YNU YOKOHAMA National University

AmpPot Dataset （PRACTICE Dataset）

MWS意見交換会

2016年5月30日（月）

横浜国立大学　松本研究室／
情報通信研究機構 サイバーセキュリティ研究室
牧田大佑 （吉岡先生の代理）

PRACTICE（Proactive Response Against Cyberattacks Through International Collaborative Exchange）：　総務省の「国際連携によるサイバー攻撃予知・即応に関する実証実験」のプロジェクト.

AmpPot Datasetとは？

- 横浜国立大学で運用している
  AmpPot（DRDoSハニーポット）
  のトラフィックデータ.
- （一応）昨年度から利用可能.

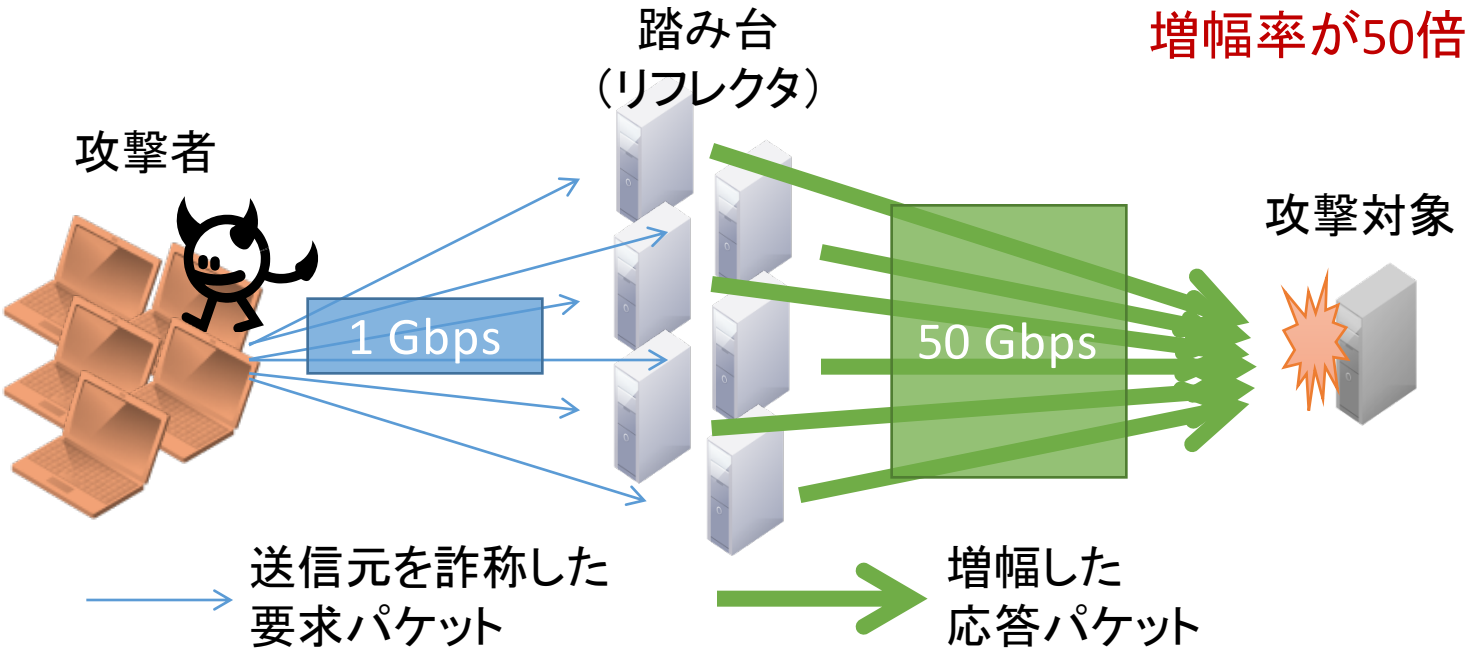
キーワード

✓ DRDoS攻撃（Amp攻撃）

✓ DRDoSハニーポット（AmpPot）

DRDoS攻撃（1/2）

- DRDoS（Distributed Reflection DoS）攻撃
  - インターネット上のサーバ（DNS，NTP等）を踏み台にして実行する分散型のサービス妨害攻撃.
  - サーバで通信を増幅させる（Amp攻撃）.



