5か年計画実証実験施策であり、マルウェア感染の削減等により安心・安全なインターネットの実現を目指す（2013年11月１日開始）



ACTIVE施策の概要

■ ACTIVE（Advanced Cyber Threats response InitiatiVE）

- ISP等の通信事業者やセキュリティベンダなどが参加
  - マルウェア感染防止やマルウェア駆除に向けた取り組みについて、25の企業や団体が参加（2013年10月11日現在）
- 施策の背景
  - 昨今、マルウェア感染による国家機密の情報窃取など、サイバー攻撃の脅威が増大
  - 悪性サイトの閲覧により感染するなどマルウェアの感染手法が巧妙化し、利用者が自力で検知することが困難

マルウェア感染防止の取り組み

① マルウェア配布サイト等のURL情報をリスト化
② マルウェア配布サイト等にアクセスしようとする利用者に注意喚起
③ マルウェア配布サイト等の管理者に対しても適切な対策を取るように注意喚起

マルウェア駆除の取り組み

① マルウェアに感染した利用者のPCを特定
② 利用者に適切な対策を取るように注意喚起
③ 注意喚起の内容に従い、PCからマルウェアを駆除

6）APTによる攻撃の対策（JASAによる活動例)

境界でのAPT対策の限界

境界での対策	対策の目的	対策の限界
標的型メール対策（イノキュレーション）	標的型メールを開く人の割合を減らす	一人でも標的型メールを開いたら侵入される
出口対策	情報を持ち出す際の異常な通信を検知し、遮断する	正常な通信に偽装される、又は、対策機器を回避した通信を確立されると検知できない

運用管理者の悩み

クライアントが信用できない

数千台のPCの中で、乗っ取られた（かもしれない）1台をどのように発見するのか？

監視対象が特定できない

日々業務に使われている組織内部のシステムの、どの部分を監視すればよいか？

ポリシーが不明確だ

機器などが挙げてきたアラート情報などのうち、何を、どの観点で見ればよいか？

・・・・など

対策の基本

自らの「不健康（不調）」を検知する

そのために、日頃の「健康である状態」を把握しておく

不調を感じたら素人判断はせず、早めに専門家に相談する
同時に、インシデントハンドリングの態勢に入る

検知のための確認ポイント

潜伏：標的内部のPCに入り込む

対象	ポイント
従業員	変なメールや、送られてきたCDやUSBを開いてしまったという報告等。
	実行すると変なエラーやPCが再起動するようなファイルを開いてしまったという報告。
	PCが不調になった(再起動を繰り返す)という報告等。
POP/IMAPログ	怪しい添付ファイルの読み込み（たとえば、.exeとか、未知の拡張子とか・・）
PC再起動の検知	L2で同じセグメントにあれば、再起動時に発生するArp広告（ブロードキャスト）を見つけられる可能性がある。
イントラサイトログ	refererに不審なサイトURLが書かれているなど
ウイルス検知ログ	Loaderなどリスクは低いものの、影響が大きいウイルスが検知されたPCの現認と、感染経路の把握
	リアルタイムスキャンで検知されず、定期スキャンでウイルスが検知されたPCの現認と、感染経路の把握
	複数のPCで同種のウイルスが検知された場合のPCの現認と、感染経路の把握

橋頭堡：標的内部のPCの支配

対象	ポイント
ウイルス検知ログ	リアルタイムスキャンで検知されず、定期スキャンでウイルスが検知されたPCの現認と、感染経路の把握
	複数のPCで同種のウイルスが検知された場合のPCの現認と、感染経路の把握
プロキシ通信ログ	特定のホストとの通信数が多いPCの把握（C&Cサーバとの通信を補足することを目的とする）
	夜間にも関わらず特定のホストと通信しているPCの把握(C&Cサーバとの通信を補足することを目的とする）
	送受信の「総量」と「回数」が多いPCの把握(C&Cサーバとの通信を補足することを目的とする）
	DynamicDNSと通信しているPCの把握（C&Cサーバとの通信を補足することを目的とする）
	海外サーバへのpostメソッドの多いPCの把握(C&Cサーバとの通信を補足することを目的とする）
PC現認	異変のあるPCのタスクスケジューラの確認（ウイルス動作を確認する。ファイルパスに注目）
	異変のあるPCのスタートアップの確認(ウイルス動作を確認する。ファイルパスに注目）

検知のための確認ポイント

索敵：対象NW情報の収探索

対象	ポイント
サーバセキュリティログ	anonymousによる隠し共有へのアクセスの把握(Windows) ※
サーバセキュリティログ	ログイン試行の把握 ※
サーバログ	ポートスキャンによる、syslogのconnection from bad portログの把握(Unix/Linux)

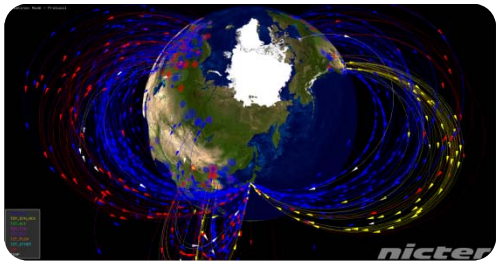
浸透：対象NW内の踏み台を増殖

対象	ポイント
従業員	PCが不調になった(再起動を繰り返す)という報告等。
ウイルス検知ログ	複数のPCで同種のウイルスが検知された場合のPCの現認と、感染経路の把握
プロキシ通信ログ	特定のホストとの通信数が多いPCの把握(C&Cサーバとの通信を補足することを目的とする)
プロキシ通信ログ	夜間にも関わらず特定のホストと通信しているPCの把握(C&Cサーバとの通信を補足することを目的とする)
プロキシ通信ログ	送受信の「総量」と「回数」が多いPCの把握(C&Cサーバとの通信を補足することを目的とする)
プロキシ通信ログ	DynamicDNSと通信しているPCの把握(C&Cサーバとの通信を補足することを目的とする)
プロキシ通信ログ	海外サーバへのpostメソッドの多いPCの把握(C&Cサーバとの通信を補足することを目的とする)
プロキシ通信ログ	複数のPCから同一のホストに対してアクセスをしている先の把握(C&Cサーバとの通信を補足することを目的とする)
PC現認	異変のあるPCのタスクスケジューラの確認(ウイルス動作を確認する。ファイルパスに注目)
PC現認	異変のあるPCのスタートアップの確認(ウイルス動作を確認する。ファイルパスに注目)

