DNSSEC普及状況アップデート
＋
ランダムサブドメイン攻撃検知手法の紹介

佐藤 一道*　　下田 晃弘**　　石橋 圭介**

*NTTコミュニケーションズ株式会社
**NTTネットワーク基盤技術研究所

自己紹介

- 2008年4月
  - NTT研究所入社
- 2008年～2012年ごろまで
  - DNSトラフィックトレンド分析
  - マルウェア感染端末/悪性サイト検知技術の開発
- 2012年～2013年ごろまで
  - セキュリティログ分析基盤(SIEM)の開発
- 2013年～2014年ごろまで
  - インターネット構造分析技術の開発
  - DNS Amp攻撃/ランダムサブドメイン攻撃検知技術の開発
- 2014年～2015年5月まで
  - QoE(ユーザ体感品質)に基づいた動画配信制御技術の開発
- 2015年6月～
  - NTTコミュニケーションズへ転籍
  - サーバ/NW機器の監視システムの開発/保守/運用に従事

本日のお品書き

- DNSSEC普及状況アップデート
  - 人気WebサイトTOP100万のドメイン名のDNSSEC対応状況を調査
  - DNS Summer Days 2013[1]/2014[2]で発表された分析結果を更にアップデート
    - ✓ 2013で佐藤が調査状況を報告
    - ✓ 2014で大本さんがアップデート!!ありがとうございます!!
- ランダムサブドメイン攻撃検知手法の紹介
  - 2014年2月ごろから発生している、DNSサーバへのDDoS攻撃に利用されているドメイン名を効率よく検知する手法のご紹介

[1] http://dnsops.jp/event/20130718/20130718-dnssec-sato-1.pdf
[2] http://dnsops.jp/event/20140627/SummerDays2014ohmoto.pdf

DNSSEC普及状況調査

はじめに(2013年の再掲)

- DNSSECの”真の普及”とは?
  - 1. 多くのユーザが利用している有名ドメイン名が、DNSSEC対応すること
    - ✓ Google、Facebook、Twitterなど
  - 2. 多くのユーザが利用しているキャッシュサーバが、DNSSEC検証機能をONにすること

ということで

- 下位ゾーンのDNSSEC対応状況を調査
  - 人気Webサイトのドメイン名のDNSSEC対応状況を調査し、DNSSECの”真の普及”状況を明らかにする
- キャッシュサーバの検証機能のON/OFF状況を調査
  - DNSSEC Validatorの普及状況を調査

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

調査概要

- 人気WebサイトTop100万のドメイン名に対して名前解決を実施し、その応答を分析
  - 署名付ドメイン名数
  - 署名付ドメイン名のTLD数分布

- 署名付ドメイン名のDNSSEC検証結果を分析
  - Secure数
  - Insecure+Bogus数

データセット

- 人気Webサイトリスト
  - Alexa Top100万リストを利用
    - ✓ 2015年7月12日に取得したデータを利用
- 名前解決およびDNSSEC検証結果データ
  - DNSSEC検証機能をONにしたUnboundを用意
    - ✓ 7月なので
  - $ dig +dnssec @localhost ドメイン名 {A|DS|DNSKEY}で名前解決を実施
    - ✓ drillを使わなかった理由は特にありません。。。
  - tcpdumpでパケットキャプチャ
    - ✓ pcap大好きです

おまけ: Alexaリストの詳細

人気ランキング

- 人気ランクTOP20に大きな変動はない
  - 2015年ではebay.com、yandex.ruが新たに出現
- jpドメインは2015年ではYahoo!、Googleのみ

順位	2014年6月	2015年7月
1	google.com	google.com
2	facebook.com	facebook.com
3	youtube.com	youtube.com
4	yahoo.com	baidu.com
5	baidu.com	yahoo.com
6	wikipedia.org	amazon.com
7	qq.co	wikipedia.org
8	taobao.com	qq.com
9	live.com	twitter.com
10	twitter.com	taobao.com

順位	2014年6月	2015年7月
11	amazon.com	google.co.in
12	linkedin.com	live.com
13	google.co.in	sina.com.cn
14	sina.com.cn	linkedin.com
15	hao123.com	weibo.com
16	blogspot.com	yahoo.co.jp
17	weibo.com	google.co.jp
18	tmall.com	ebay.com
19	sohu.com	yandex.ru
20	yahoo.co.jp	blogspot.com