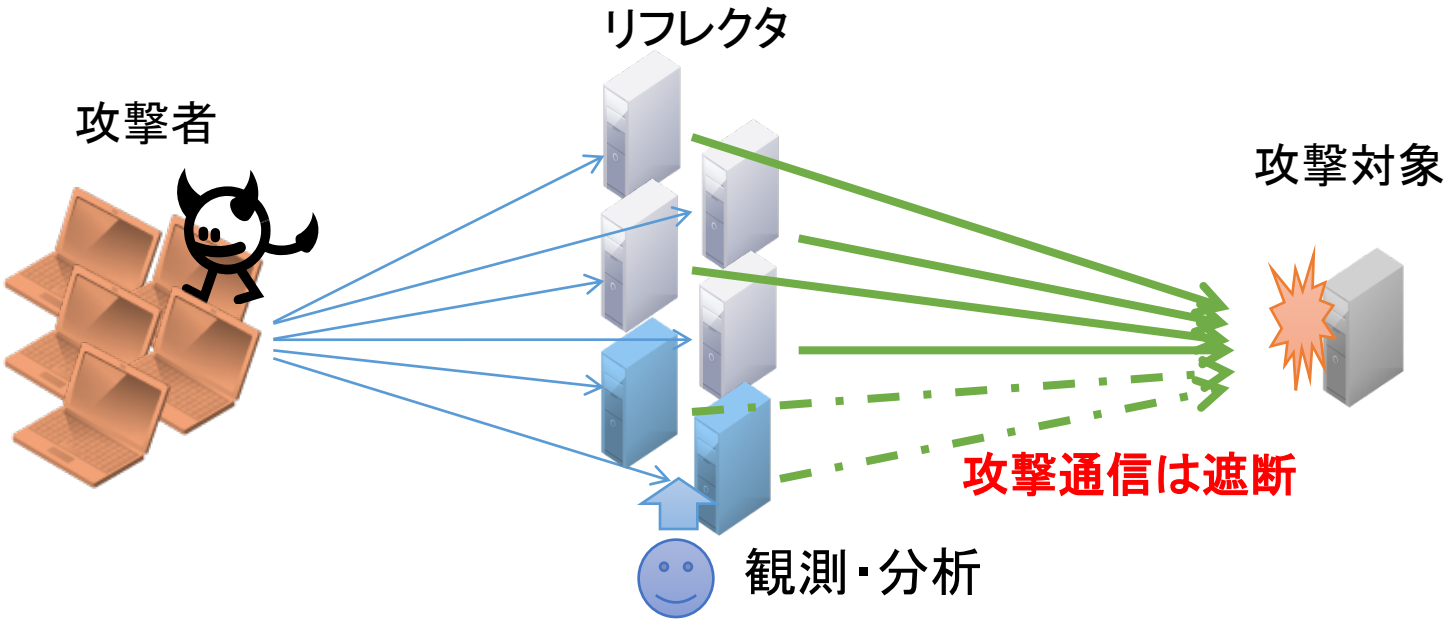
DRDoS攻撃（2/2）

- 2013年3月　Spamhausへの攻撃　300 Gbps

- 2013年～　サイバー攻撃に悪用
  - Anonymous
  - Lizard Squad
  - DD4BC
  - Armada Collective
  - etc.