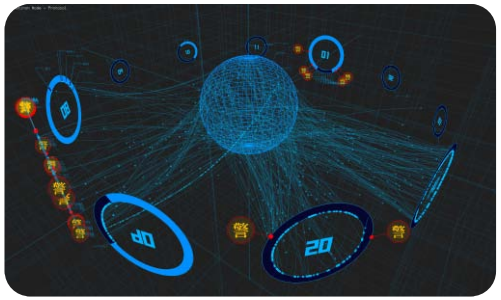
7）NICTにおける研究活動（対策への活用）

nicterとそのスピンオフ技術たち

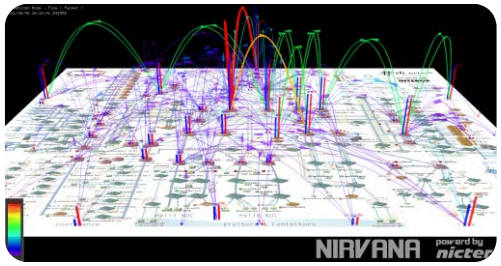
1. インシデント分析センター
   nicter



2. 対サイバー攻撃ラートシステム
   DAEDALUS



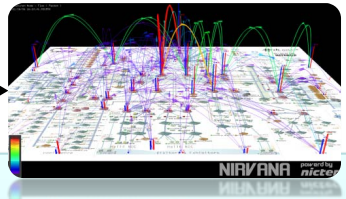
3. ネットワークリアルタイム可視化システム
   NIRVANA



鳥の目/虫の目

nicter

DAEDALUS



NIRVANA

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）

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

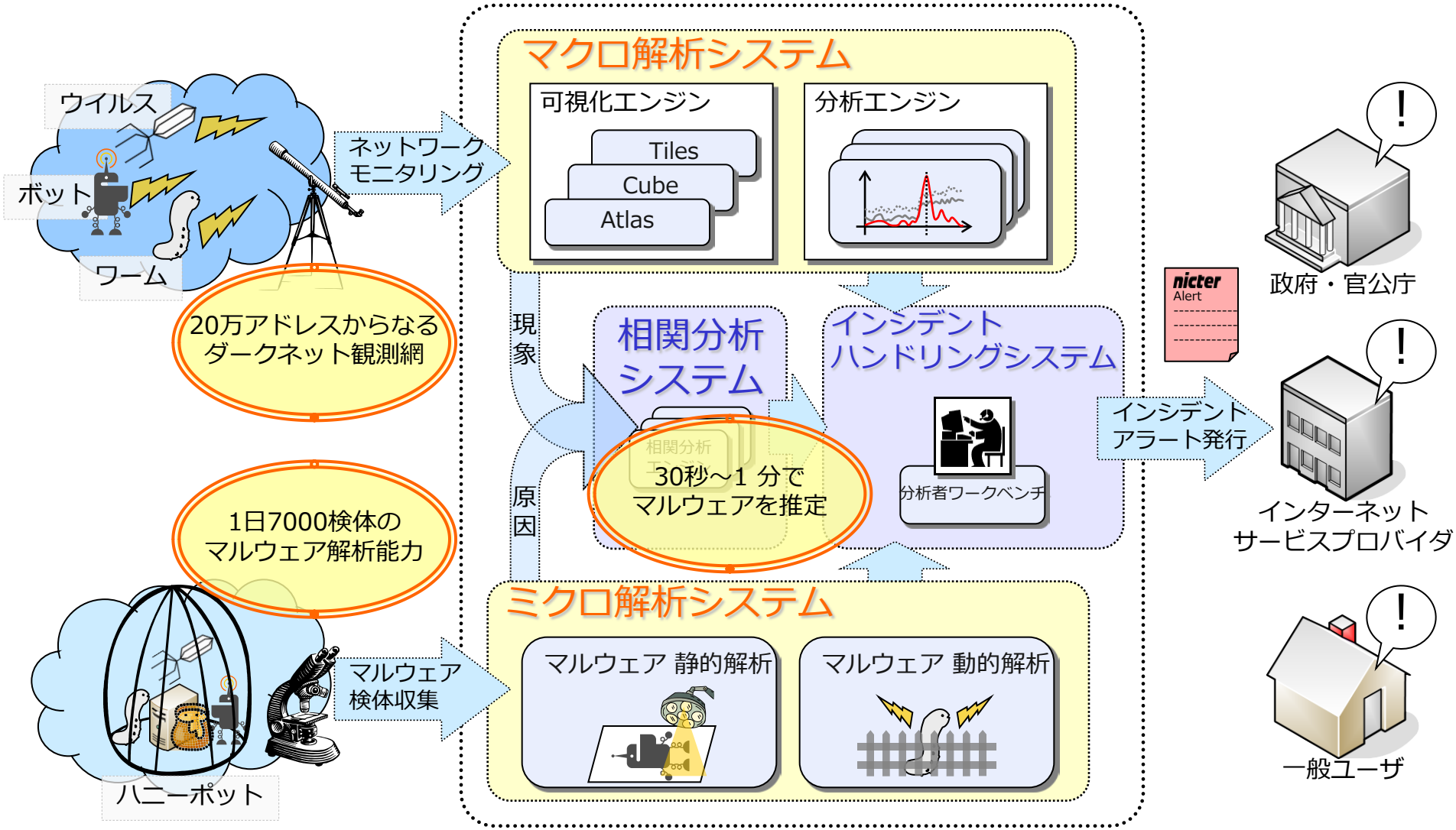
目的:

