悪性サイトドメインの長期観測結果に基づく
ブラックリスト利用の有効性に関する一考察

MWS2013

2013/10/22

NTT Communications
須藤 年章

ここ数年の状況

- Web経由での感染、Web経由での情報流出
- さまざまな誘導手段を用いて悪性サイトへ誘導
- ユーザーが集まりやすいサイトやサービス経由での感染

- モバイル、ホスティング、クラウドサービスの拡大
  - PC利用率の低下、ユーザー環境の変化
  - 攻撃用サイトの構築のしやすさの向上
- ユーザーリテラシの低下
  - クラウド、ホスティング、スマホなどを使って、知識がなくても簡単にネット上のサービスが利用できる
  - PCの使い方なんて適当でいい

簡単な手法でユーザーは誘導され感染してしまう

対策

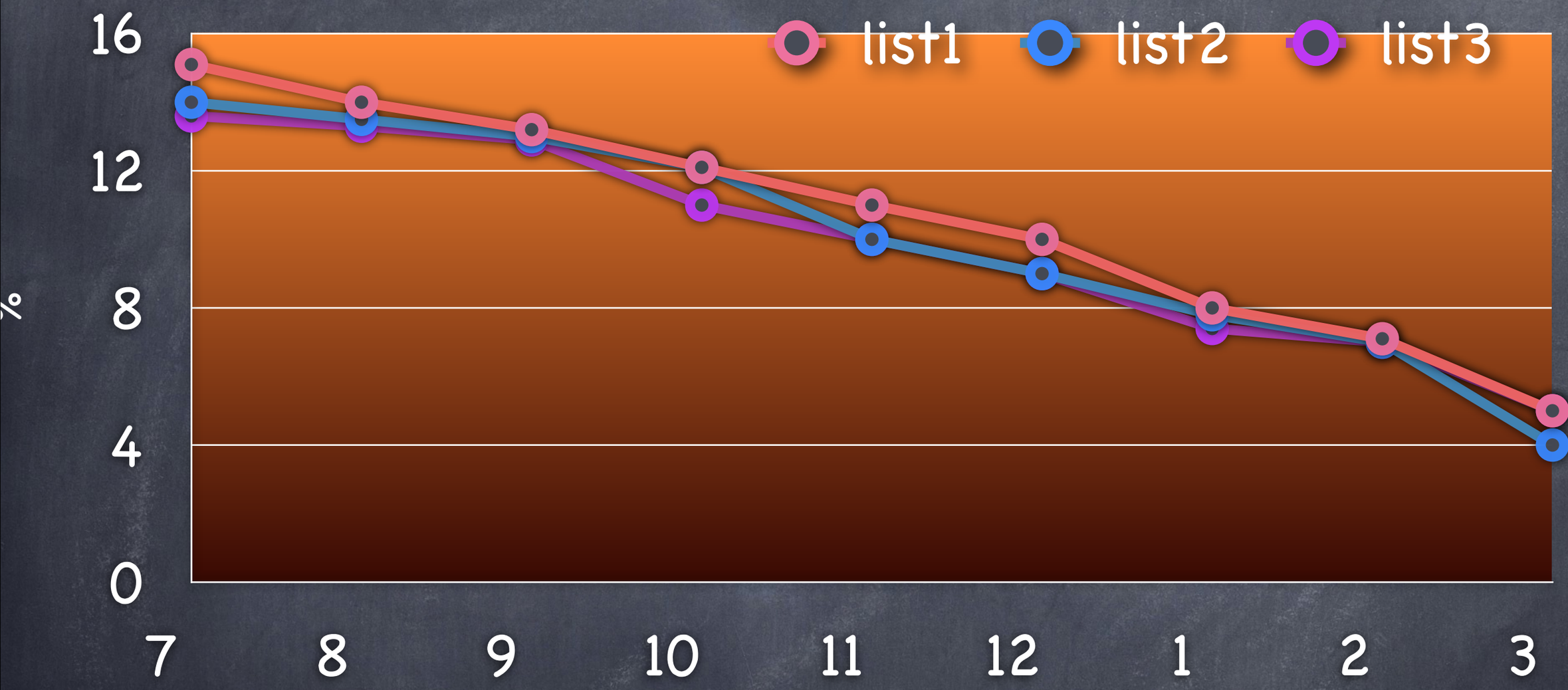
- 不正なサイトにアクセスしないように
- アクセスしても感染しないように
- 初期感染してもそれ以上の被害の拡大を止める
- そのためのblacklistの拡充方法の模索

blacklistでegress filter

blacklistへの疑問

- 大量なshort lived domainの扱い
- リスト量の価値
  - 100のサイトへの通信をとめるために数億
- 長期に登録されている情報の価値
  - 一年間だれもアクセスしない
  - 逆に古いドメインが期間を開けて別の攻撃で再利用
- beta bot/dummy/test
- sinkhole,blackhole,honeypot
- 正規ドメインの扱い