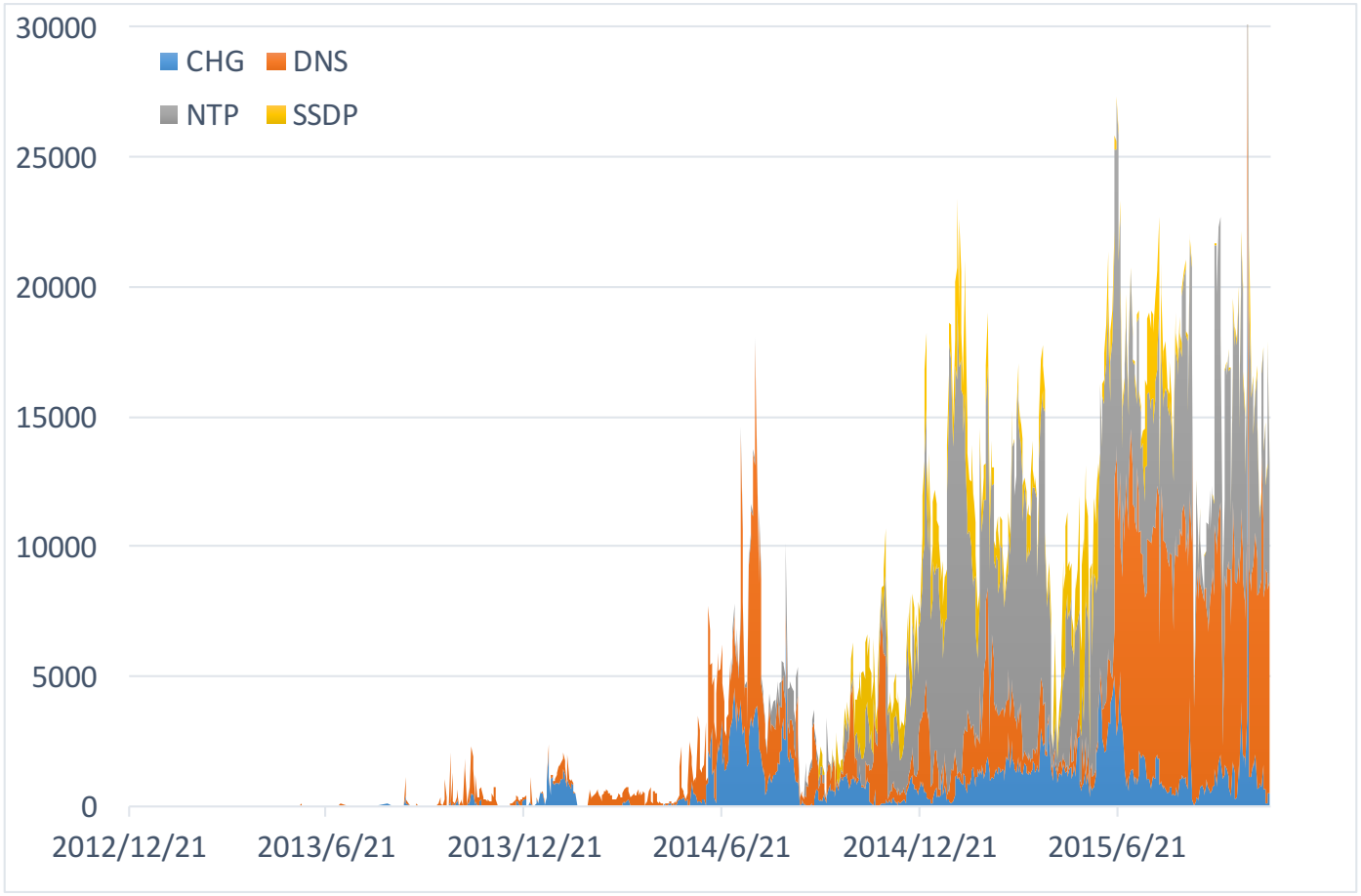
AmpPot（DRDoSハニーポット）

- DRDoS攻撃を観測するハニーポット.
  - 囮のリフレクタをインターネット上に設置.

