企業や政府関係組織への最新攻撃動向

～ Anonymousなどによる最近の攻撃について ～

株式会社インターネットイニシアティブ
セキュリティ情報統括室

根岸 征史

今年度前半の主要トピック

- Anonymous, LulzSecなどによる Hacktivismの台頭
- 国内外におけるサイバースパイ活動
- CAへの侵入、偽証明書発行

実際のところ、どの程度の脅威なのか?

攻撃動向の変化

2011

1	2	3	4	5	6	7	8	9	10	11	12

LulzSec以前

“アラブの春”支援

政治的主張が強い

HBGary事件

LulzSec登場

企業、メディア、政府などを攻撃

世間の注目を集め、活動範囲の枠も拡げる

LulzSec以後、AntiSec開始

多数のハッカーが参加

主に政府関係組織を攻撃

混沌、まとまりのなさ

ネットからリアルへ

OpBART, OWSなどのデモ活動に注力

多数のAnon逮捕

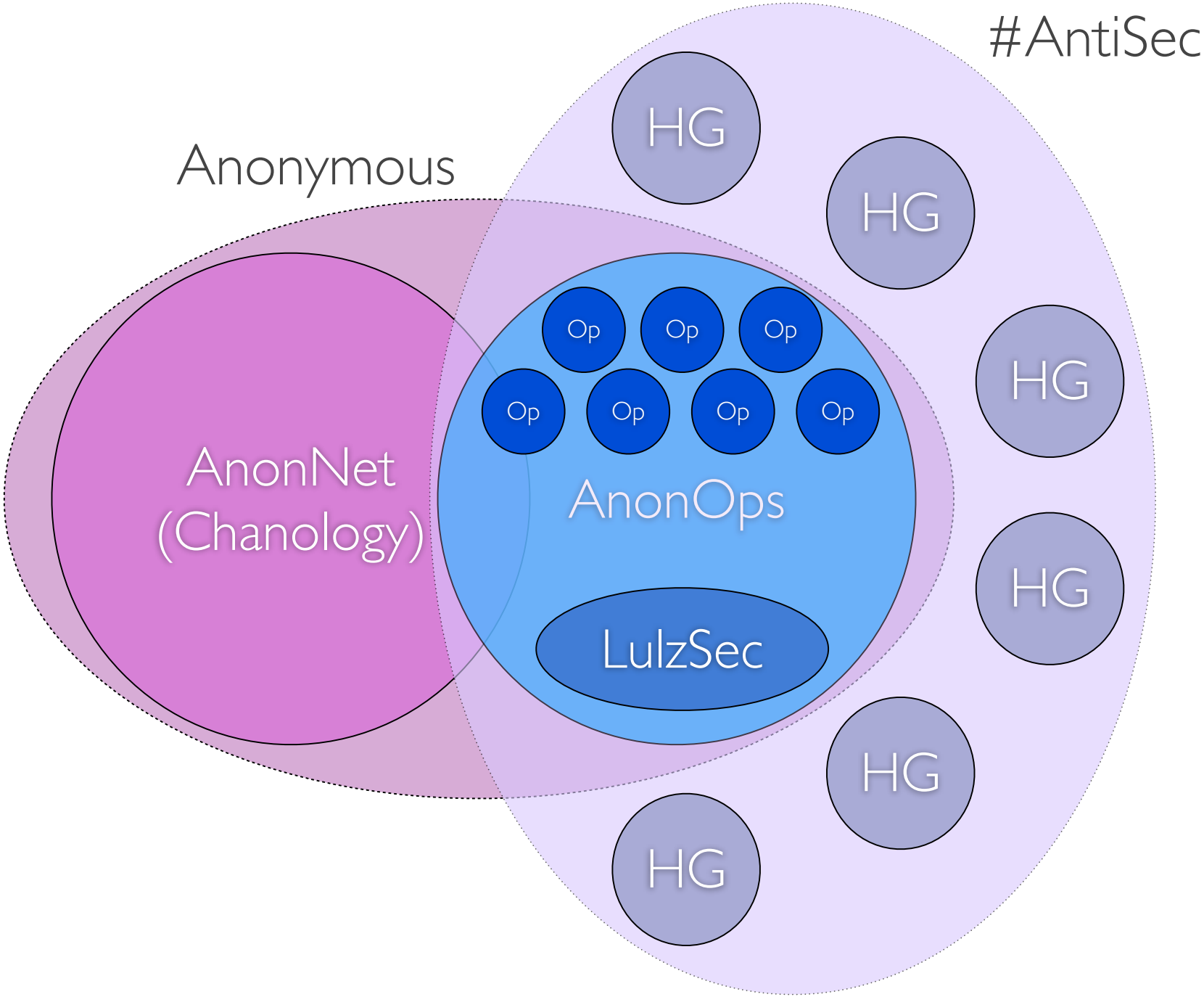
攻撃の特徴

攻撃主体

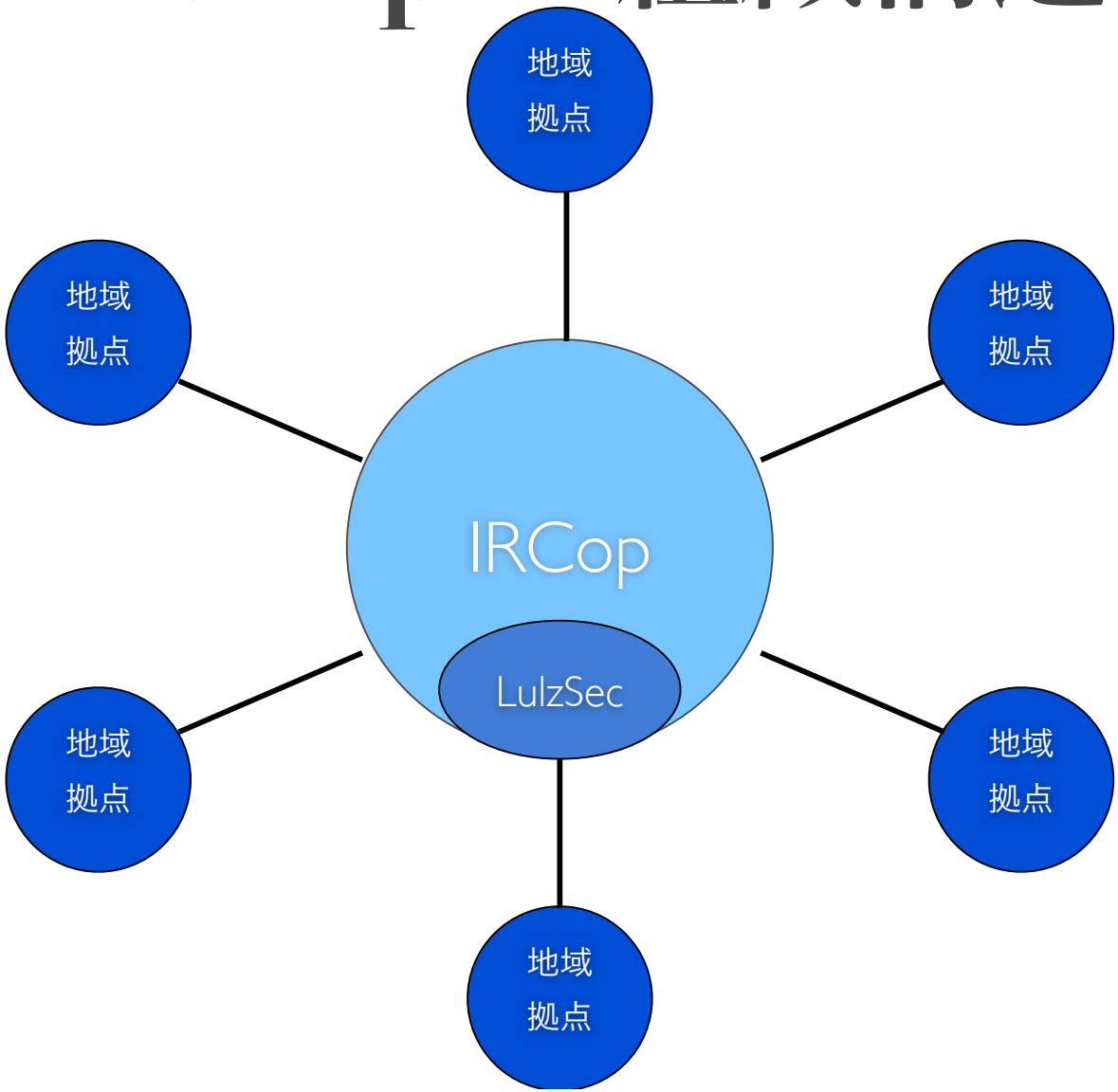
* Anonymousは「国際的ハッカー集団」なのか?
* Hacktivist? Activist?
* 内部抗争、分裂、裏切り、内部情報暴露