出現TLD数ランキング

- 依然としてcomがリストの半数以上を占める
- jpは6位と変わらない
- com、deの出現数が減少し、その他のTLDの出現数が若干増加しているが、要因は不明

順位	2014年6月		2015年7月	
	TLD	出現数	TLD	出現数
1	com	524,927	com	506,556
2	net	50,855	net	50,423
3	ru	39,121	ru	43,308
4	org	38,276	org	42,225
5	de	34,041	de	28,317
6	jp	19,326	jp	22,230
7	uk	19,148	br	19,463
8	br	17,137	uk	18,115
9	pl	13,604	in	16,561
10	fr	13,421	pl	14,291

順位	2014年6月		2015年7月	
	TLD	出現数	TLD	出現数
11	it	12,555	it	12,892
12	in	12,204	fr	12,494
13	info	10,464	cn	10,907
14	cn	9,209	info	10,625
15	au	8,168	ir	9,712
16	nl	8,061	au	8,995
17	es	7,693	nl	8,390
18	ir	7,327	es	7,210
19	eu	5,010	kr	5,690
20	ca	4,842	gr	5,184

出現新gTLDドメイン名ランキング

- 新gTLDドメインのランクは最上位でも1,788位であり人気サービスが出現したとは言えない

順位	2015年7月
1,788	searchengines.guru
2,452	gidonline.club
2,778	namu.wiki
2,944	songspk.link
3,606	udacha.club
4,180	trending.report
4,300	securetracking.link
5,704	mabanque.bnpparibas
5,766	altadefinizione.gratis
7,561	opensubtitles.website

順位	2015年7月
8,987	giveaways.club
9,235	genial.guru
9,324	buzzit.club
9,539	sushis.kim
9,766	ptc.onl
10,714	e-reading.club
11,549	kodi.wiki
11,606	seventorrents.xyz
11,694	couponcouponcoupon.club
11,716	animeid.moe

出現新gTLD数ランキング

- 新gTLDの出現数は最大でも430個であり、普及しているとは言えない

順位	2015年7月	
	TLD	出現数
1	club	430
2	xyz	353
3	link	225
4	dev	225
5	website	147
6	today	133
7	top	104
8	guru	92
9	work	87
10	ninja	85

順位	2015年7月	
	TLD	出現数
11	rocks	77
12	click	72
13	science	68
14	media	68
15	tokyo	62
16	sexy	55
17	space	53
18	wang	43
19	life	43
20	pics	37

DNSSEC普及状況分析結果

Alexa Top 100万リスト名前解決結果

- NXDomain、ServFail、その他の項目数が大きく減少
  - リストの質が変わった可能性があるが、原因は不明

	2013年5月	2014年6月	2015年7月
NoError	959,252	978,834	995,390
NXDomain	18,113	15,964	1,447
ServFail	1,361	1,743	3,163
その他	21,274	3,459	0
合計	1,000,000	1,000,000	1,000,000