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。

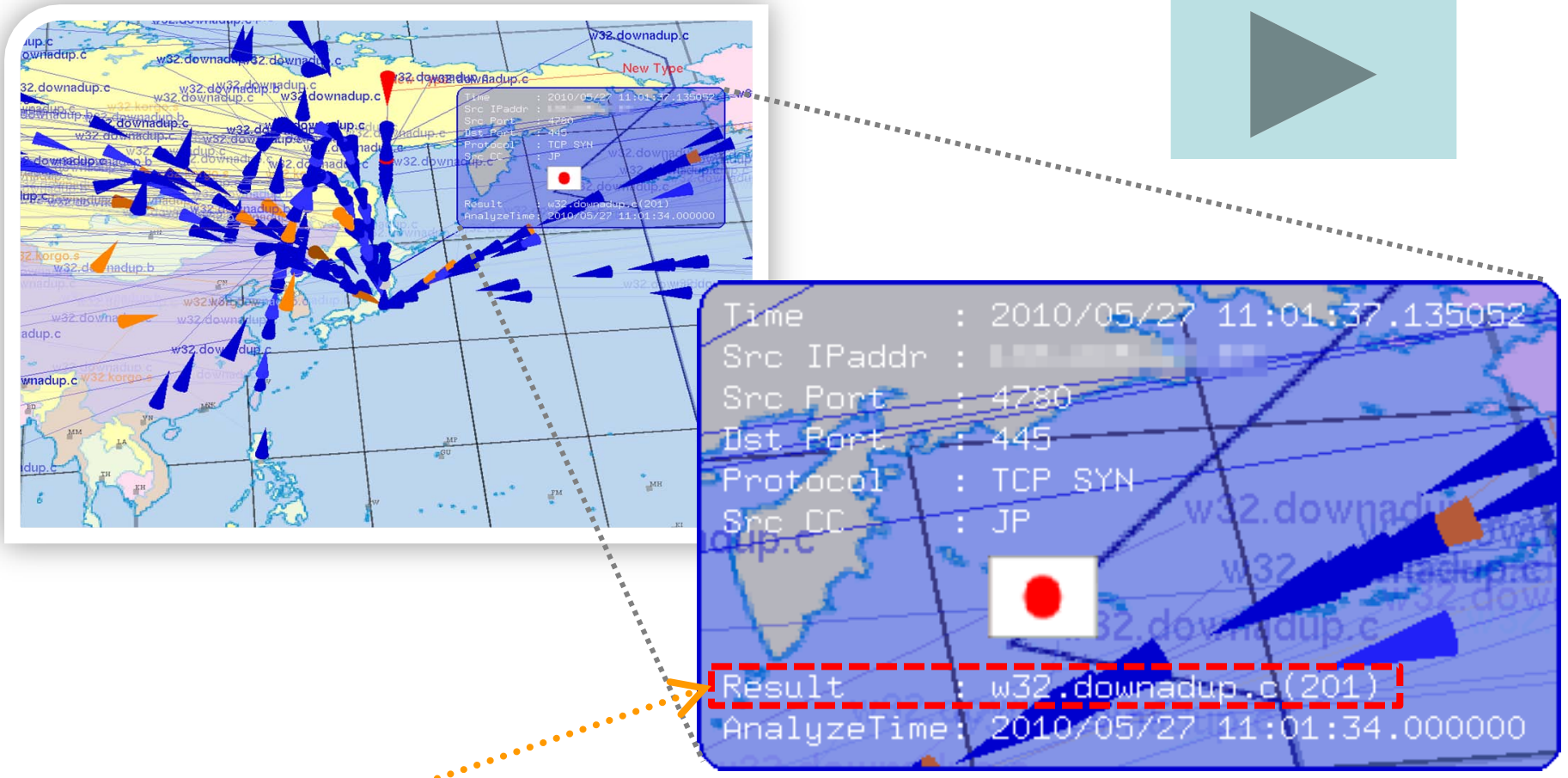
主要コンポーネント

- 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

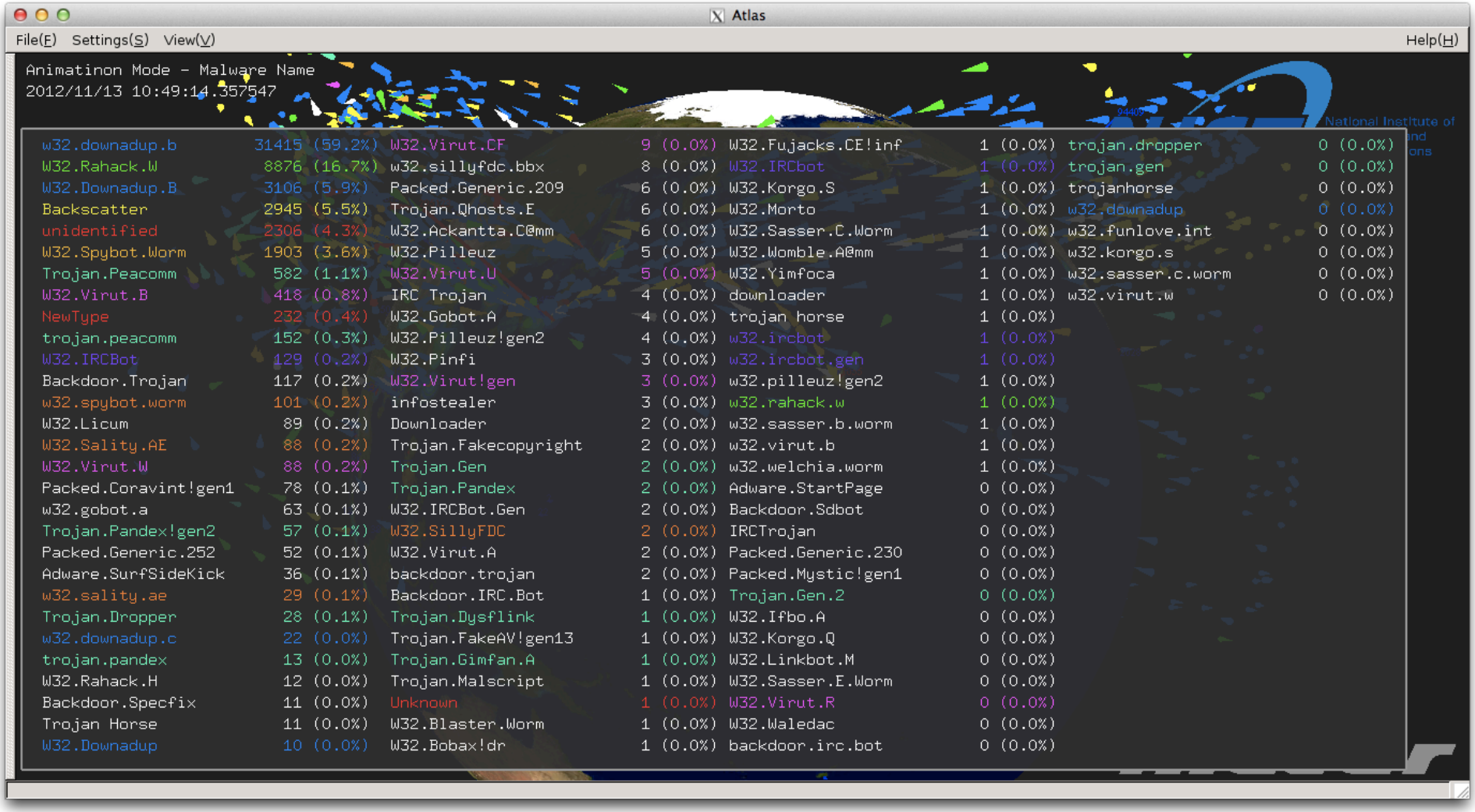

マクロ解析システム
可視化エンジン
Tiles
Cube
Atlas
分析エンジン
ウイルス
ボット
ワーム
ネットワーク
モニタリング
20万アドレスからなる
ダークネット観測網
現象
原因
相関分析
システム
相関分析
30秒～1 分で
マルウェアを推定
インシデント
ハンドリングシステム
分析者ワークベンチ
nicter
Alert
インシデント
