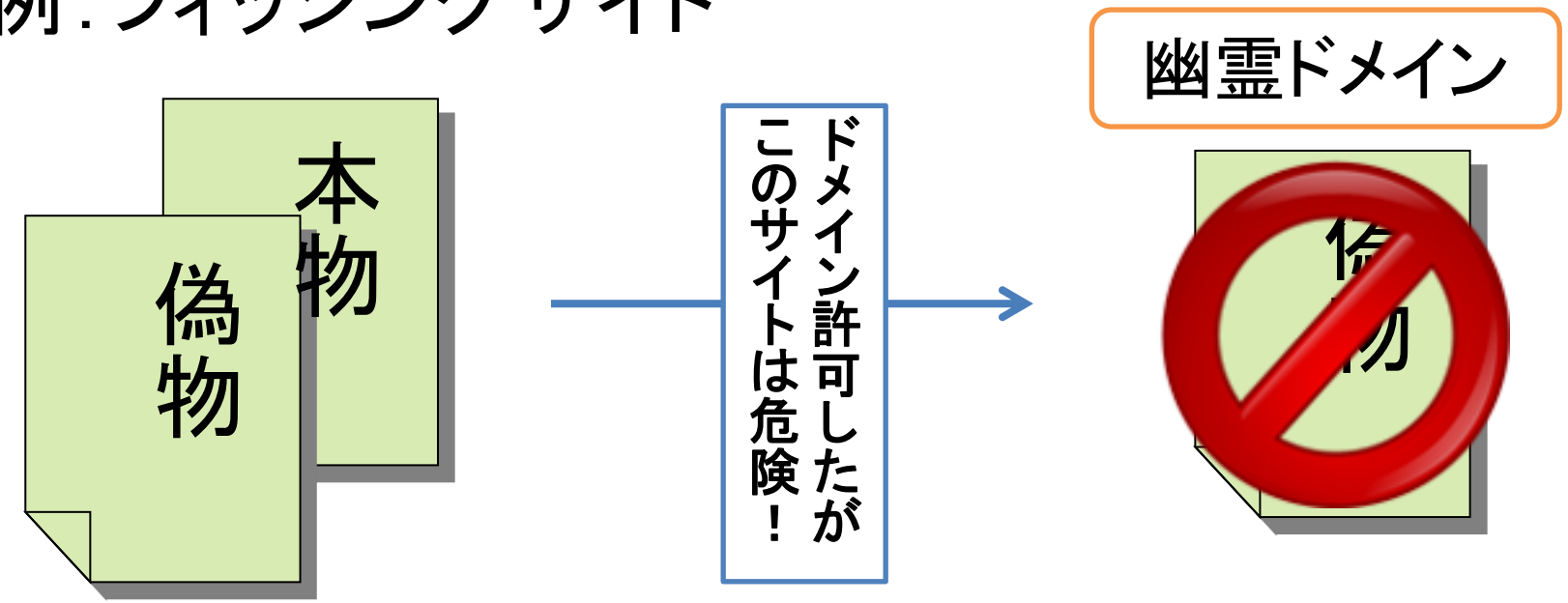
C11 DNSキャッシュ保持に関する脆弱性"ghost domain"の研究

発表者：1BDRM001　有水　智大
指導教員：菊池　浩明

背景

- 悪意あるホストが利用するドメインは上位DNSサーバーから削除・転送先を変更することで使用不能にする対策がとられる

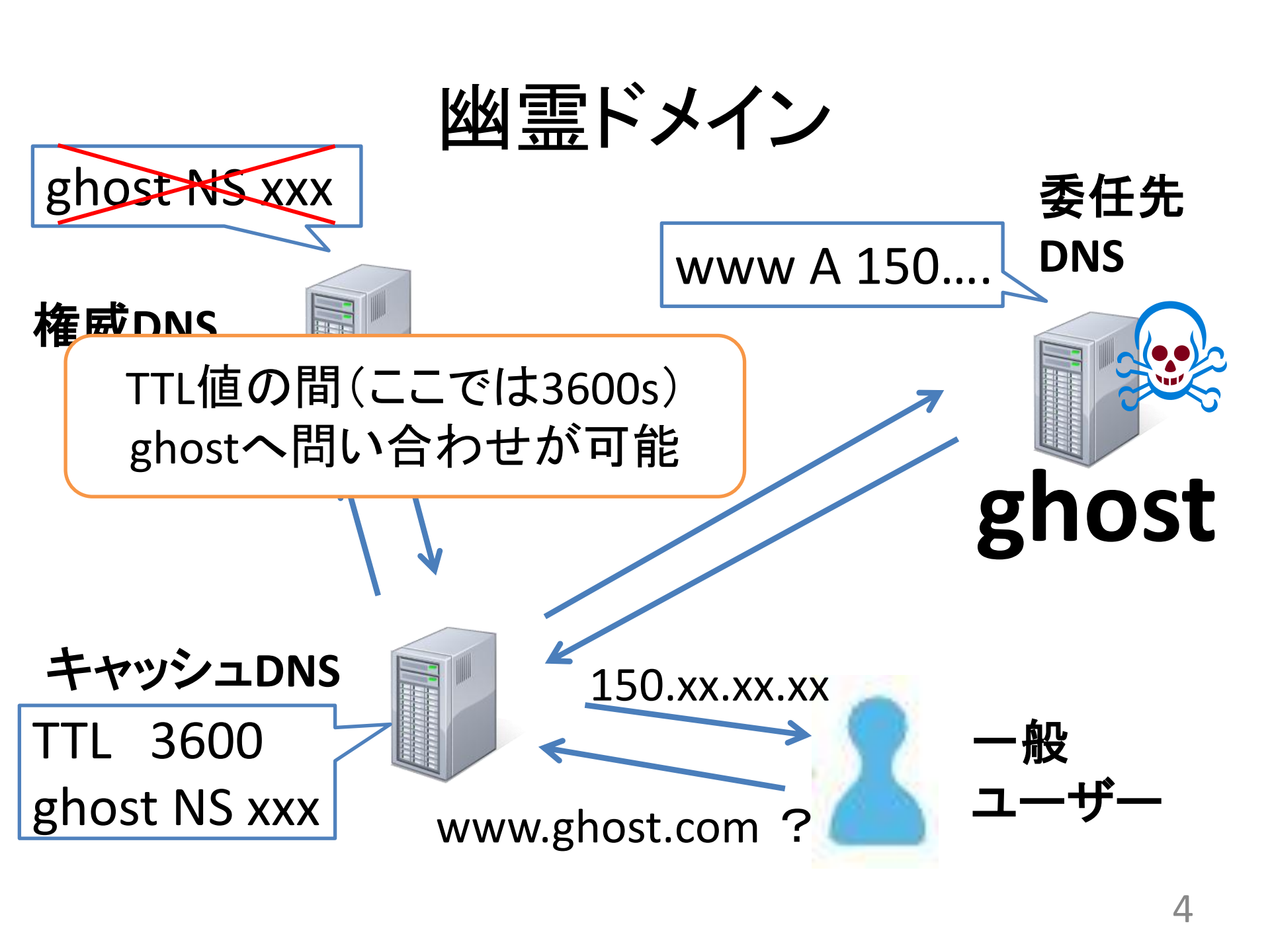
例：フィッシングサイト



幽霊ドメイン

- 2012年2月8日中国・清華大学の Haixin Duan（段海新）らによって報告される
- パブリックDNSに使用することで多くの一般ユーザーに影響

幽霊ドメイン


ghost NS xxx
委任先
DNS
www A 150....
権威DNS
TTL値の間（ここでは3600s）
ghostへ問い合わせが可能
ghost
キャッシュDNS
TTL 3600
ghost NS xxx
150.xx.xx.xx
www.ghost.com ？
一般
ユーザー

幽霊ドメイン

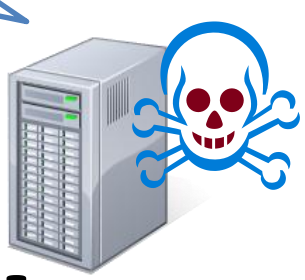
~~ghost NS xxx~~

委任先DNS

www A 150....