「メディアの思い込みとは違い、アノニマスとは単なるハッカーのグループの事ではありません。我々アノニマスは、正しいことをしなければいけない、暗闇に光をもたらさなければいけない、そして長い間眠ってきた大衆の目を開かなければいけない、という認識を持った個人の集団です。我々の中には、弁護士、親、ＩＴ専門家、警察職員、大学生、獣医など、あらゆる職業や年代の人々がいます。アノニマスとは全ての人です。そして我々はどこにでもいます。我々にはリーダーはおろか全体を指揮する者などいません。我々個人の激しい怒りのみが我々の行動を指揮しているのです。」 http://www.youtube.com/watch?v=CTdtoRM0CyQ

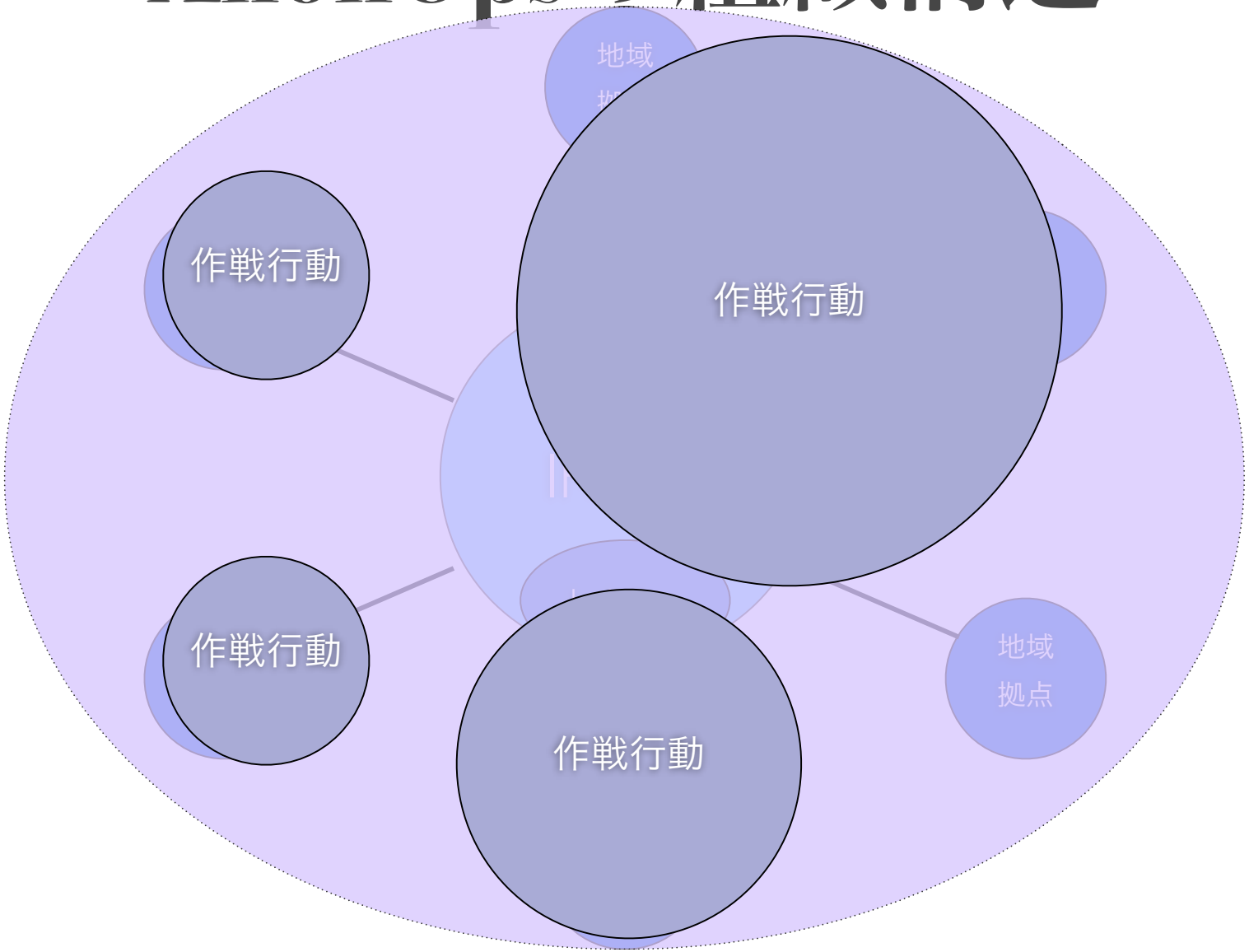
「私たちはアノニマスです。私たちの中には、弁護士、親、ＩＴ専門家、警察職員、大学生、獣医など、あらゆる 職業や年代の人々がいます。「アノニマス」とは日本語で「名無し」と言う意味です。私たちのメンバーは名前 も、顔も隠しているので、この名前を使っているのです。 なぜ私たちがそうするのか疑問に思う方がいらっしゃるかもしれません。なぜならばその理由はまず最初に、「 アノニマス」として２ｃｈのようなシステムを使っているからです。実名を使わないので、自由に話すことができるからです。話す人より、話そのものの方が大切になるからです。次の理由は、私たちの安全のために名前も、顔も隠すことができるからです。坂本堤さんのように消えたく（消 されたく）ありません。サイエントロジーの拡大を停止することができるまで、アイデンティティを守り通したいからです。 あなたもアノニマスになることができます。名前を公開する必要はありません。出来得るならば他の人にサイエントロジーの危険性を告知して欲しいと衷心より願っております。」 http://anonymousjapan.blogspot.com/


#AntiSec
Anonymous
HG
HG
HG
HG
HG
HG
Op
Op
Op
Op
Op
Op
Op
AnonNet
(Chanology)
AnonOps
LulzSec

AnonOpsの組織構造



AnonOpsの組織構造



ターゲット

- 政府系サイトへの攻撃

  #AntiSec, #OpBrazil, #OpSyria,...

- 特定企業への攻撃

  #OpSony, #OpGreenRights, #OpBART,...

- 無差別攻撃

  LulzSecによる電リクDDoS攻撃など

動機、目的

- 表現の自由、検閲反対、環境保護、格差是正、人権保護、児童ポルノ反対
- 楽しい、単なる自慢、自己表現
- 手段の目的化、目的意識の希薄化

コミュニケーション

* ソーシャルメディアのパワー

  IRC, Pad, Blog, Twitter, Facebook

* Open Proxy, VPN, Tor, i2p

* オープン、匿名、透明性

Twitter

The Lulz Boat
@LulzSec view full profile →

Lulz Security® (LulzSec), the world's leaders in high-quality entertainment at your expense - http://lulzsecurity.com/

1,333	2	357,768	3,826
Tweets	Following	Followers	Listed

The Real Sabu
@anonymouSabu view full profile →

We are all anonymous.