ブラックリストに登録されているドメインの中で実際にアクセスのあったドメインの割合



本来はブロックできない正規サービスのドメイン等も含まれるためこの割合になる。それらの要素を除外すると1%未満になる。

データセットから抽出できるドメイン

No	Dataset	抽出したドメイン数
1	MWS Dataset 2008	32
2	MWS Dataset 2009	12
3	MWS Dataset 2010	10
4	MWS Dataset 2011	2

データセットから抽出できるドメインの中で長期観測対象データが抽出できたドメイン

年度間で同じものがあるためユニークで３７個

解析用データ

domain

応答・レコード

A

AAAA

NS

TEXT

DS

NXrecord

ServerFail

レジストラ

レジストラント

ステータス

逆引き

IP所有者

AS

経路情報
ハイジャック
情報

サービス
ISP/ホスティ
ング等

定期的に取得

ドメイン、IPと利用されるサービスの関連性

解析用データ

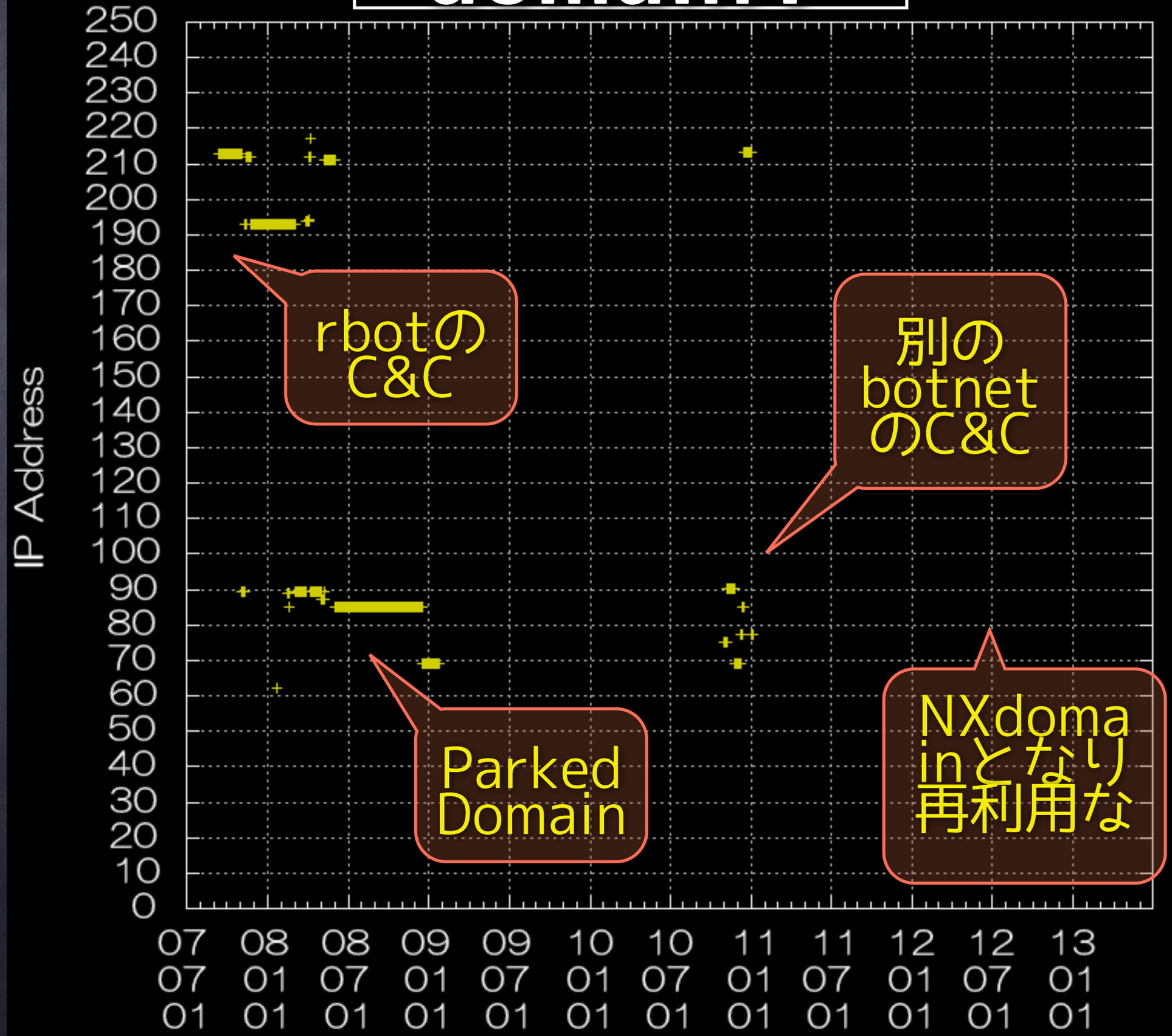
- 期間：　2007年7月1日から2013年7月31日
- ドメイン数：数万（随時追加）
  - 情報元（400種類の悪性サイト情報）
    - 独自調査
    - セキュリティ関連団体の無償リスト
    - 管理者、研究者、リサーチャー等のブログ等からの情報
    - 無償IDS等のシグネチャ情報