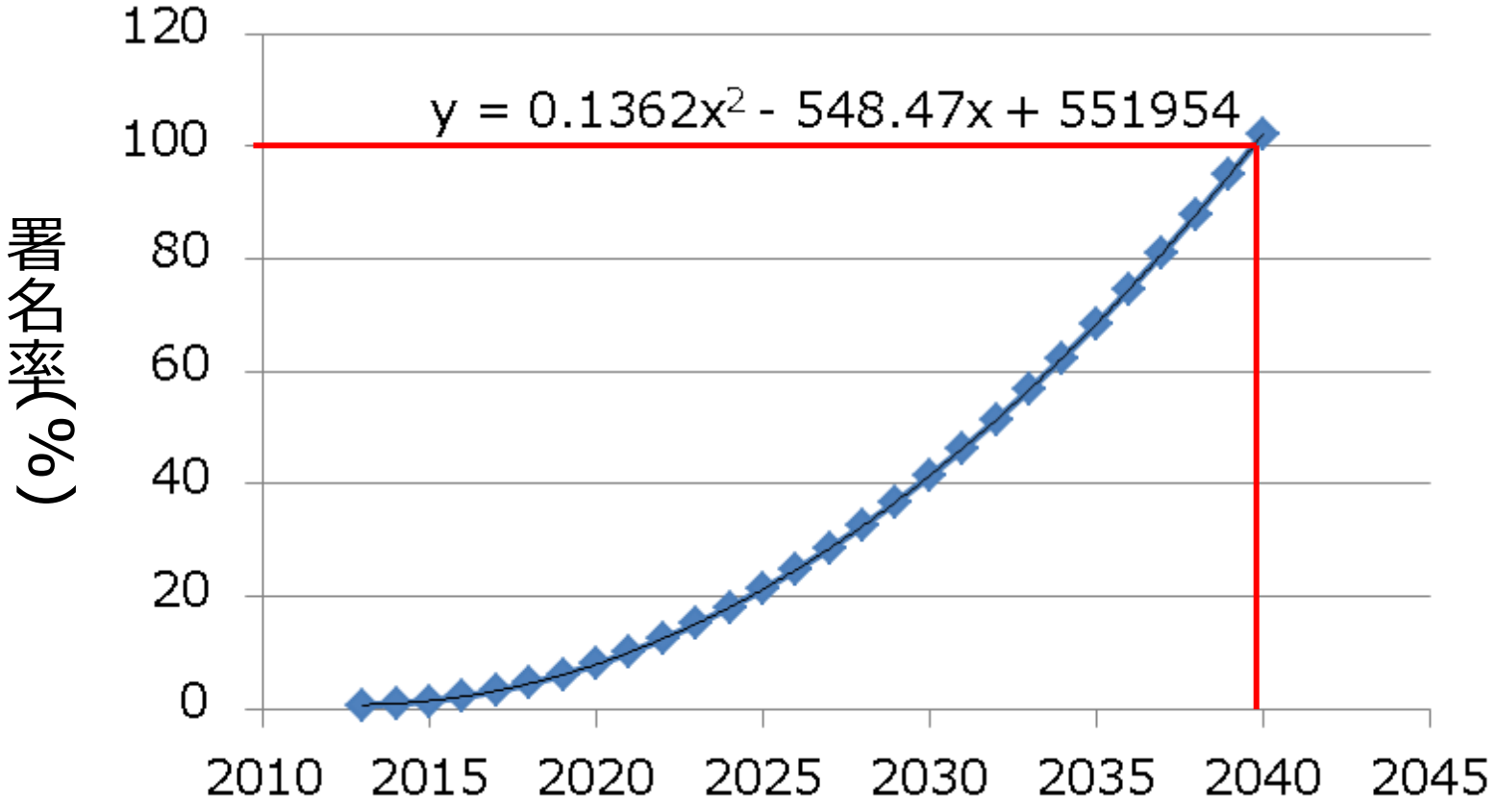
DNSSEC対応済ドメイン名数

- 署名付ドメイン名数は順調に増加
  - 署名付ドメイン名数の増加率が増加している
- 署名付増加数 ≒ Secure増加数であり、かつInsecure/Bogus数はほぼ変化していない
  - 導入方式、運用がこなれてきた?

ドメイン名数	2013年5月	2014年6月	2015年7月
署名済 (割合)	7,636 (0.76%)	9,766 (0.98%)	14,621 (1.46%)
Secure (割合)	5,827 (0.58%)	7,868 (0.79%)	12,704 (1.27%)
Insecure+Bogus (割合)	1,809 (0.18%)	1,898 (0.19%)	1,917 (0.19%)

おまけ: 目指せ署名率100%

- このままいくと、署名率が100%になるのは2040年頃
  - DNSはまだあると思います
  - 2013年から2015年までの3データのみからの予測なので眉唾です



Secureドメイン名ランキング

- 最もランクの高いSecureドメイン名は3年連続paypal.com
- Secureドメイン名に有名サービスが含まれていない傾向が続いている
- 権威サーバ側のDNSSEC対応はまだ進んでいない

2013年5月		2014年6月		2015年7月	
順位	ドメイン名	順位	ドメイン名	順位	ドメイン名
53	paypal.com	43	paypal.com	43	paypal.com
174	mozilla.org	141	mozilla.org	210	mozilla.org
191	comcast.net	284	comcast.net	226	nih.gov
340	domaintools.com	324	nih.gov	262	comcast.net
369	nih.gov	649	ca.gov	293	xfinity.com
767	ca.gov	865	comcast.com	772	weather.gov
858	irs.gov	978	irs.gov	781	usaa.com
1,076	comcast.com	1,103	wheather.gov	945	state.gov
1,124	state.gov	1,150	state.gov	998	stanford.edu
1,203	weather.gov	1,170	noaa.gov	1,090	ed.gov

TLDごとの普及状況

- 全体の傾向として、署名率、Secure率は微増傾向
  - 少しずつではあるが、DNSSECの導入が進んでいる?
- 署名率、Secure率共に高いのはcz、nl、gov、およびdev
  - 特にdevは両方100%!