アラート発行
政府・官公庁
インターネット
サービスプロバイダ
一般ユーザ
1日7000検体の
マルウェア解析能力
ハニーポット
マルウェア
検体収集
ミクロ解析システム
マルウェア 静的解析
マルウェア 動的解析

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**

相関分析結果のリアルタイム可視化 (2/2)



最新開発の新警報システム

DAEDALUS:
Darknet based “new alert system”

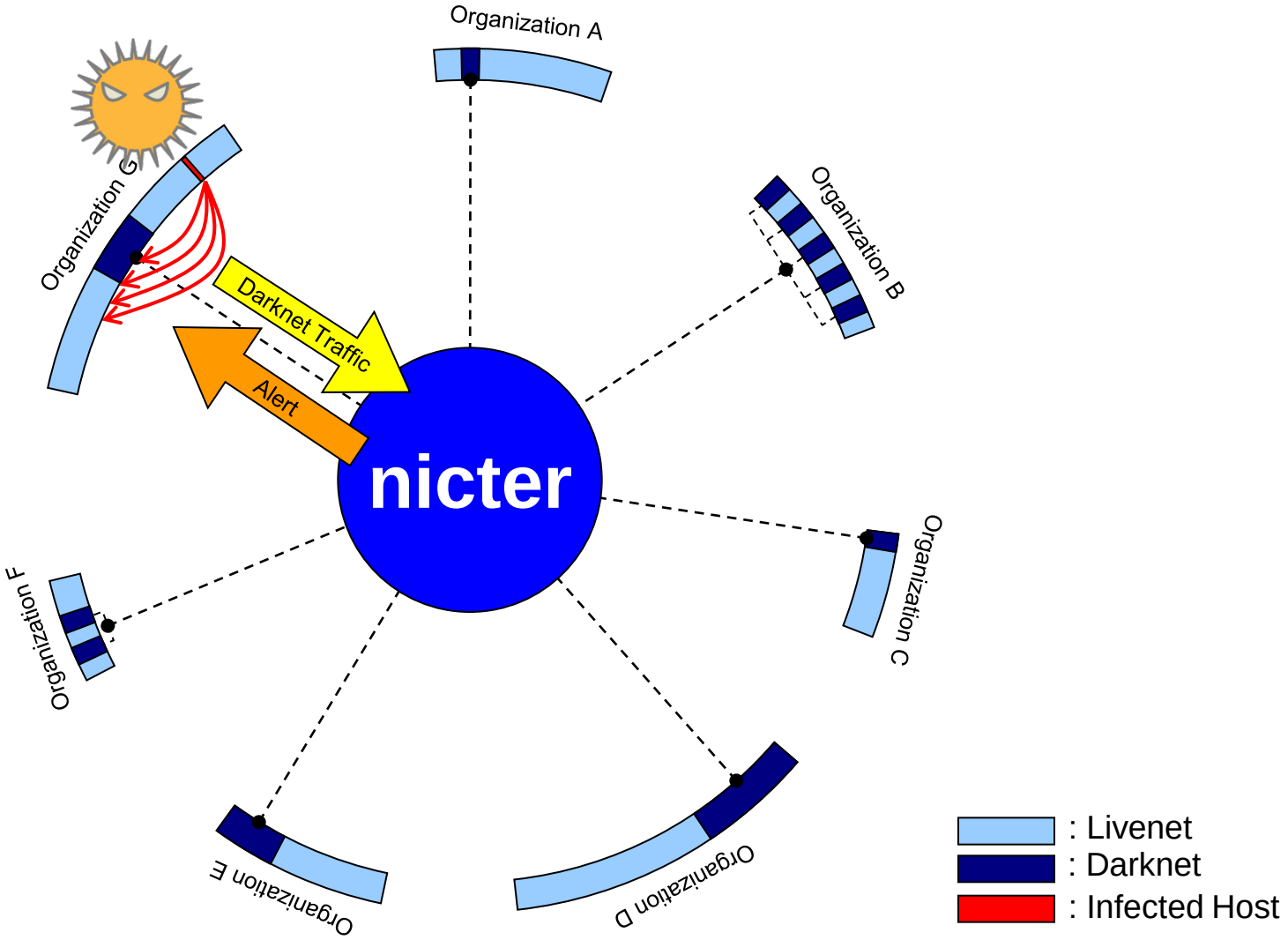
(**D**irect **A**lert **E**nvironment for **D**arknet **A**nd **L**ivenet **U**nified **S**ecurity)