4,147	14	23,305	514
Tweets	Following	Followers	Listed

AnonymousIRC
@AnonymousIRC view full profile
The Internet

We are Anonymous. We are #AntiSec We are Legion.We do not forgive. We do not forget. We love you. Expect us.Bitcoins to: 18NHixaoQekQJ3y52aBGJJwgBWX9X3myYR
http://the.internet

4,615	22	146,837	2,098
Tweets	Following	Followers	Listed

AnonOps
@anonops view full profile →

We are fighters for internet freedom.
http://anonops.blogspot.com/

440	4	65,081	1,636
Tweets	Following	Followers	Listed

Anonymous Operations
@Anon_Central view full profile →
Everywhere

57 65 20 61 72 65 20 41 6e 6f 6e 79 6d 6f 75 73 2c 20 77 65 20 64 6f 20 69 74 20 66 6f 72 20 66 72 65 65 20 66 6f 72 20 74 65 68 20 6c 75 6c 7a 21 21
http://www.anonops.org/

5,913	845	39,174	1,321
Tweets	Following	Followers	Listed

Anonymous
@YourAnonNews view full profile →
Right behind you.

We are Anonymous, We are legion, We never forgive, We never forget, Expect us.
http://youranonnews.tumblr.com/

6,910	75	35,196	815
Tweets	Following	Followers	Listed

Anonymous
@AnonymousPress view full profile →
Interwebs

We are Anonymous; We are Legion; We do not forgive; We do not Forget; Expect us!
http://www.example.com

616	105	23,805	454
Tweets	Following	Followers	Listed

Anonymous
@AnonyOps view full profile →
worldwide

** Civil & Human rights activist. * Government Corruption, be damned. * I don't break into things, I break out of things.* https://www.eff.org/pages/say-no-to-online-censorship

4,467	211	17,319	541
Tweets	Following	Followers	Listed

Topiary
@atopiary view full profile →
TopiaryHatemail@gmail.com

Simple prankster turned swank garden hedge. Worked with Anonymous, LulzSec, and other such paragons of intense cyber victory. You are free.

6	5	11,320	339
Tweets	Following	Followers	Listed

攻撃方法(1)DDoS

* 事前にターゲットや実施日時が公開されるケースが多い
  → 失敗に終わる場合も
* 正当な抗議手段と主張

LOIC (Low Orbit Ion Cannon)