権威DNS

com



ghost

3600s後…
まだ有効！

キャッシュDNS

TTL　0?
ghost NS xxx

150.xx.xx.xx

www.ghost.com ？

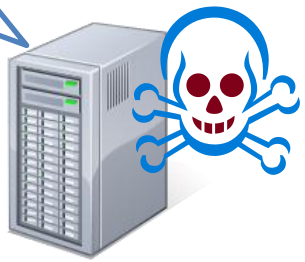
一般ユーザー

なぜ幽霊ドメインができる？

- DNSプロトコルの仕様
「親より子の
NSレコードを優先」

www A 150....
ghost NS yyy

委任先DNS



キャッシュDNS

ghost NS yyy
TTL　3600

子のNSが変更されると
次の名前解決時に
キャッシュが上書きされる
TTLも更新される

すぐに直るのか？

Bindはパッチを公開している

しかし・・・

- 移植のコスト
- ソフトウェアの互換
- 運用上の理由

研究目的

- パブリックDNSサーバーの幽霊ドメインへの現在の対応状況を調査し、パブリックDNSの危険性を明らかにする

- 予想：パッチが出てるためほぼない
- 結果：3割も残っていた！

実験

- ２台のサーバで幽霊ドメイン攻撃を再現
- 2013年1月
- 対象：全世界2791台のPublic DNSサーバ

目的

1. Public DNSサーバの対応状況
2. 攻撃の有効期間
3. 国毎の対応状況
4. DNSソフトウェア毎の対応状況

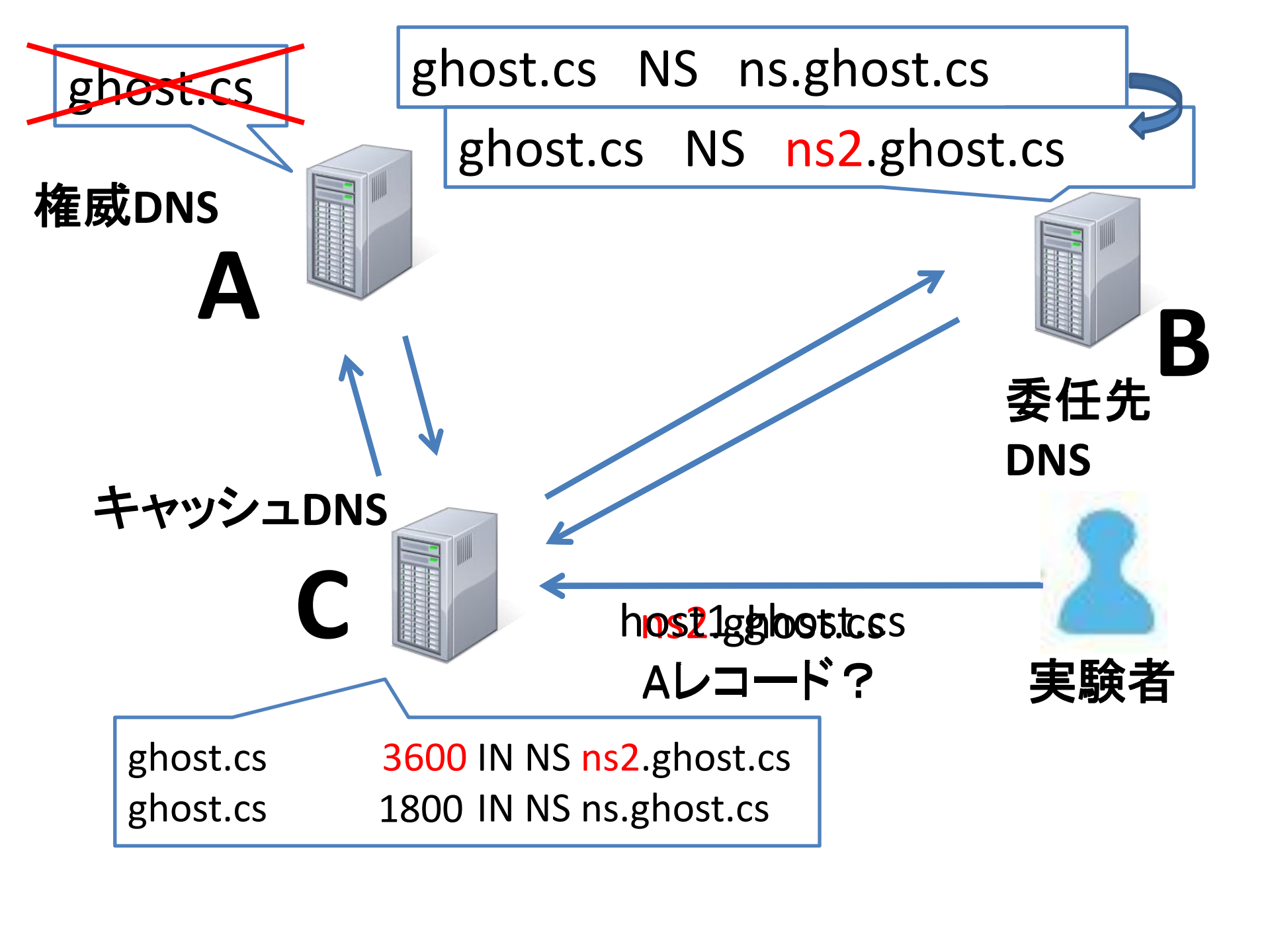
調査対象

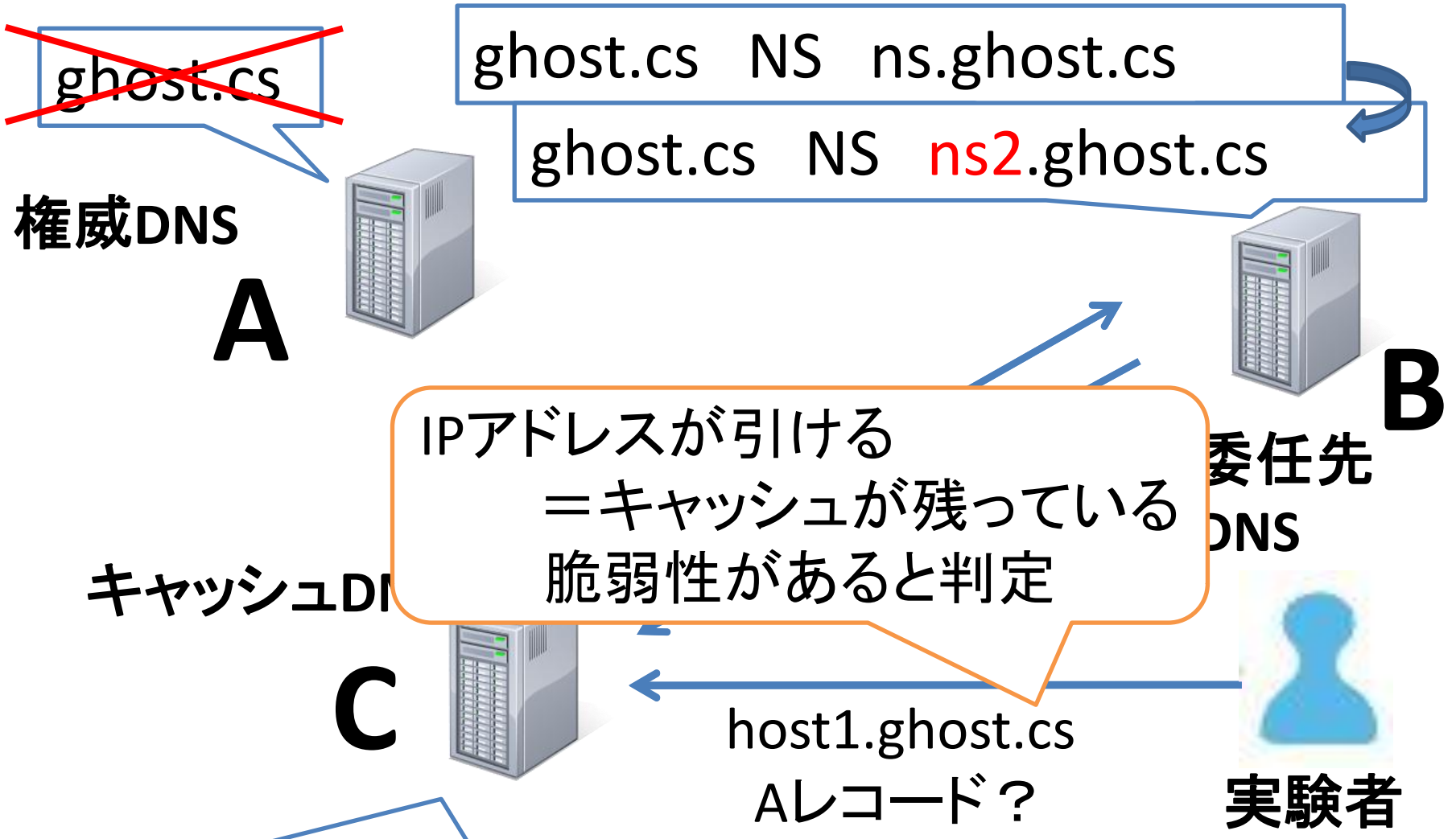
- public-dns.tkが公開しているパブリックDNSの2013年1月のデータベースを用いた
- 2791件について調査