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。

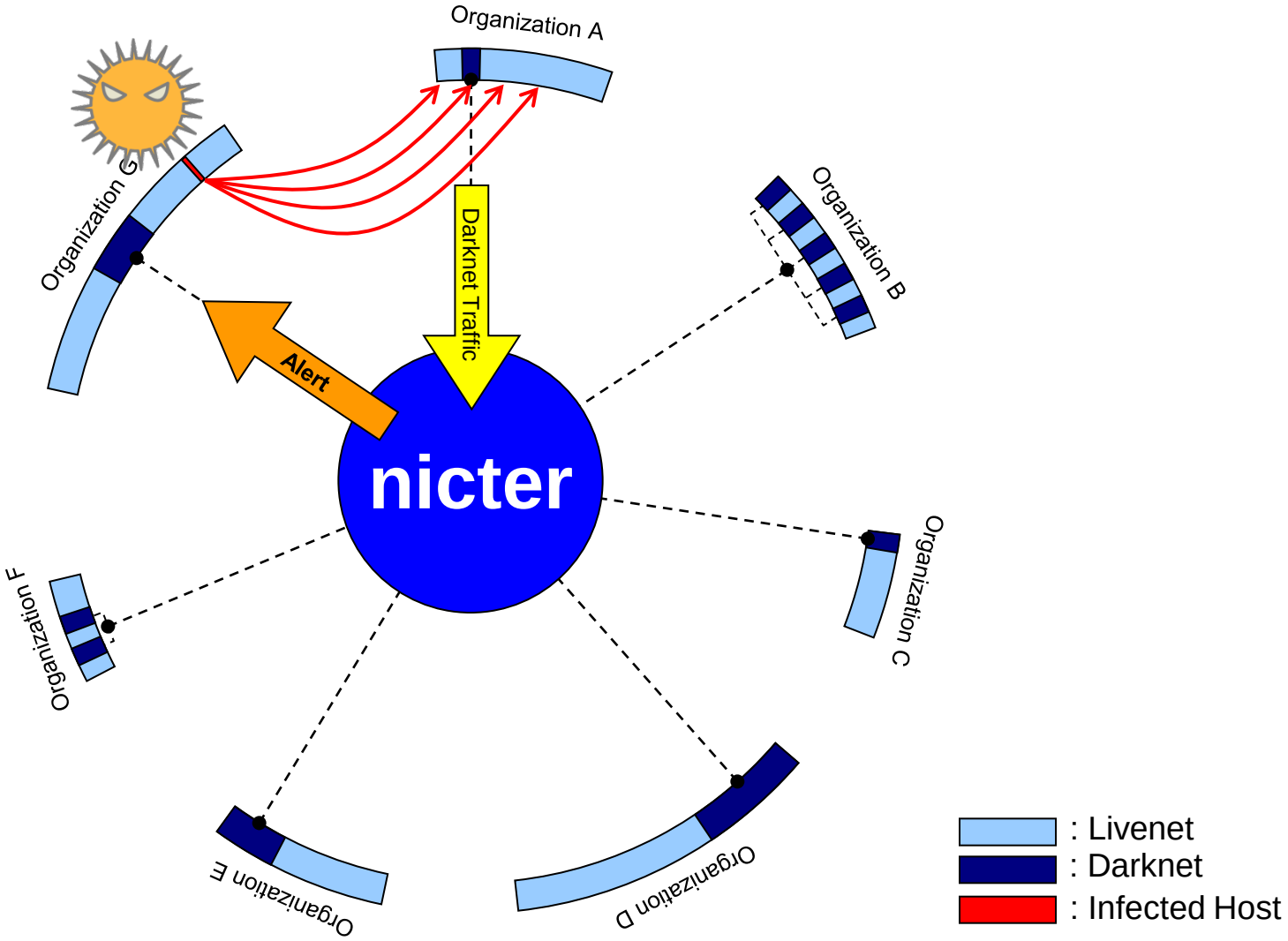
ケース1

組織内感染（内部アラート）

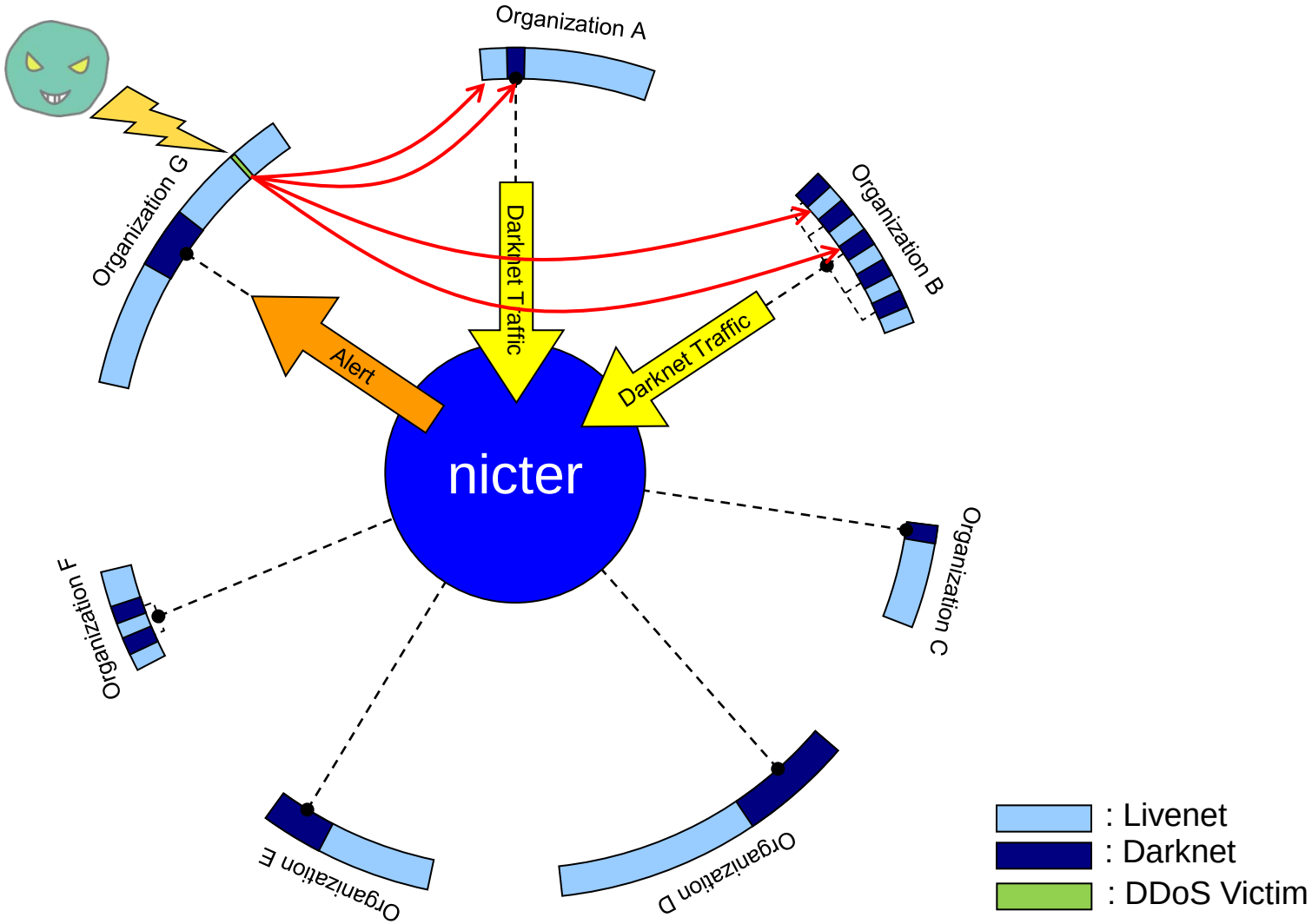


ケース2

組織外への攻撃（外部アラート）

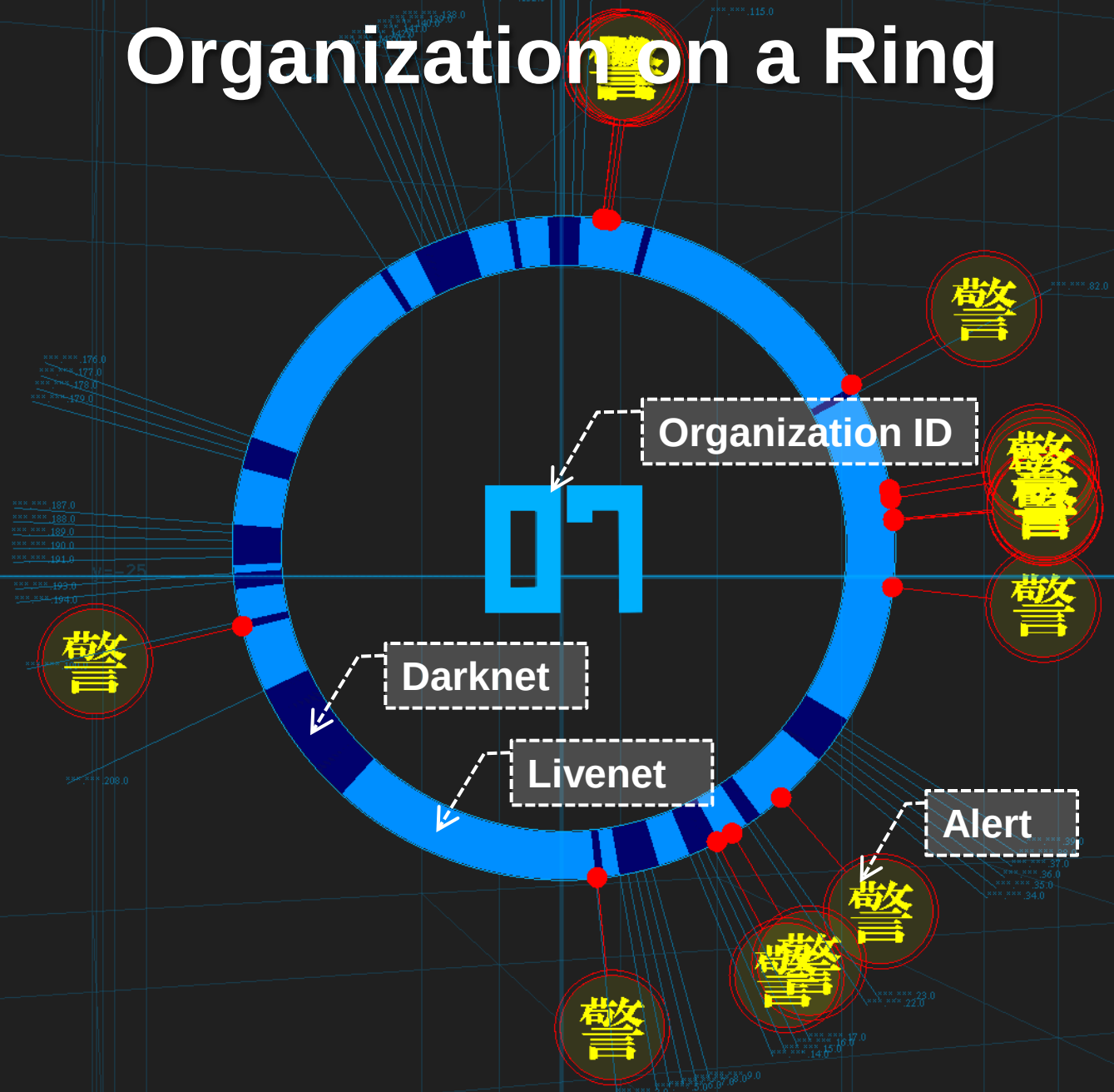


DDoS攻撃の跳ね返り（バックスキャッタ）




DAEDALUS-VIZ
(DAEDALUS可視化エンジン)