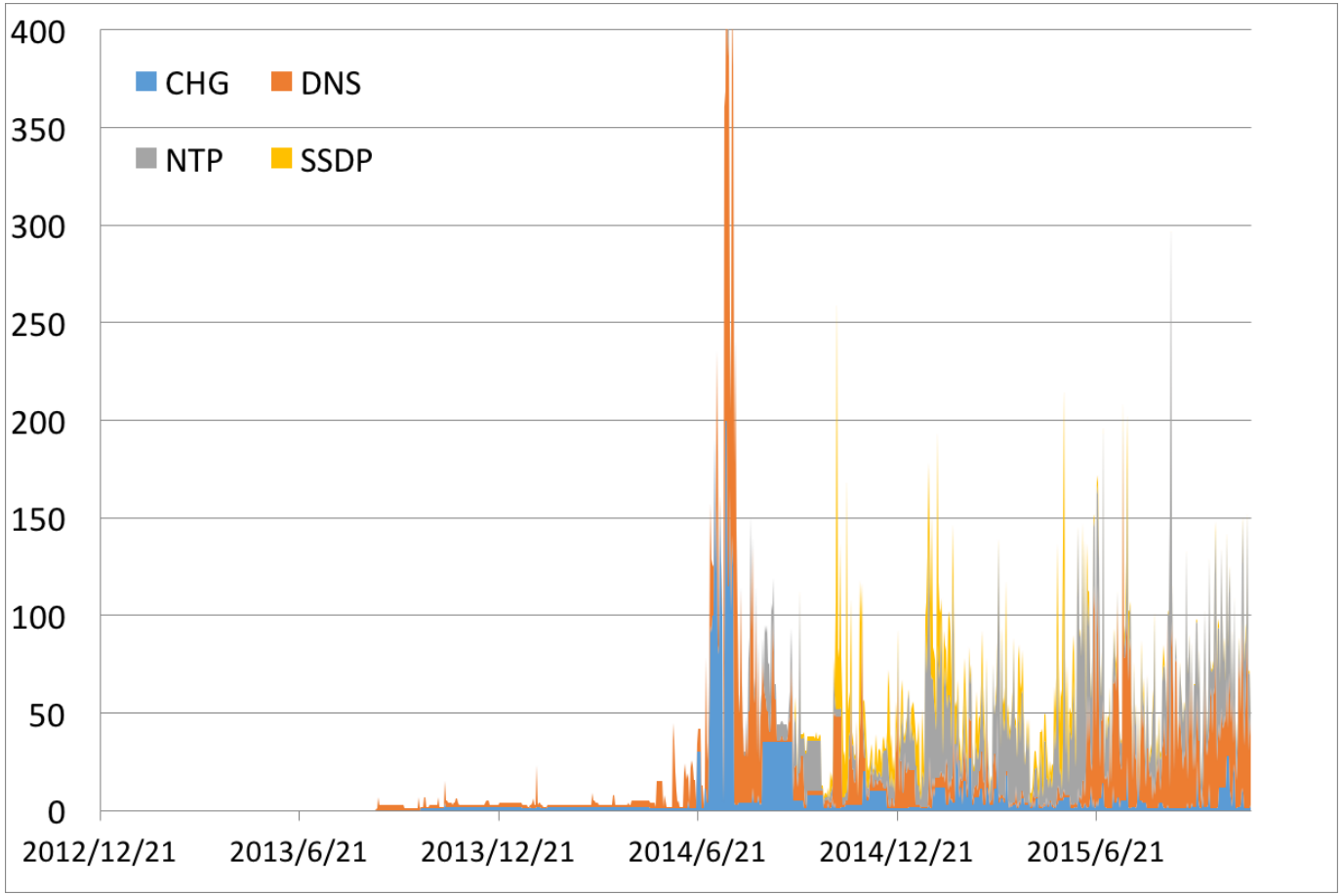


[RAID2015] Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks."