IPv4/IPv6 Address	Hostname	Location	Software / Version	Checked at	State	Whois
67.159.206.12	ns1.forona.net	United States, Seattle	9.3.1	3 minutes ago	valid	Whois
67.158.135.243	ns2.icserv.net	United States, Rexburg	9.2.4	3 minutes ago	valid	Whois
67.138.100.3	ns2.clearvoicetel.com	United States, Meridian	9.4.3	3 minutes ago	valid	Whois
67.138.100.2	ns1.clearvoicetel.com	United States, Meridian	9.4.3	3 minutes ago	valid	Whois
67.128.48.2	ns.accesscom.net	United States, Houma	9.7.2-P2	3 minutes ago	valid	Whois
67.107.71.186	67.107.71.186.ptr.us.xo.net	United States, Fort Worth	9.2.4	4 minutes ago	valid	Whois
66.98.184.137	ns1.hospedaxe.com	United States, Houston	9.2.2	4 minutes ago	valid	Whois
66.9.5.15	ns-back.thirteen.org	United States, New York	9.3.6-P1-RedHat-9.3.6-16.P1.el5	4 minutes ago	valid	Whois
66.71.191.34	ns5.9netweb.it	United States, Parsippany	surely you must be joking	4 minutes ago	valid	Whois
66.70.189.93	ns.oscarbravo1.com	United States, Trumbull	9.2.2-P3	4 minutes ago	valid	Whois
66.7.219.42	ns2.pixnj.com	United States, Orlando	9.3.6-P1-RedHat-9.3.6-20.P1.el5	4 minutes ago	valid	Whois
66.7.212.210	ns25.manufrog.com	United States, Orlando	9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6	4 minutes ago	valid	Whois
66.7.208.125	ns2.ecoagencia.com	United States, Orlando	9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6	4 minutes ago	valid	Whois
66.7.205.41	ns2.dj4design.com	United States, Miami	9.2.4	4 minutes ago	valid	Whois
66.7.205.147	ns1.ecoagencia.com	United States, Miami	9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6	5 minutes ago	valid	Whois

Add new nameservers

Public DNS Servers by country


ghost.cs
ghost.cs NS ns.ghost.cs
ghost.cs NS ns2.ghost.cs
権威DNS
A
B
委任先
DNS
キャッシュDNS
C
host1.ghost.cs
ns2.ghost.cs
Aレコード？
実験者
ghost.cs 3600 IN NS ns2.ghost.cs
ghost.cs 1800 IN NS ns.ghost.cs