など

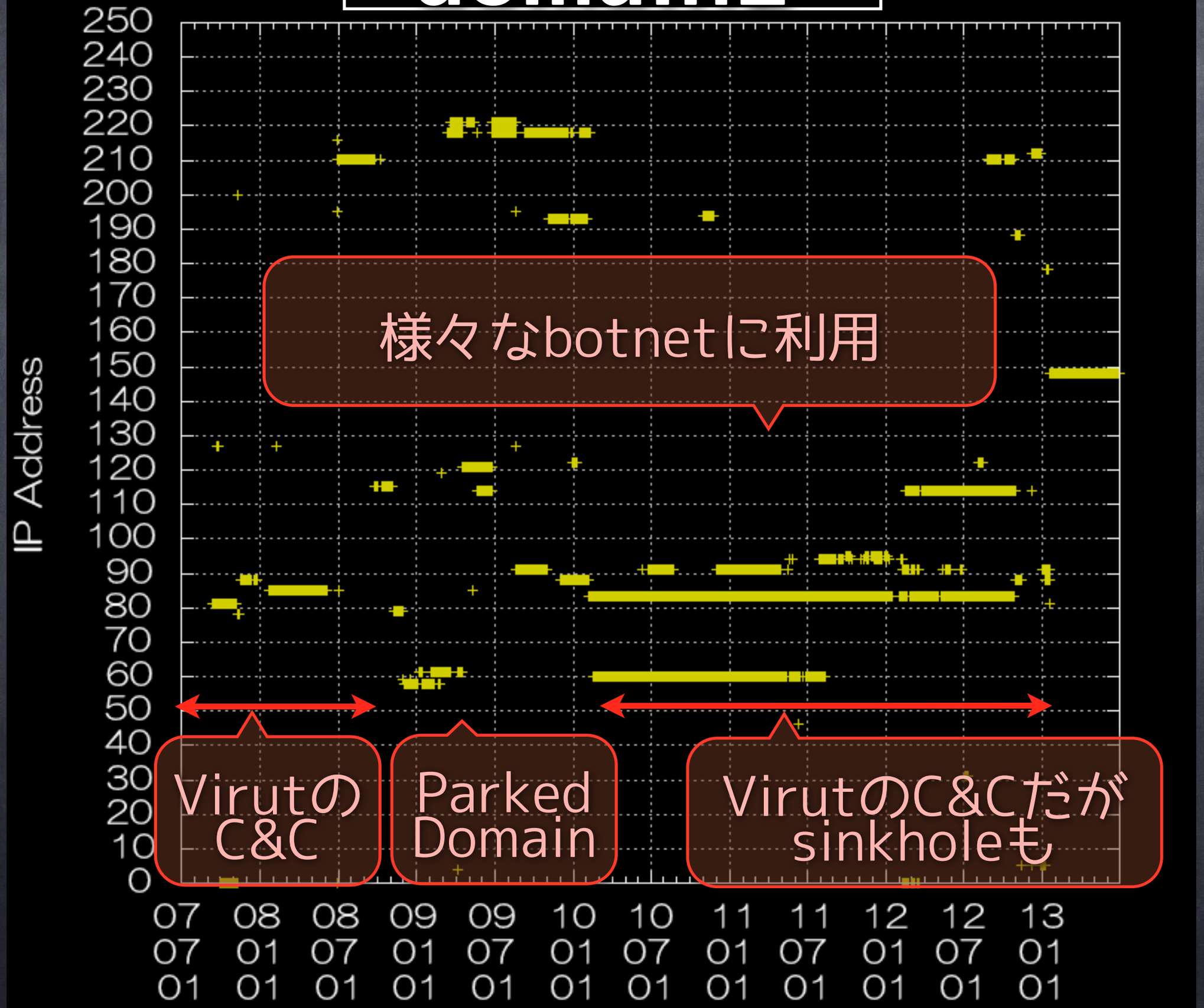
有効なAレコードが設定されていた期間

有効なグローバルアドレスが設定されていた期間
最短19時間　最長1717日(継続中)