DRDoS攻撃件数


30000
25000
20000
15000
10000
5000
0
CHG
DNS
NTP
SSDP
2012/12/21
2013/6/21
2013/12/21
2014/6/21
2014/12/21
2015/6/21

日本宛の攻撃件数


400
350
300
250
200
150
100
50
0
CHG
DNS
NTP
SSDP
2012/12/21
2013/6/21
2013/12/21
2014/6/21
2014/12/21
2015/6/21

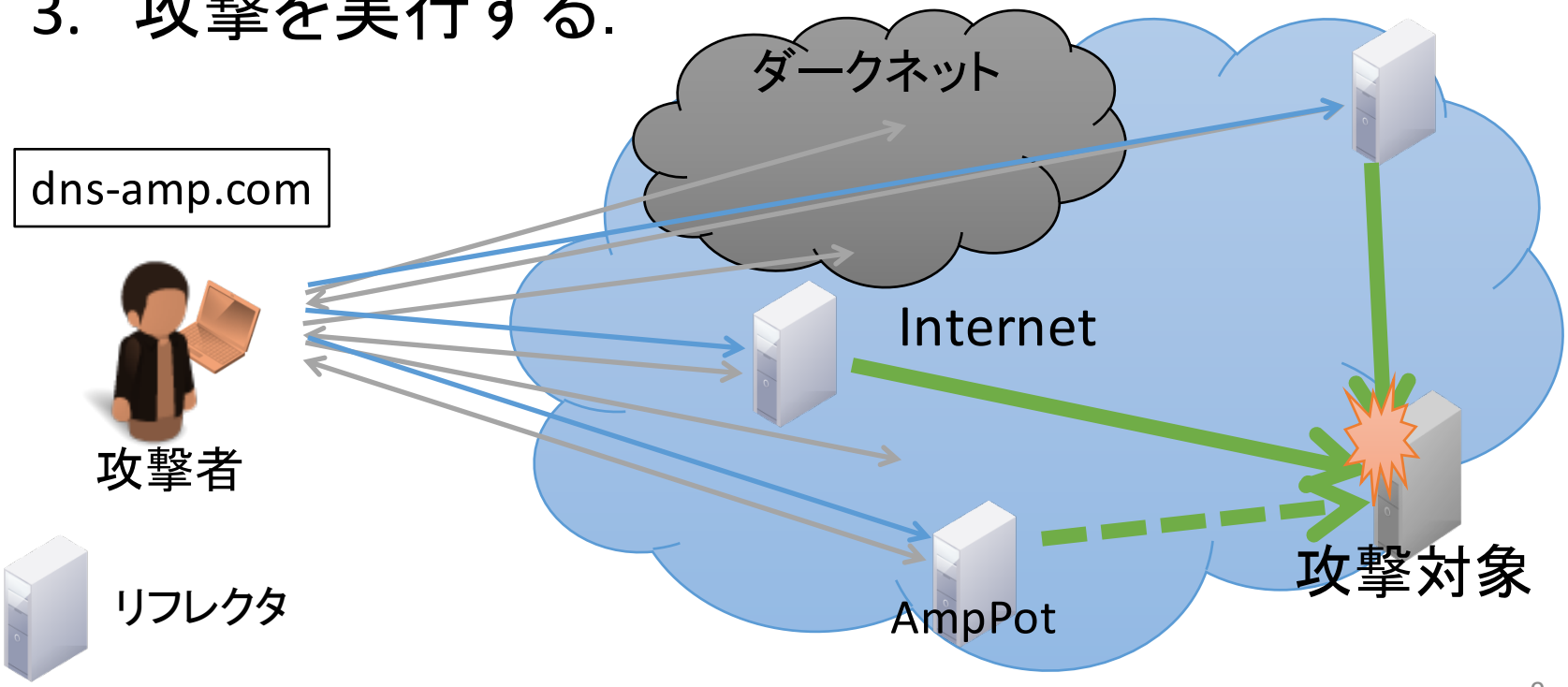
既存研究の例（1）

ダークネットとの相関

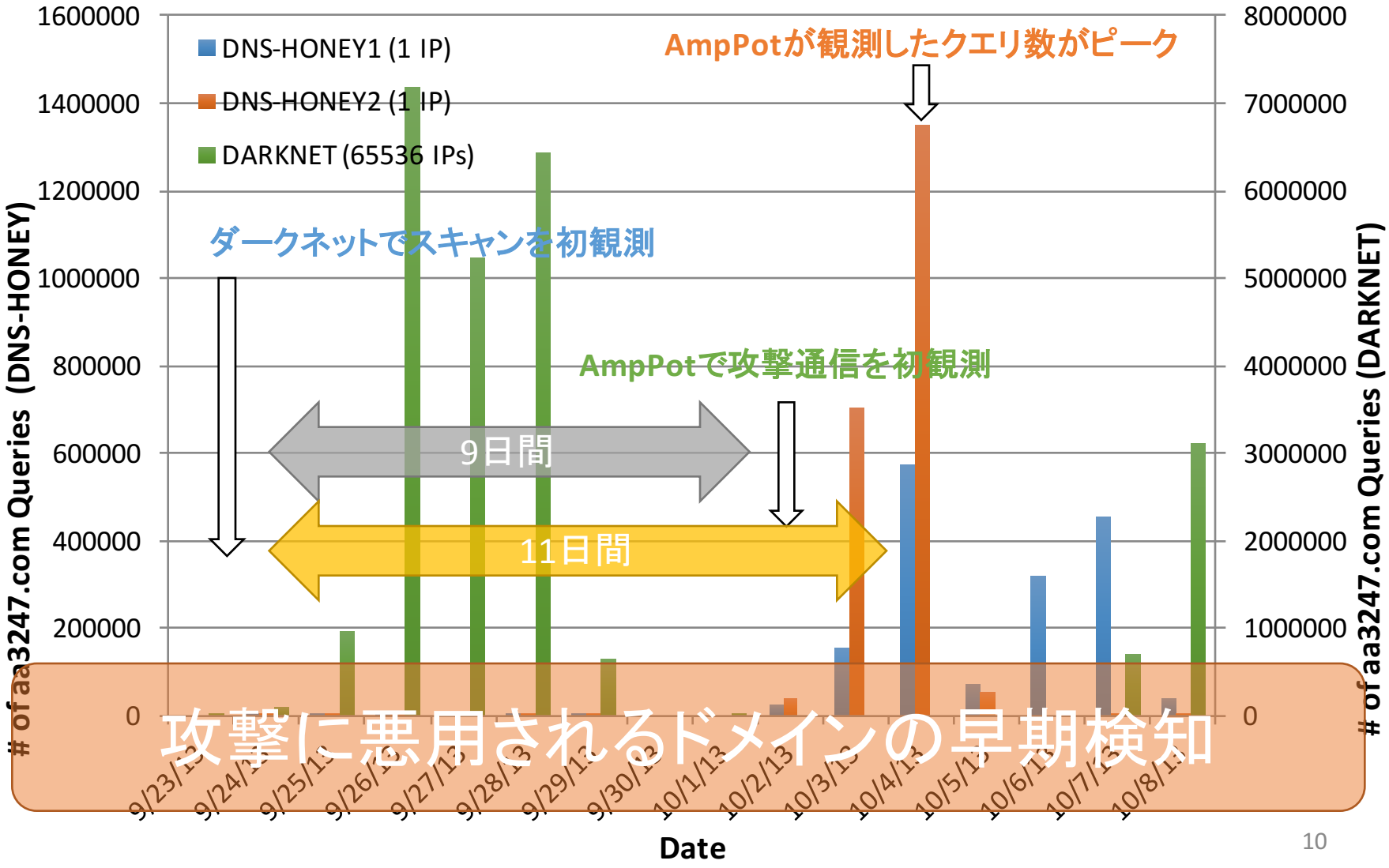
牧田大佑，吉岡克成，松本勉，中里純二，島村隼平，井上大介：DNSアンプ攻撃の事前対策へ向けたDNSハニーポットとダークネットの相関分析，情報処理学会論文誌，Vol.56，No.3，pp.921-931，2015.