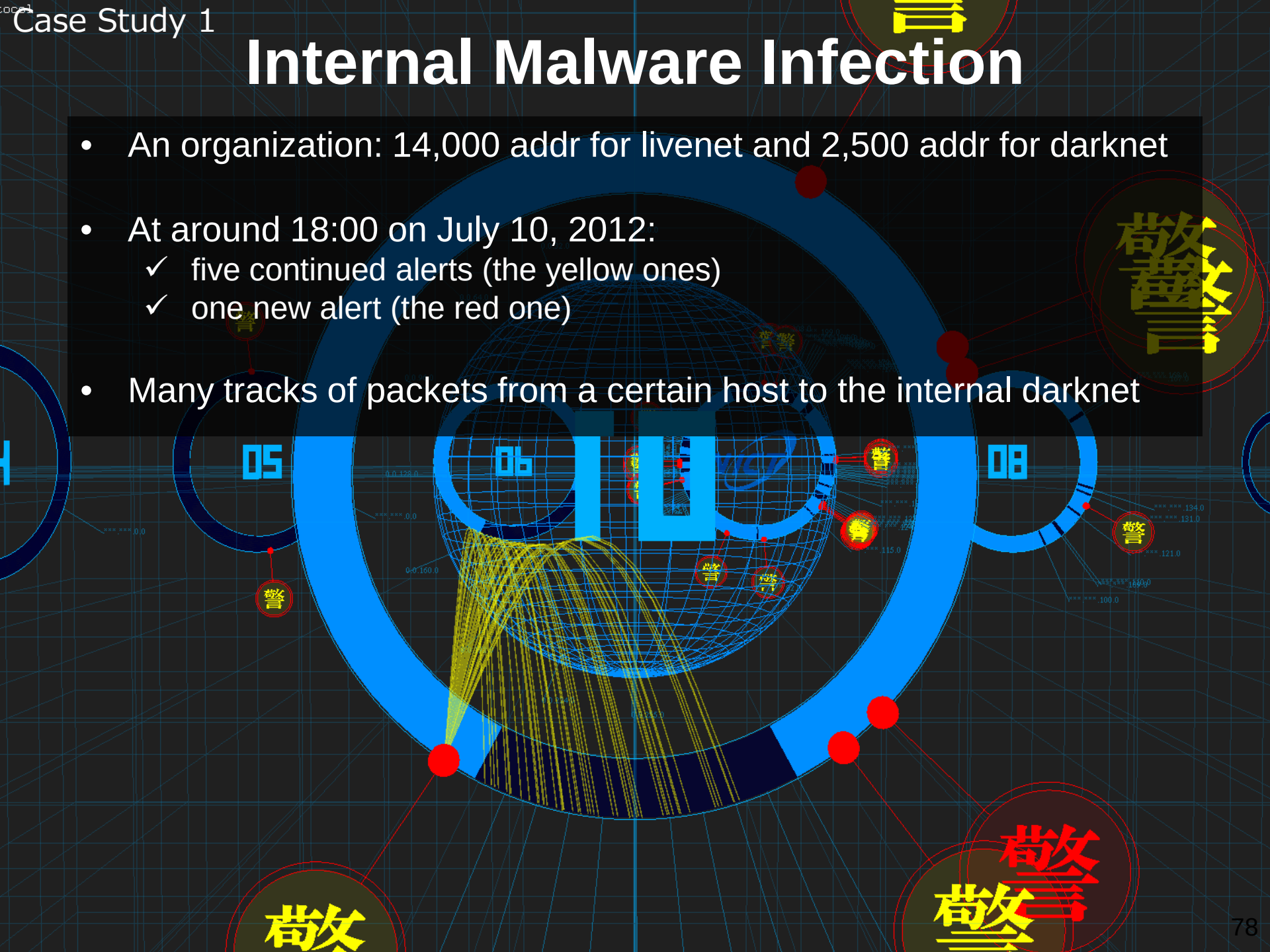
Organization on a Ring



New Alert

Internal Malware Infection

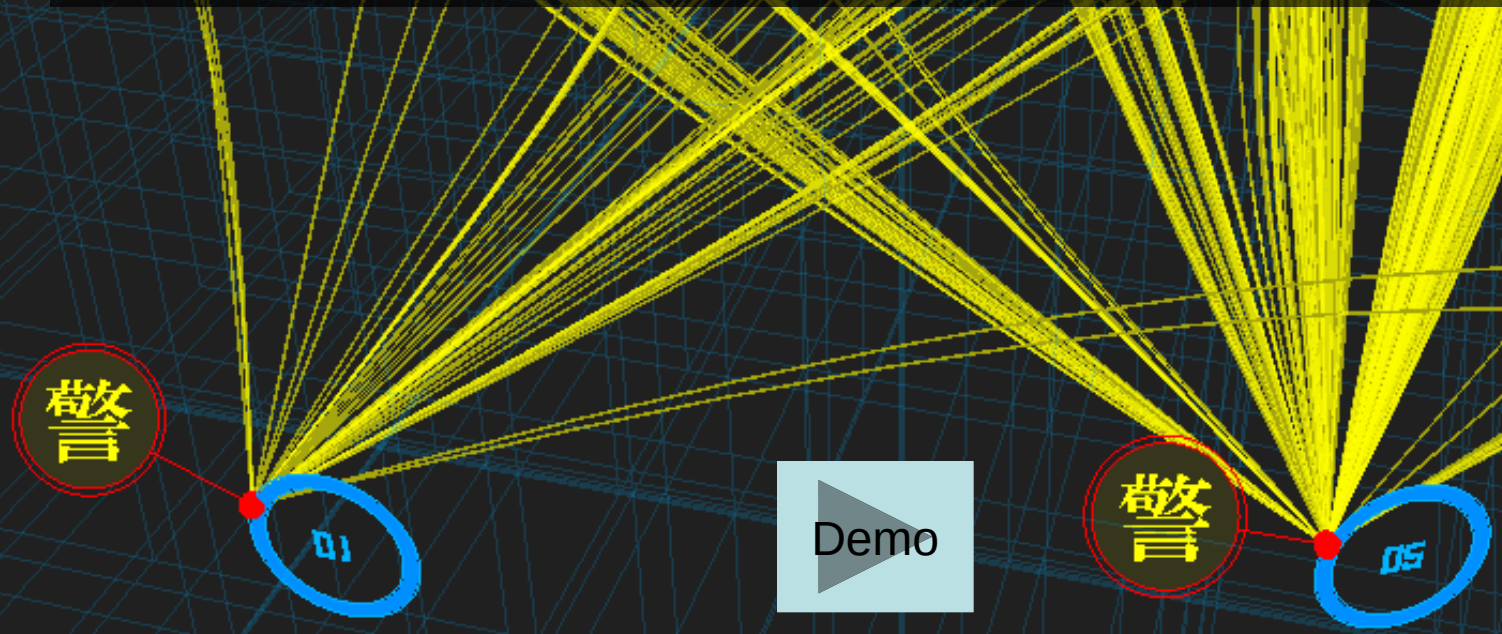
- An organization: 14,000 addr for livenet and 2,500 addr for darknet
- At around 18:00 on July 10, 2012:
  - ✓ five continued alerts (the yellow ones)
  - ✓ one new alert (the red one)
- Many tracks of packets from a certain host to the internal darknet



DDoS Backscatter

Promotion Video?

- On June 16, 2012:
  - ✓ Anonymous announced that they had initiated OperationJapan against the Anti-Counterfeiting Trade Agreement (ACTA).
- From June 26 to 30:
  - ✓ the Web site of the Democratic Party Japan (DPJ) was under a DDoS attack by Anonymous.
  - ✓ the backscatter were distributed to many organizations, which is a typical behavior reflective of a DDoS attack with random IP spoofing



Demo

ネットワークリアルタイム可視化システム

NIRVANA

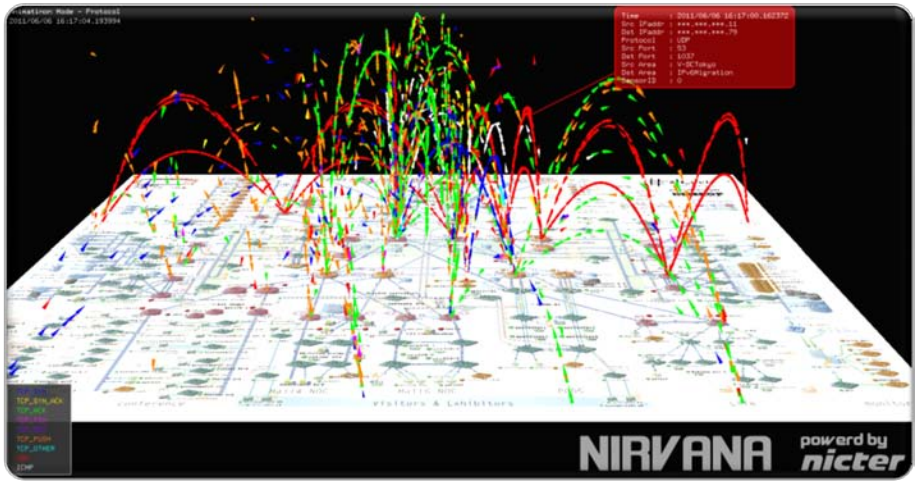
(**n**icter **r**eal-network **v**isual **ana**lyzer)