TLD	出現数(A)		署名付ドメイン名数(B)		Secureドメイン名数(C)		署名率(B÷A)		Secure率(C÷B)	
	2014年	2015年	2014年	2015年	2014年	2015年	2014年	2015年	2014年	2015年
com	524,927	506,556	2,203	3,042	1,573	2,247	0.42%	0.60%	71.40%	73.87%
nl	8,061	8,390	1,719	2,497	1,620	2,388	21.32%	29.76%	94.24%	95.63%
cz	4,631	4,817	1,506	1,623	1,441	1,565	32.52%	33.69%	95.68%	96.43%
br	17,137	19,463	962	1,331	951	1,318	5.61%	6.84%	98.86%	99.02%
se	3,460	3,240	923	871	417	683	26.68%	26.88%	45.18%	78.42%
no	--	2,381	--	820	--	804	--	34.44%	--	98.05%
fr	13,421	12,494	372	565	351	540	2.77%	4.52%	94.35%	95.58%
gov	858	1,077	355	410	349	400	41.38%	38.07%	98.31%	97.56%
net	50,855	50,423	260	387	188	293	0.51%	0.77%	72.31%	75.71%
org	38,276	42,225	259	341	170	245	0.68%	0.81%	65.64%	71.85%
jp	--	22,230	--	341	--	339	--	1.53%	--	99.41%
dev	--	225	--	225	--	225	--	100.00%	--	100.00%
eu	5,010	4,594	167	224	139	196	3.33%	4.88%	83.23%	87.50%
us	--	2,536	--	224	--	224	--	8.83%	--	100.00%
pl	13,604	14,291	125	202	117	180	0.92%	1.41%	93.60%	89.11%
de	34,041	28,317	87	172	69	137	0.26%	0.61%	79.31%	79.65%
be	2,984	2,580	90	109	70	93	3.02%	4.22%	77.78%	85.32%
edu	2,342	3,074	73	84	58	69	3.12%	2.73%	79.45%	82.14%
tw	--	4,697	--	78	--	68	--	1.66%	--	87.18%
pt	--	1,735	--	69	--	60	--	3.98%	--	86.96%

Validatorの普及状況

- 調査方法
  - Verisignlabsの調査データをもとにValidator普及状況を調査
  - http://validator-search.verisignlabs.com