攻撃者のシナリオ
（DNSを悪用した攻撃の場合）

1. 攻撃に使用するドメインを用意する.
2. リフレクタを探索するスキャンを行う.
3. 攻撃を実行する.



事例） aa3247.com



既存研究の例（2）

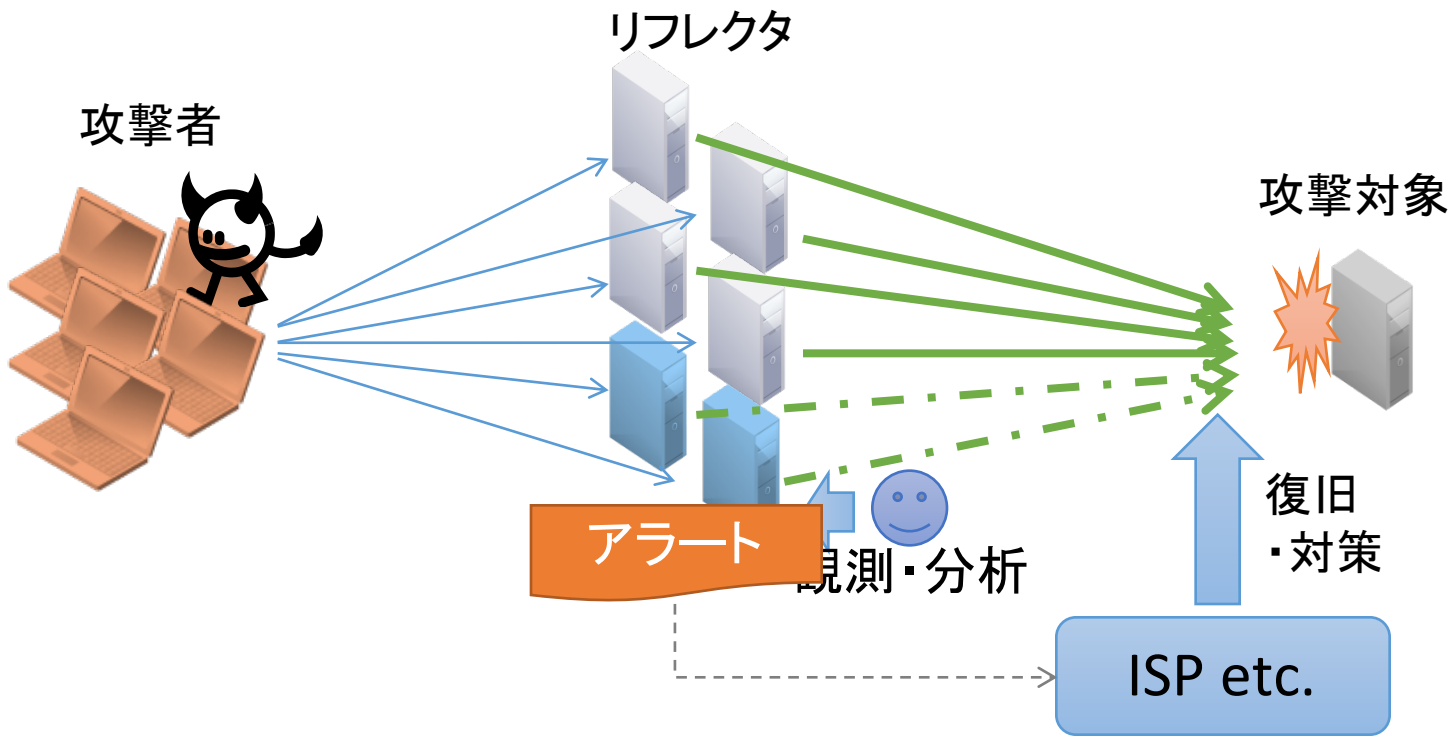
アラートシステム

牧田大佑，西添友美，小出駿，笥見拓也，金井文宏，森博志，吉岡克成，松本勉，井上大介，中尾康二：早期対応を目的とした統合型DRDoS攻撃観測システムの構築，電子情報通信学会，暗号と情報セキュリティシンポジウム，2015．

浦川順平，澤谷雪子，山田明，窪田歩，牧田大佑，吉岡克成，松本勉：ハニーポット監視によるDRDoS攻撃の早期規模推定，電子情報通信学会，暗号と情報セキュリティシンポジウム（SCIS），2015．