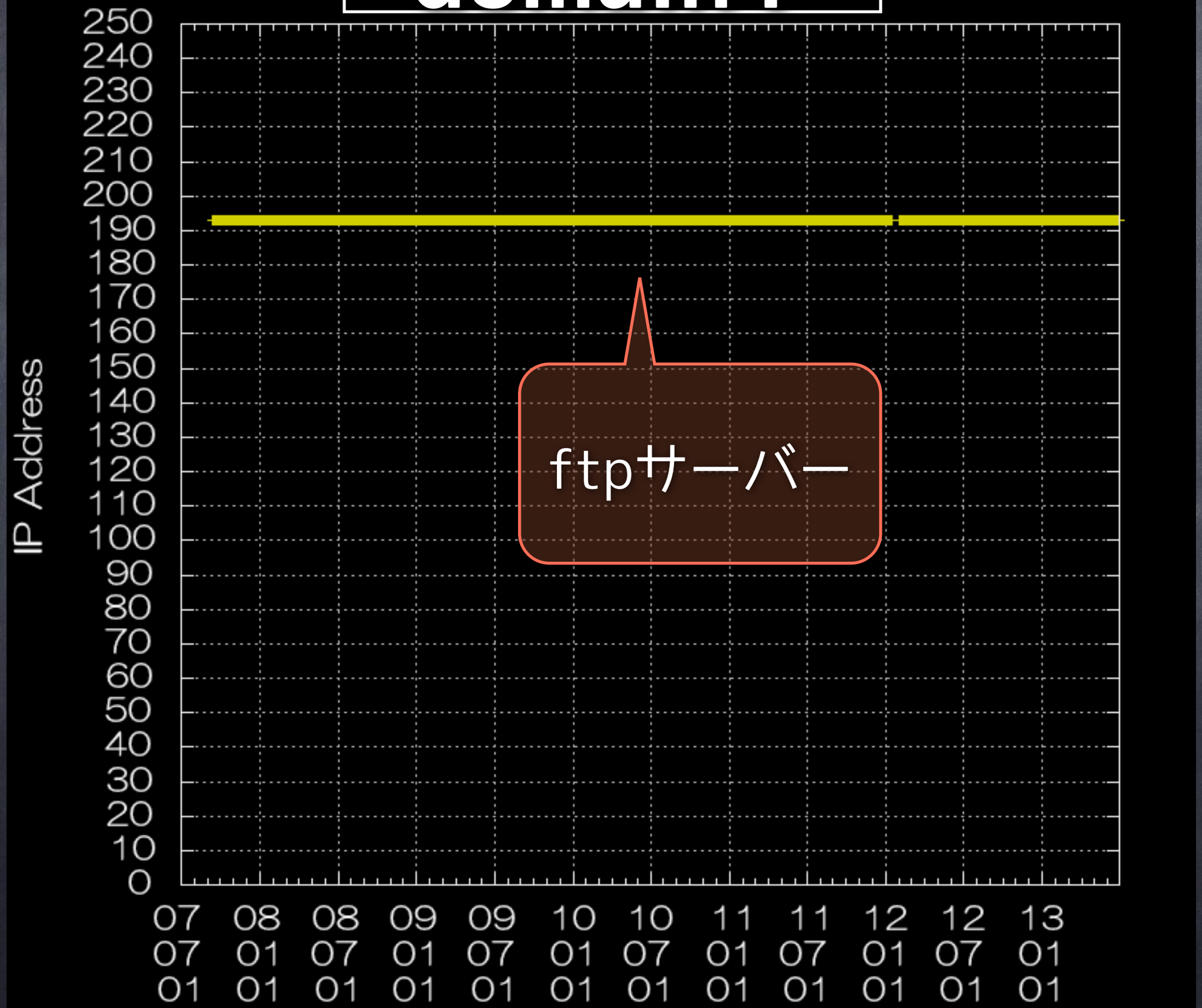
domain1


IP Address
250
240
230
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
07 07 01
08 01 01
08 07 01
09 01 01
09 07 01
10 01 01
10 07 01
11 01 01
11 07 01
12 01 01
12 07 01
13 01 01
rbotの C&C
別の botnet のC&C
Parked Domain
NXdomain となり 再利用な

domain2


IP Address
250
240
230
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
07 07 01
08 01 01
08 07 01
09 01 01
09 07 01
10 01 01
10 07 01
11 01 01
11 07 01
12 01 01
12 07 01
13 01 01
様々なbotnetに利用
VirutのC&C
Parked Domain
VirutのC&Cだがsinkholeも