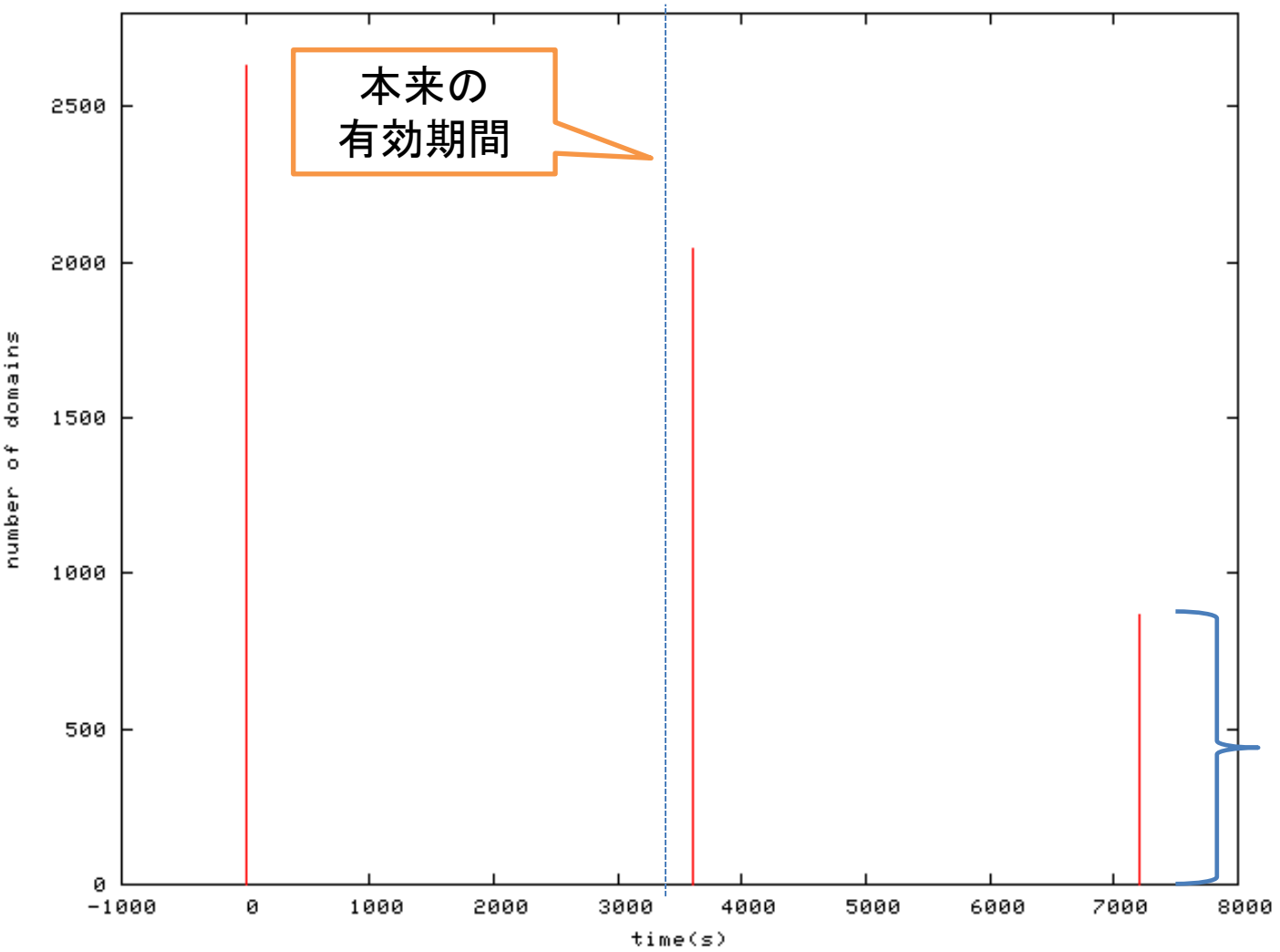

ghost.cs
ghost.cs NS ns.ghost.cs
ghost.cs NS ns2.ghost.cs
権威DNS
A
B
委任先
DNS
IPアドレスが引ける
＝キャッシュが残っている
脆弱性があると判定
キャッシュDN
C
host1.ghost.cs
Aレコード？
実験者
ghost.cs 1800 IN NS ns2.ghost.cs
ghost.cs 0 IN NS ns.ghost.cs

結果1　主要パブリックDNS

	IPアドレス	脆弱性
Google	8.8.8.8	なし
	8.8.4.4	なし
DNS Advantage	156.154.70.1	有
	156.154.71.1	有
OpenDNS	208.67.222.222	有
	208.67.220.220	有
Norton	198.153.192.1	有
	198.153.194.1	有
GTEI DNS	4.2.2.1	有
	4.2.2.2	なし

2時間後にはクリア

結果２　幽霊ドメイン生存数



ドメイン数

$\frac{800}{2700}$

生存期間(s)

結果3　国毎の割合

世界で二番目に危険

	DNS数	脆弱性有	割合
イタリア	74	27	0.365
日本	97	28	0.289
ベルギー	35	9	0.257
ドイツ	285	72	0.253
カナダ	38	9	0.237
中国	67	15	0.224
スウェーデン	509	108	0.212
アメリカ	888	180	0.203
オランダ	72	13	0.181
フランス	102	18	0.176
イギリス	212	33	0.156

実験4　DNSソフトウェア毎の割合

パッチ有

	総DNS数	脆弱性有	割合
bind 9.5以前	1169	1024	0.876
bind 9.6以降	412	268	0.650
Power DNS	45	32	0.711
unbound	8	4	0.500
dnsmasq	12	9	0.750

考察

- Google以外の主要パブリックDNSはキャッシュ更新を1回だけ許している
  - Bindを用いていないパッチを当てず
  - キャッシュの削除で対策
- 幽霊ドメインの生存数が1時間後2000,2時間後800と段階的に減っている
  - キャッシュの定期的な削除を行っている