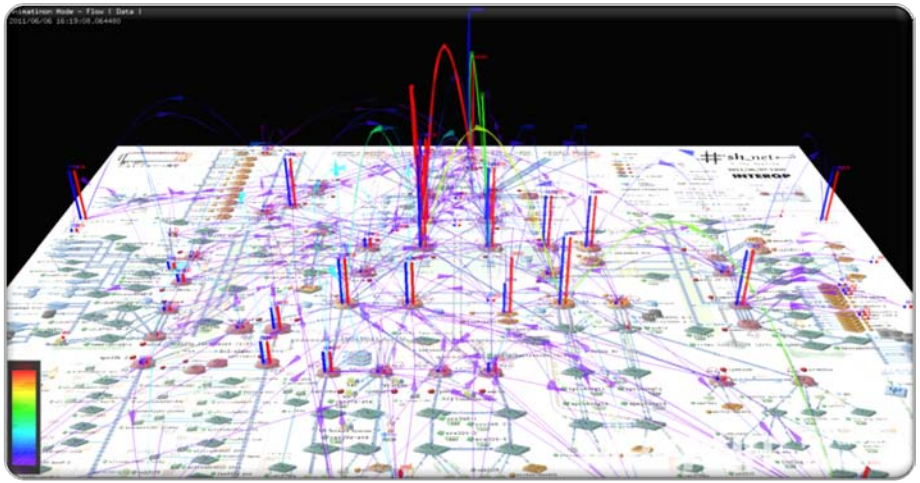
NIRVANA：目的

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）

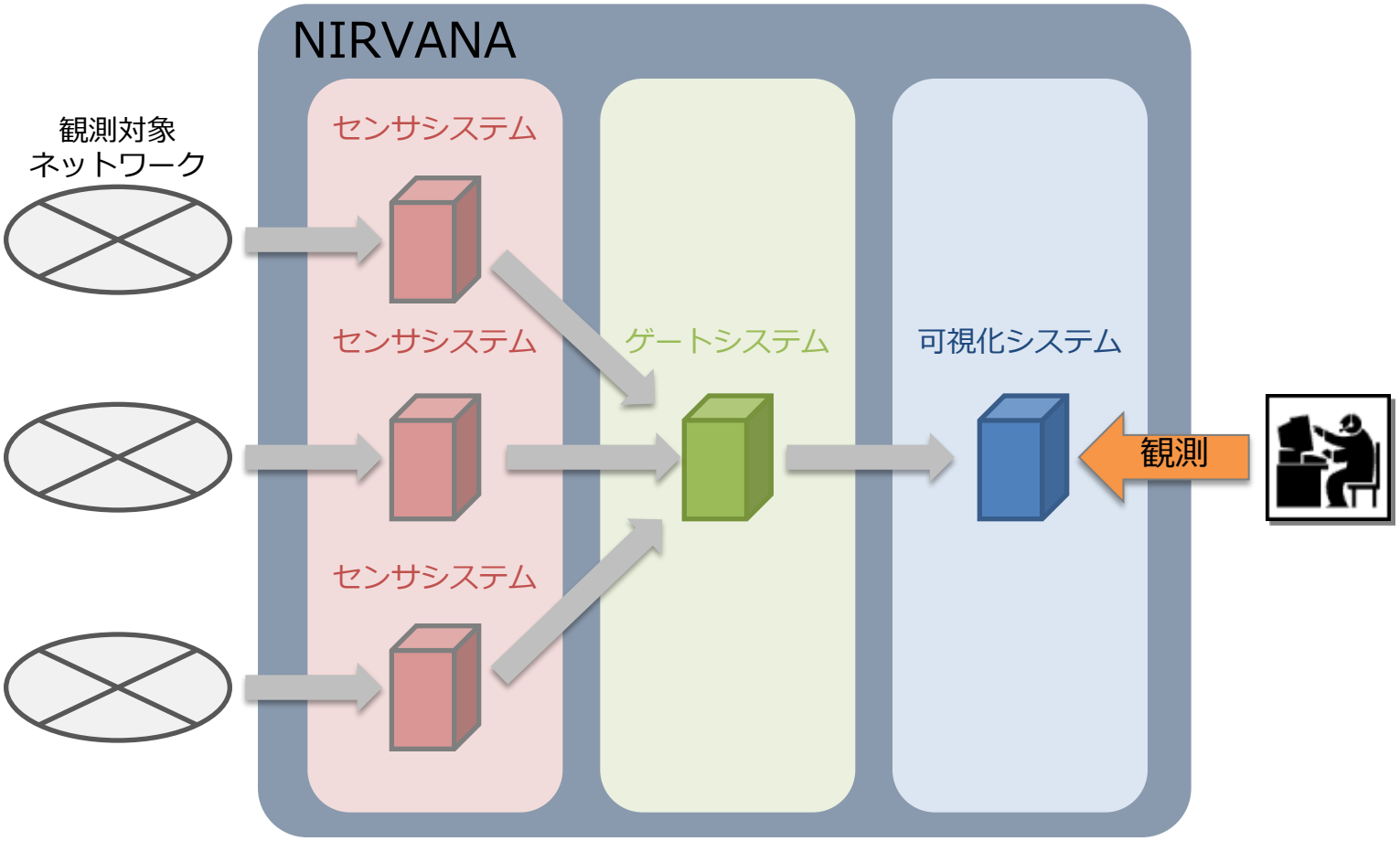
管理コストの軽減
（管理の迅速化・効率化）





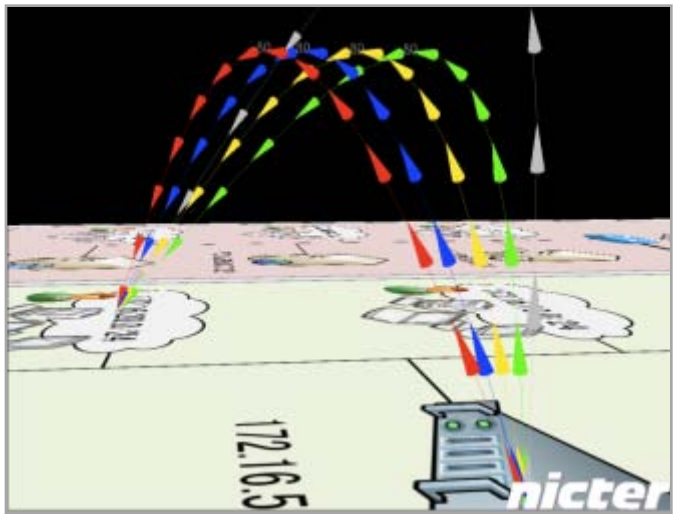
NIRVANA：システム構成

- 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。

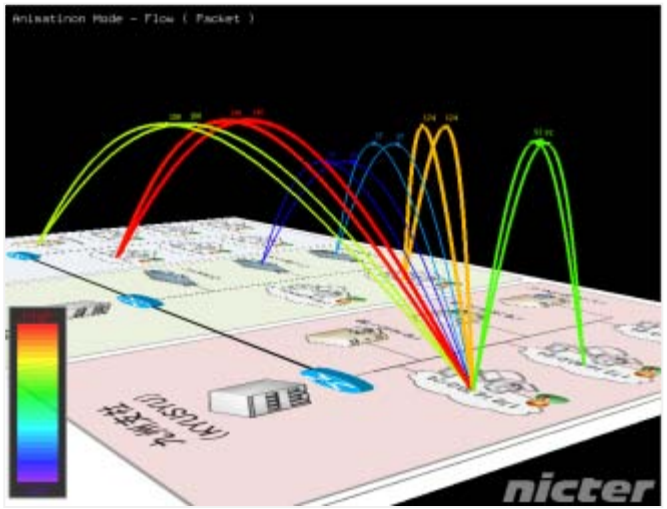


NIRVANA：トラフィック表示方法

- 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。



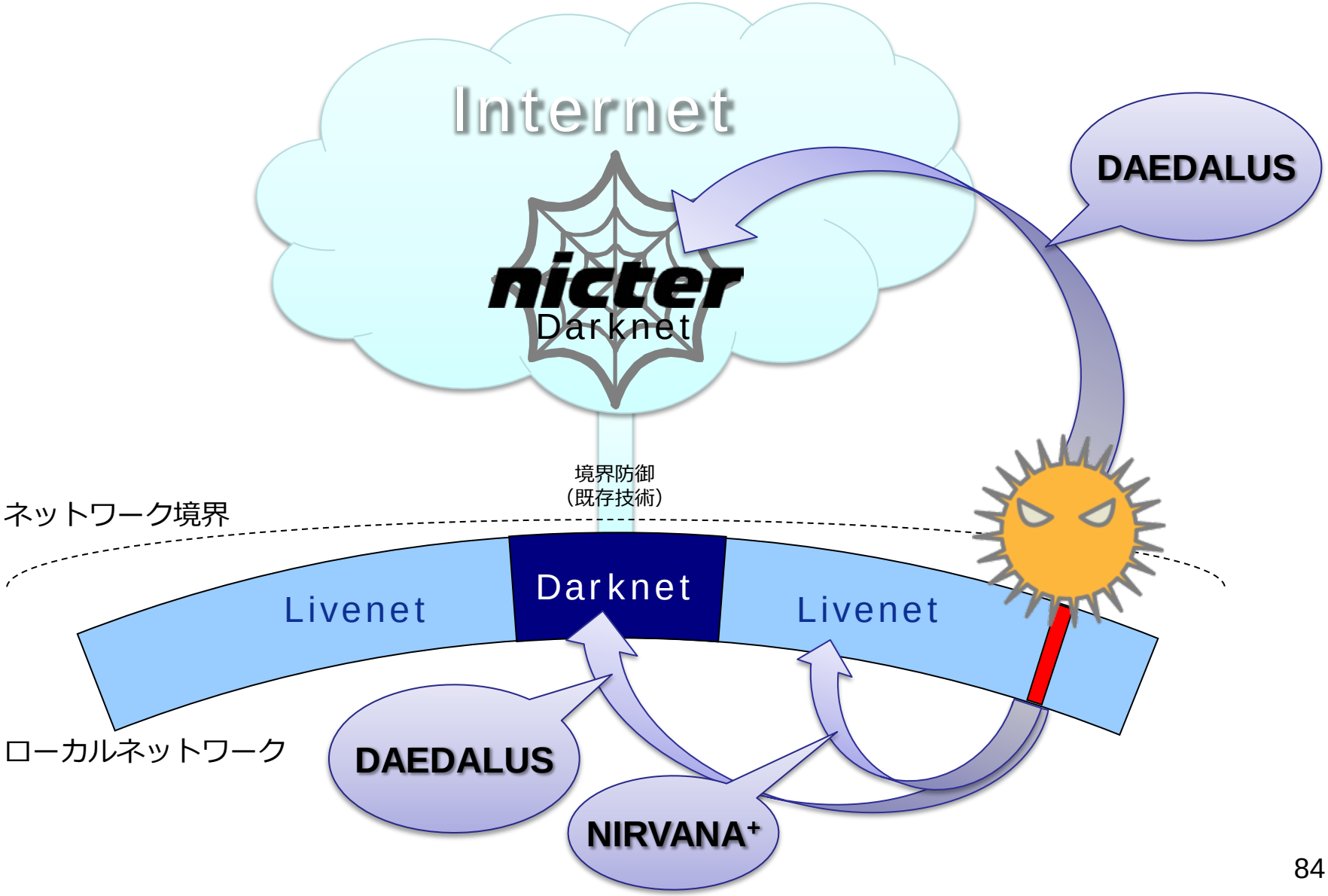
- フローモード
  - ✓ リボン状のフローの高低や色温度でトラフィック量を表現。
  - ✓ 大量のトラフィックを処理可能。



Demo

今後のNICTにおける研究・技術開発の方向性

nicter + DAEDALUS + NIRVANA+ による多層防御



NICT研究活動のまとめ

- 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）