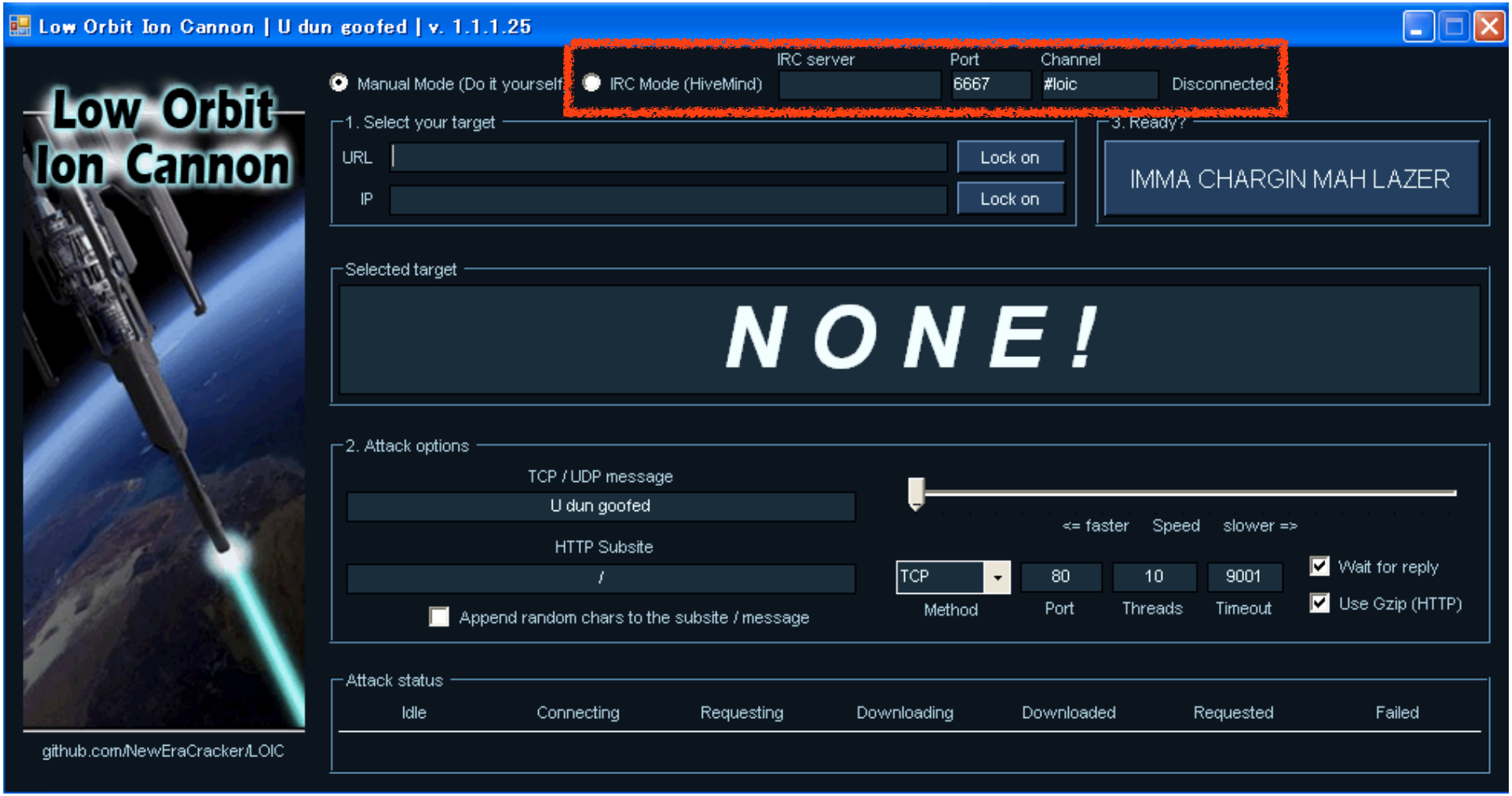
- LOIC, HOIC, JS LOIC, Java LOIC, PyLOIC, ...
- IRCモード (Hivemind) → Botnet機能

  数十人から数百人の参加者

- LOICにはIPアドレス詐称機能はない

  → Backscatterで攻撃が観測されている

LOIC (Low Orbit Ion Cannon)



#opsony

Congratulations, Sony.

You have now received the undivided
Anonymous. Your recent legal action again
hackers, GeoHot and Graf_Chokolo, ha
alarmed us, it has been deemed wholly un

You have abused the judicial system in a
censor information on how your products wo
victimized your own customers merely for po
sharing information, and continue to target
who seeks this information. In doing so you
the privacy of thousands. This is the informat
willing to teach to the world for free. Th
information you wish to suppress for sake
greed and complete control of the us

Now you will experience the wrath of A
You saw a hornets nest, and stuck your p
You must face the consequences of yo
Anonymous style.

Knowledge is Free.
We are Anonymous.
We are Legion.
We do not Forgive.
We do not forget.