- 調査結果
  - 2014年からValidatorの普及率はほぼ変化なし
  - Validator側の普及は進んでいない

	2012年9月 (データ公開時)	2014年6月 (大本さん調査)	2015年7月
普及率	3.66%	4.56%	4.76%

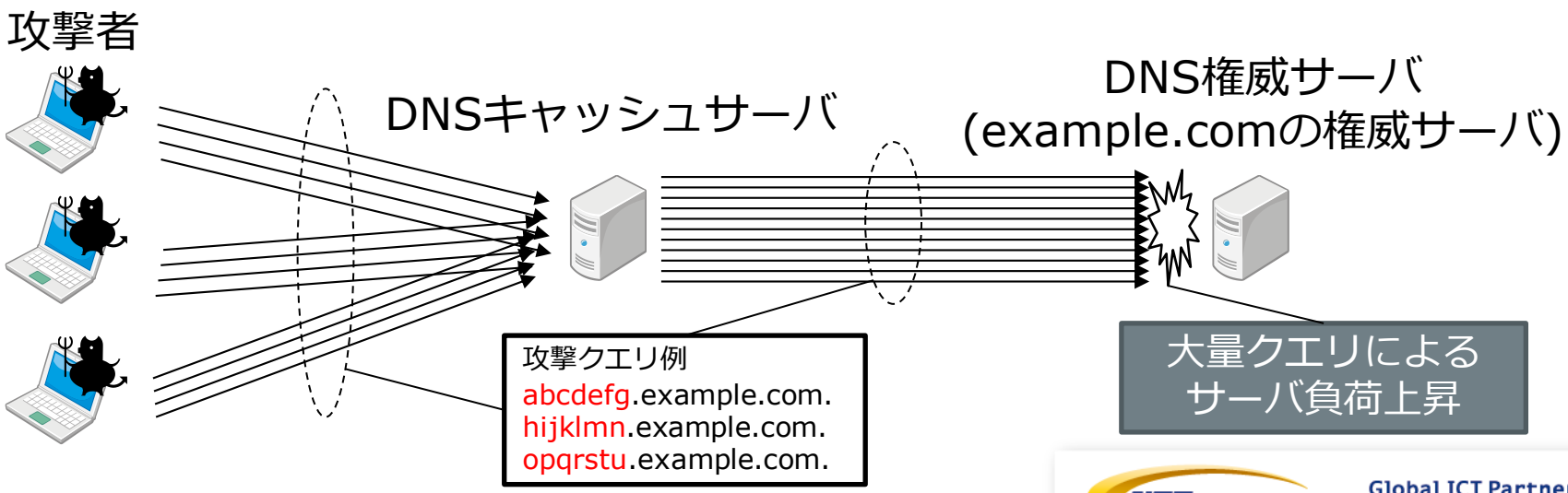
まとめ

- Alexa Top 100万リストをベースにDNSSEC対応状況を調査
  - 人気のあるSecureドメイン名は2013年から引き続きplaypal.com、mozilla.org
  - ただし、有名サービスのDNSSEC対応は進んでいない
  - TLD別にみると、nl、cz、gov、devのDNSSEC対応が進んでいる
- Verisignlabs公開データによるのValidator普及率を調査
  - Validatorの普及率は2014年から横ばいであり、普及は進んでいない
- 調査の結果、DNSSECの”真の普及”は依然として進んでいないと考えられる