考察

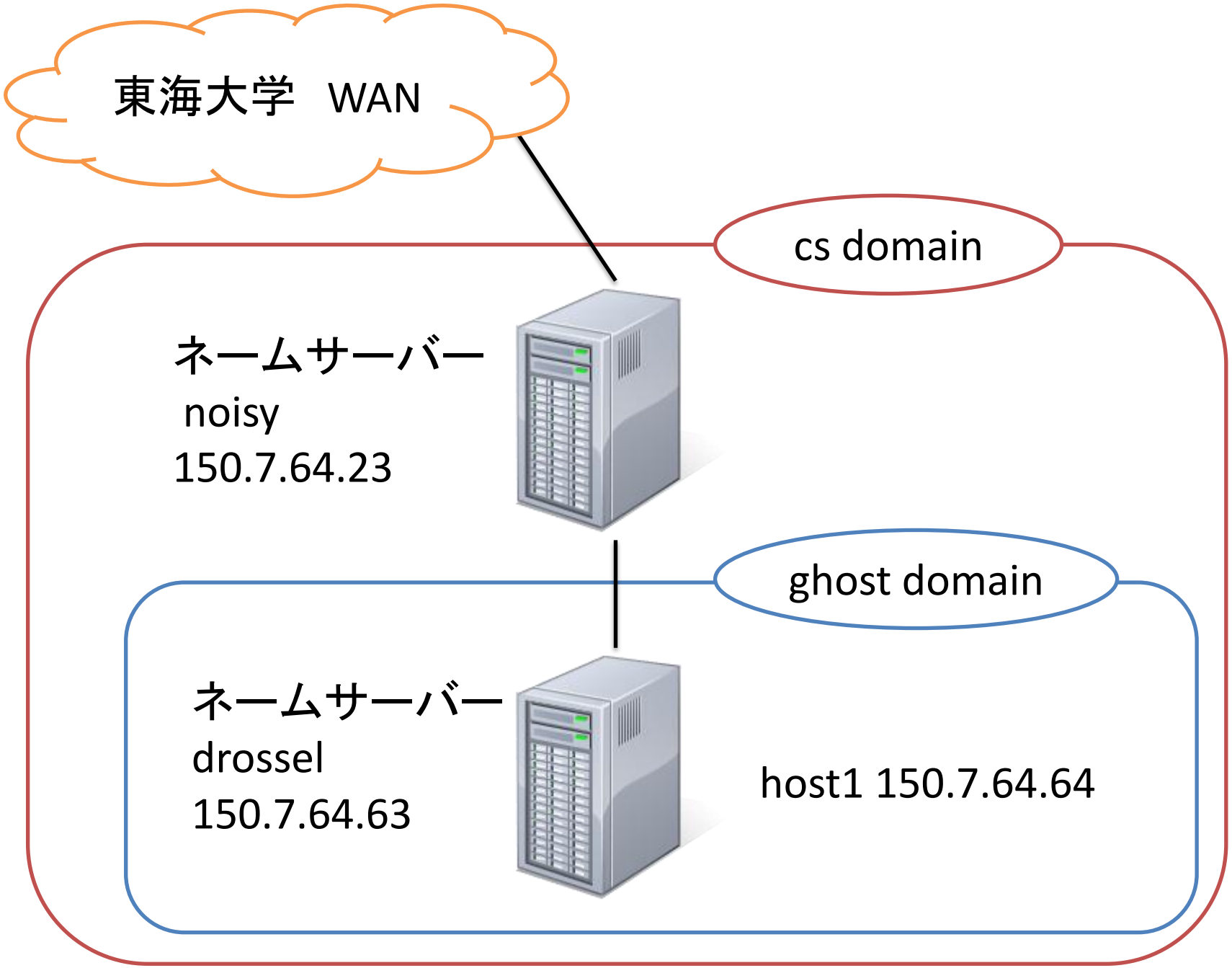
対応が遅れている理由

- 移植のコスト
- ソフトウェアの互換
- パッチがない（Bind9.6以降以外）
- 更新が面倒

まとめ

- パブリックDNSに脆弱性が2013年1月現在でも約3割残っていることを明らかにした
- 幽霊ドメイン脆弱性において日本が世界で二番目に危険な国であることを明らかにした
- 幽霊ドメイン脆弱性をついた攻撃を検知することを今後の課題とする

- ご清聴ありがとうございました


東海大学　WAN
cs domain
ネームサーバー
noisy
150.7.64.23
ghost domain
ネームサーバー
drossel
150.7.64.63
host1 150.7.64.64