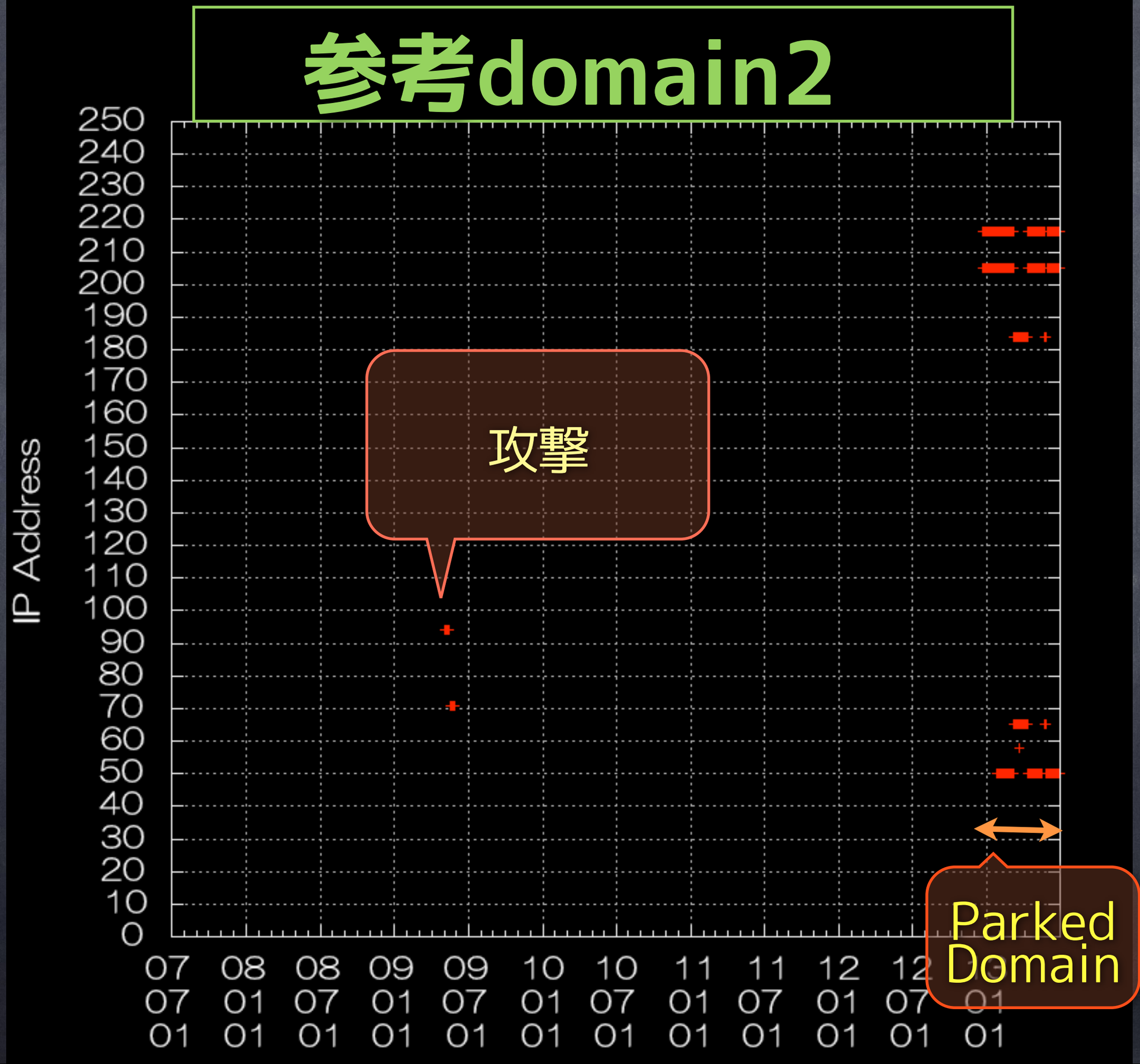
domain4


IP Address
250
240
230
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
07 07 01
08 01 01
08 07 01
09 01 01
09 07 01
10 01 01
10 07 01
11 01 01
11 07 01
12 01 01
12 07 01
13 01 01
ftpサーバー