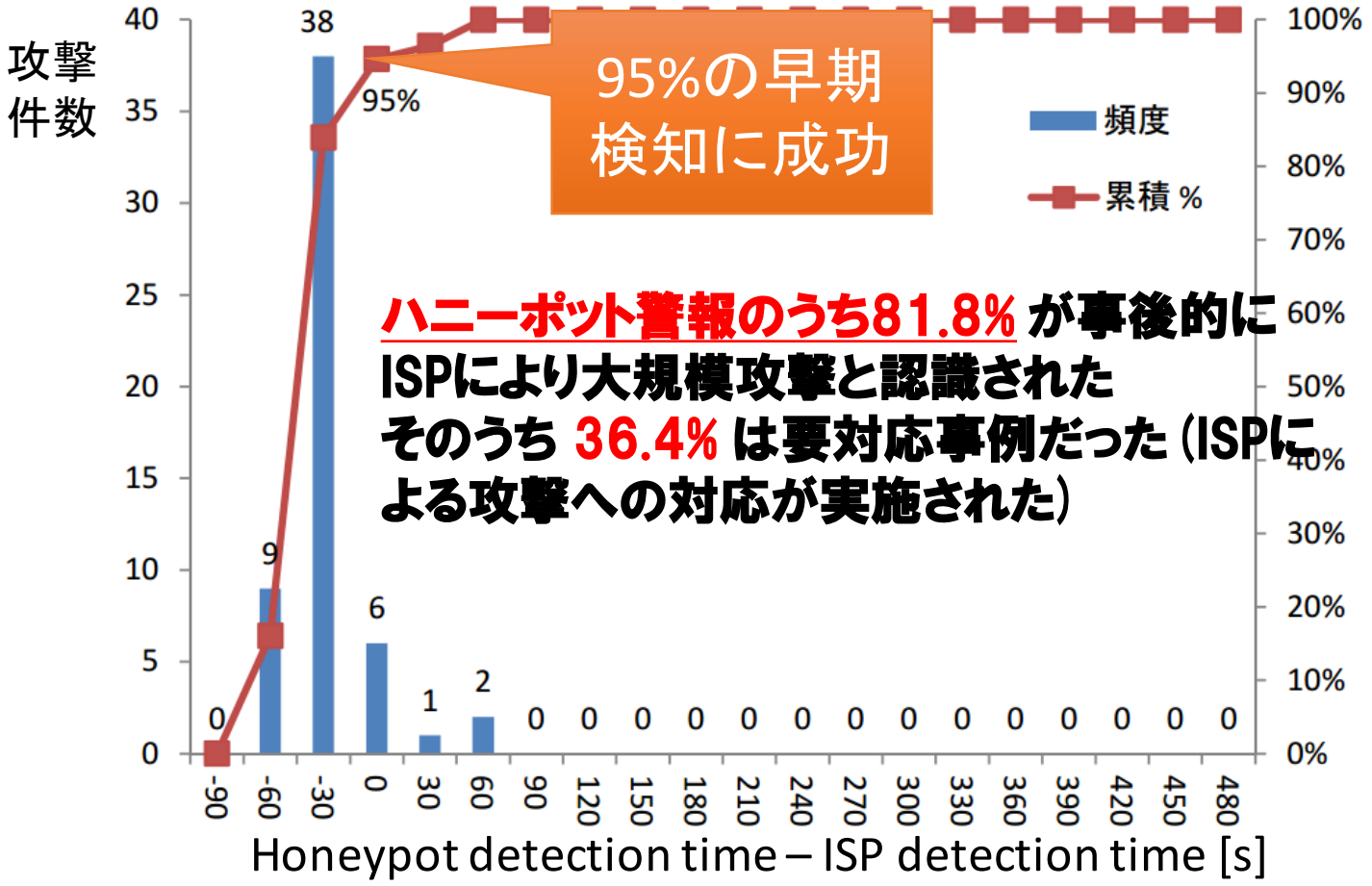
DRDoSアラートシステム

- AmpPotを用いた攻撃情報のリアルタイム共有.



牧田大佑，西添友美，小出駿，筒見拓也，金井文宏，森博志，吉岡克成，松本勉，井上大介，中尾康二：早期対応を目的とした統合型DRDoS攻撃観測システムの構築，電子情報通信学会，暗号と情報セキュリティシンポジウム，2015.

ISPによるDoS検知時刻との比較（2014年8～11月）



浦川順平，澤谷雪子，山田明，窪田歩，牧田大佑，吉岡克成，松本勉：ハニーポット監視によるDRDoS攻撃の早期規模推定，電子情報通信学会，暗号と情報セキュリティシンポジウム（SCIS），2015.