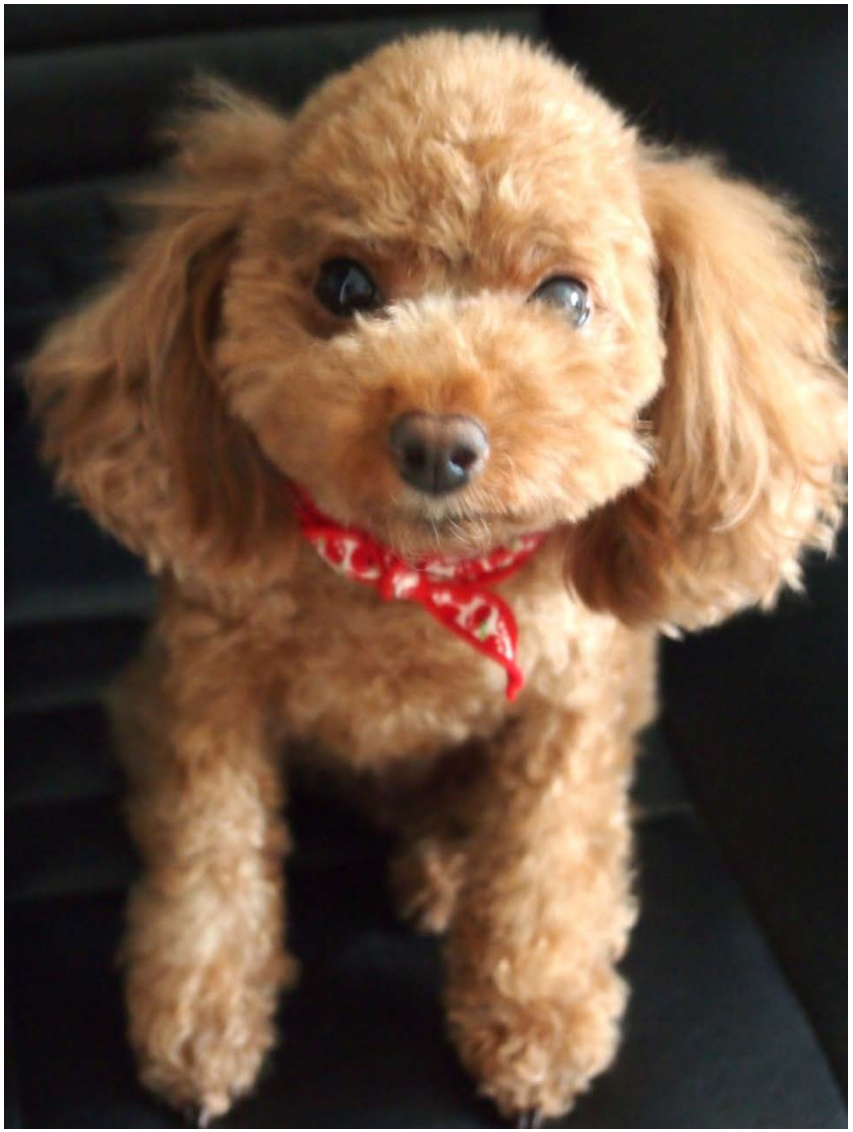
||

サイバーセキュリティの新たな地平

サイバー攻撃対策総合研究センター：APTなどの新種攻撃にも解析・対策

まとめ

- 脅威の根源にある「マルウェア」
  - ✓ 愉快犯、自己顕示目的 → 金銭目的、またはサイバーテロ
  - ✓ 小規模 → 大規模分散協調
  - ✓ 脅威の多様化、隠蔽化、深刻化（重要インフラなど）APTによる攻撃等
- 情報セキュリティ対策の強化、及び広域連携
  - ✓ 通信事業者としては、顧客の安心安全に向けたセキュリティ対策（spam対策、DoS対策、Web改ざん検知、侵入検知など）の施策を導入実施が重要
  - ✓ 対策の有効化としても大規模対応が不可欠、Telecom-ISAC、セプターカウンシル（重要インフラ）連携、国際関連機関などとの連携が要
  - ✓ 攻撃者と同等なスキルを持ち、国際規模の対策防御連携体制を組むことにより、より早い時点で攻撃を食い止めること（早期発見・対策）が重要
  - ✓ サイバーセキュリティ研究は、実践研究。多くの事象の共有、関連事業者との連携がその成功のカギ。（大学だけの研究ではデータ不足）関連事象の連携性分析技術（拡張的SIEMの概念）が本質となると考える
  - ✓ 暗号関連技術の適切な活用も鍵。学術面だけでなく、実装面、運用面の強化が重要（マルウェアも暗号を活用する時代）



ご静聴ありがとうございました