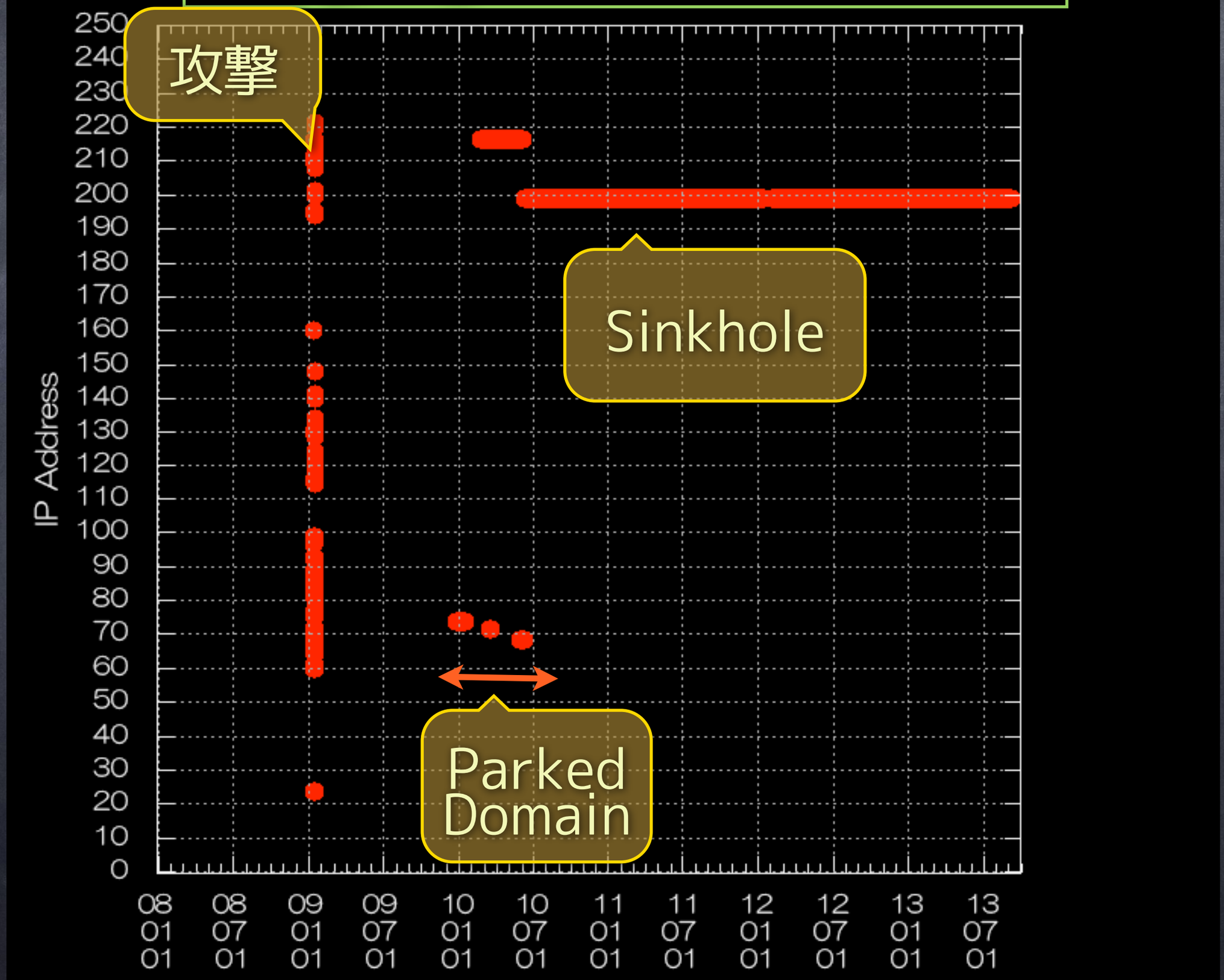
参考domain1


IP Address
250
240
230
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
07 07 01
08 01 01
08 07 01
09 01 01
09 07 01
10 01 01
10 07 01
11 01 01
11 07 01
12 01 01
12 07 01
13 01 01
Kraken？
1年後1日だけ
復活

参考domain2


IP Address
250
240
230
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
07 07 01
08 01 01
08 07 01
09 01 01
09 07 01
10 01 01
10 07 01
11 01 01
11 07 01
12 01 01
12 07 01
01 01
攻撃
Parked Domain

参考domain3


攻撃
Sinkhole
Parked Domain
IP Address
250
240
230
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
08 01 01
08 07 01
09 01 01
09 07 01
10 01 01
10 07 01
11 01 01
11 07 01
12 01 01
12 07 01
13 01 01
13 07 01

結果１

攻撃に再利用されたドメイン	19（51.3%）
再利用されなかったドメイン	10（27.0%）
継続攻撃利用中ドメイン	1（2.7%）
最初から対処済みドメイン	7（18.9%）
一般サイトへの転用	0（0.0%）

- 2013年7月31日時点でAレコードのあるドメインは７個
  - Parked Domain
  - 対策中ドメイン
  - ftpサイト
  - Sinkhole

結果２

有効なAレコードが設定されていた日数	平均701日