AmpPot Dataset

AmpPot Dataset

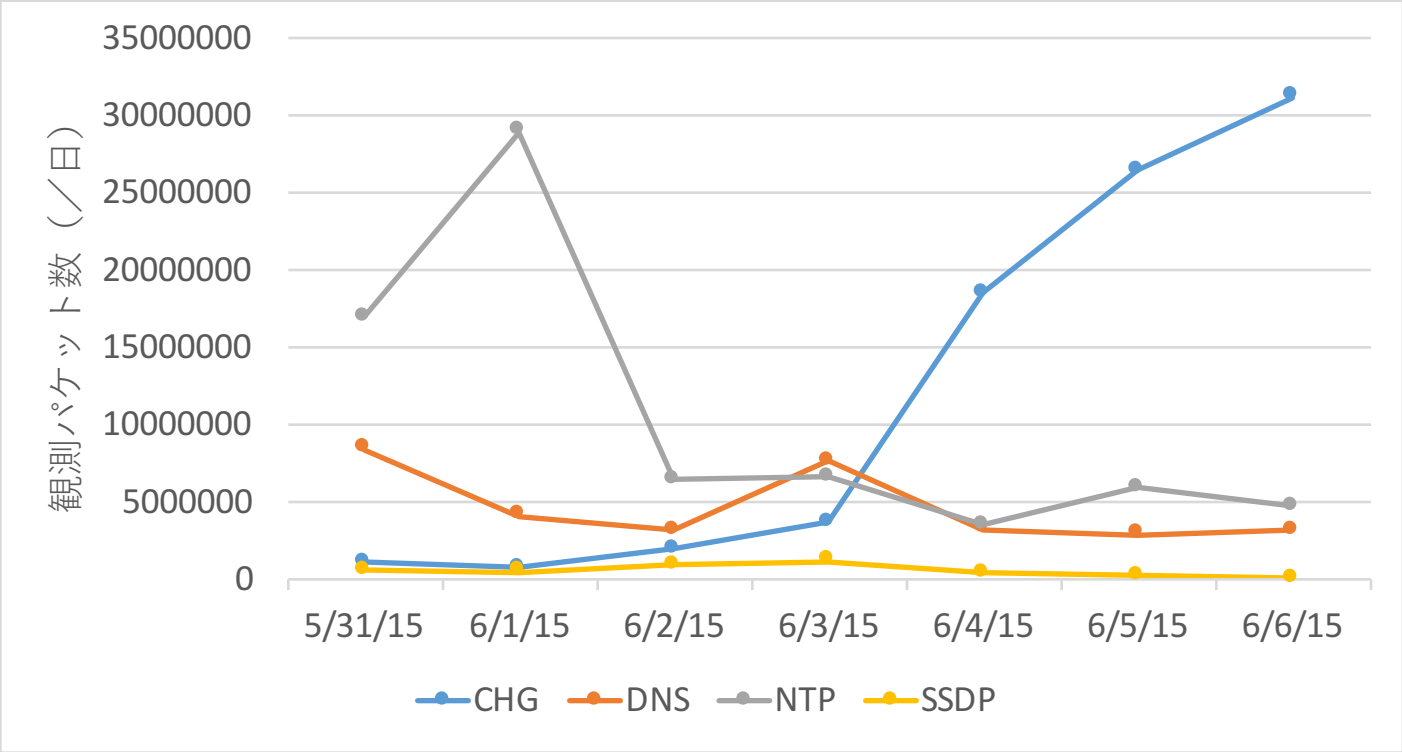
データの内容	AmpPotのトラフィックデータ（クエリのみ）
データ形式	PCAPファイル
AmpPotの台数	1台＠日本
対応サービス	CHG（19/udp, Character Generator） DNS（53/udp, Domain Name System） NTP（123/udp, Network Time Protocol） SSDP（1900/udp, Simple Service Discovery Protocol）
期間	2015年5月31日～6月6日（1週間）
データサイズ	2.1 GByte（gzip圧縮後）
データに含まれる通信の中身	• DRDoS攻撃 • スキャン • その他？（e.g. DNS水責め攻撃）

（注意）
実際の攻撃先のIPアドレスを含むので，データの取扱いにはご注意下さい。

通信からわかる情報

- 攻撃対象
- 攻撃の通信量（踏み台１台あたり）
- 攻撃の継続時間
- 攻撃に使われるサービスの種類
- 攻撃に使われるリクエストの内容
- 踏み台を探す通信（スキャン）の内容・頻度
- etc.

データの基礎統計



（1週間の合計）	CHG	DNS	NTP	SSDP
パケット数	83,021,625	32,057,243	72,449,159	3,223,331
通信先アドレス数	4,304	405	104,446	6,415

ご要望等ございましたら
ご連絡下さい

（吉岡先生） yoshioka@ynu.ac.jp

（牧田） makita-daisuke-jk@ynu.jp