Expect us.

irc.anonops.ru:6667
http://irc.lc/anonops/opsony

攻撃方法 (2) 情報漏洩

* SQLインジェクション, LFI/RFIなどの脆弱性を悪用する
* 狙われてから脆弱性が見つかるのか、脆弱性があるから狙われるのか?
* 取得した情報をPastebin/TPB/MediaFireなどで公開
  ただし自ら不正利用することはほとんどない?
  → 被害の実態は不明

#AntiSec

Type	Name (Order by: Uploaded, Size, ULed by, SE, LE) View: **Single** / Double	SE	LE
Other (Other)	Texas Takedown Thursday: Chinga La Migra IV Uploaded 09-02 20:26, Size 2.56 GiB, ULed by AntiSecurity	8	0
Other (Other)	Fuck FBI Friday IV: Vanguard Defense Industries Uploaded 08-19 15:57, Size 1.05 GiB, ULed by AntiSecurity	8	0
Other (Other)	Corrupt Brazil (Satiagraha) Uploaded 08-10 03:23, Size 4.73 GiB, ULed by AntiSecurity	6	1
Other (Other)	Shooting Sherriffs Saturday Uploaded 08-06 19:47, Size 7.39 GiB, ULed by AntiSecurity	30	2
Other (Other)	Fuck FBI Friday III: ManTech Uploaded 07-29 23:30, Size 390.19 MiB, ULed by AntiSecurity	25	0
Other (Other)	Military Meltdown Monday: Mangling Booz Allen Hamilton Uploaded 07-11 20:02, Size 130.5 MiB, ULed by AntiSecurity	26	0
Other (Other)	Fuck FBI Friday II: IRCFederal Uploaded 07-08 17:46, Size 107.31 MiB, ULed by AntiSecurity	14	0
Other (Other)	Turkish Takedown Thursday Uploaded 07-07 00:44, Size 21.79 MiB, ULed by AntiSecurity	9	0
Other (Other)	Chinga La Migra III Uploaded 07-01 16:56, Size 55.02 MiB, ULed by AntiSecurity	7	0
Other (Other)	Chinga La Migra II Uploaded 06-29 15:26, Size 155.7 MiB, ULed by AntiSecurity	12	0
Other (Other)	antisec01 Uploaded 06-29 00:44, Size 379.42 MiB, ULed by AntiSecurity	8	1

http://thepiratebay.org/user/AntiSecurity/

攻撃による影響

* 被害にあった日本企業

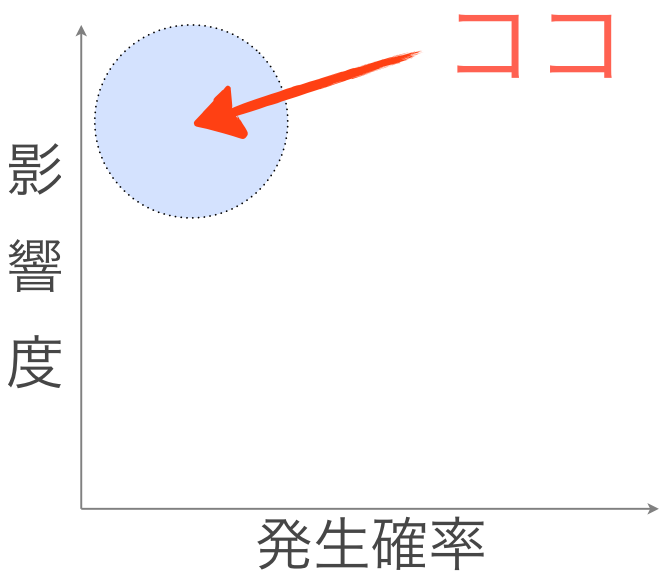
  実は非常に少ない、しかも海外子会社ばかり

* 属性の問題

  国籍、業種など

  → 日本語は最強のファイアウォールか?

発生確率は低いが、起きた場合の影響が大きいリスク



対応策

攻撃の予測は可能か?

* 情報収集/分析能力の強化

  すべて自分達だけでやる必要はない

  一般のニュース、同業他社への攻撃、

  自社の評判、などの公開情報

* 自組織に影響が及ぶか否かの判断

対応

- 攻撃原因を取り除く
- 攻撃者に関する情報の分析と対応
  (攻撃の動機や方法→脆弱性確認)
- 監視体制の強化 (なにかあれば即応)
- 攻撃の影響把握、ダメージコントロール