最短	19時間
最長	1717日(継続中)

攻撃終了後、契約期間満了まで削除されず放置

最近流行のDrive-by攻撃にくらべて長い
用途、機能によってこれらの特性は変わる

ドメイン作成から攻撃終了まで

ドメイン作成

数日

攻撃

攻撃終了

1～3年

契約更新

契約更新せず

攻撃再利用

最近流行の攻撃はこの部分が短く再利用がない

レジストラによる対策

数週間

再登録受付

別の契約者

攻撃

一般

Datasetからは見えない最近の状況

- Drive-by等で用いられる攻撃サイトは数時間しか利用されないshort livedな傾向が強い
- ドメイン作成後最初は攻撃利用せず普通のドメインとして存在させ、普通の通信をさせる→ある日突然攻撃に移行
- Cloud系キャッシュ,プロキシサービスの利用

用途の違いによる特性の違い

まとめ

- 攻撃が終了しても契約期間満了まで放置、対策後の再販売
  - 同一攻撃への再利用、別の攻撃での再利用がある
  - アクセス数稼ぎのためのインフラとか、悪用できる可能性
  - ドメインは同じでも利用しているサーバー、サービスが変わる
- 一度攻撃に利用されたドメインは二度と使えなくしてもいいのでは？
  - シンプルな判断をしたい
    - 「ブラックホール済みドメイン。ここへのアクセスがあっても問題なし」みたいな判断がしたい
  - 攻撃に協力的なレジストラ、ホスティングがあるため永久ブラックリスト化しDNS等で対策実施も
- Sinkhole、Blackholeの判別
- 用途別、攻撃別に分析が必要

今後考慮すべき要素

- PC利用者の激減にともなう環境と対応の変化
  - コンシューマと企業等の環境の乖離
- クラウドサービスの展開
  - コンシューマ用の端末はどこに？ストリーミング化やネットのこちら側とあちら側
- 制限されたセキュリティポリシーが適用されている企業においては、そもそもアクセス先が限定されている

ネットワーク内での対策の機能強化
適用する環境毎にカスタマイズしたブラックリストの作成機能とその適用