ランダムサブドメイン攻撃検知手法

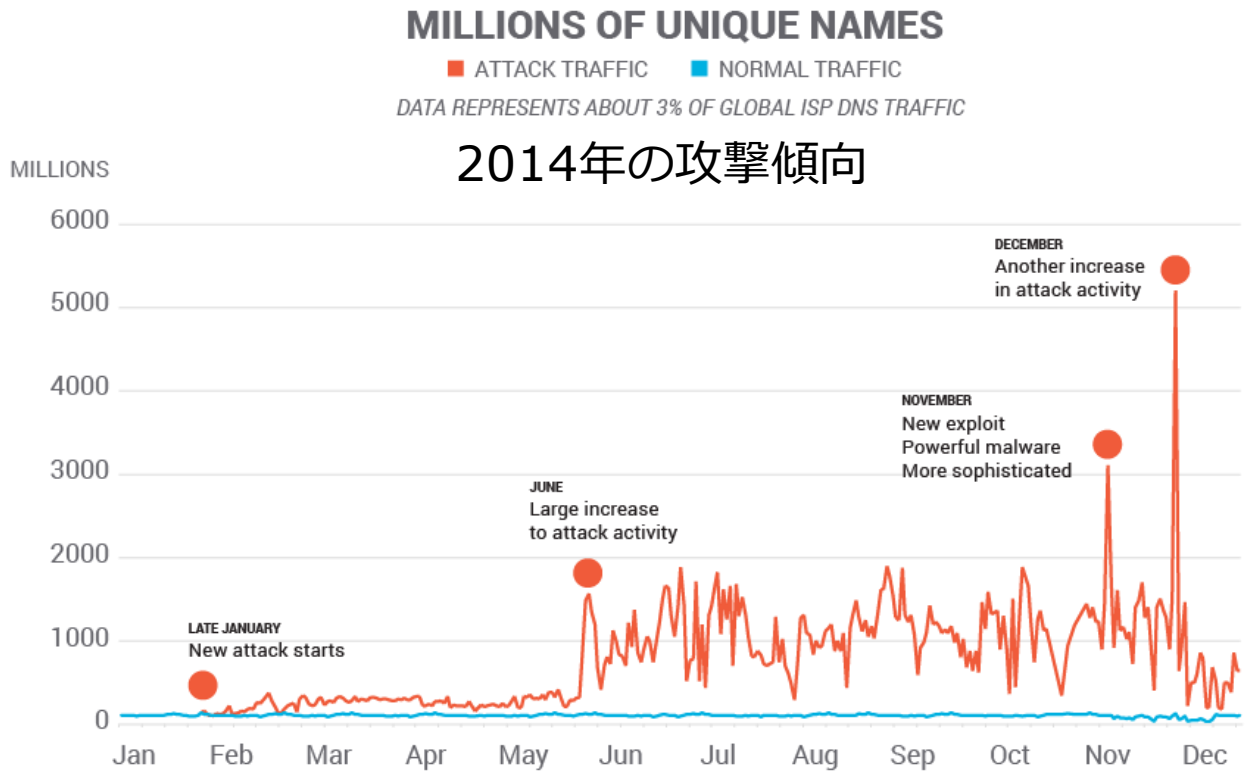
ランダムサブドメイン攻撃とは？

- 攻撃の目的
  - DNS権威サーバの負荷上昇を狙ったDDoS攻撃だと考えられる
- 攻撃手法
  - 1. <ランダム文字列>.example.comのような大量クエリを、DNSキャッシュサーバへ送信する
  - 2. DNSキャッシュサーバから権威サーバへ大量クエリが送信される
  - 3. 大量クエリによりexample.comのDNS権威サーバが後負荷になり、当該ドメインを利用したサービスが停止する
- 送信元
  - オープンリゾルバまたはボット



攻撃の傾向

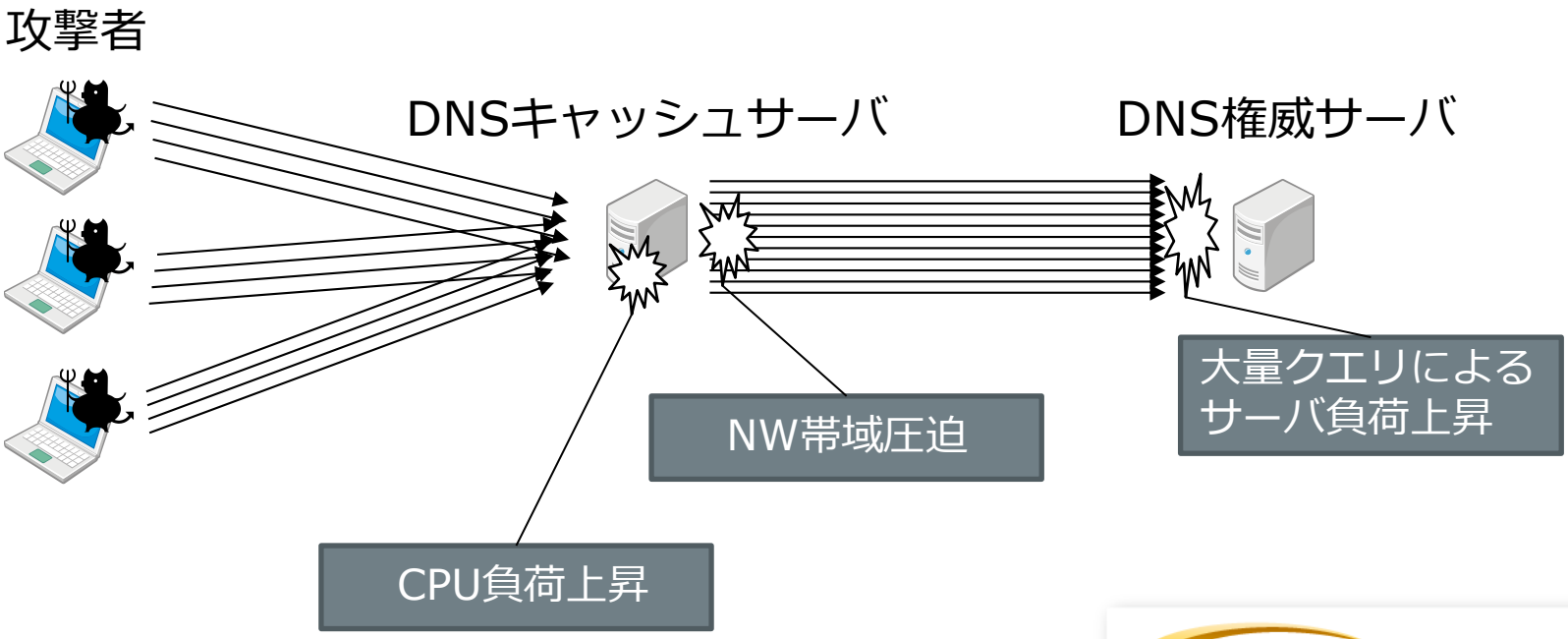
- nominum社の調査[3]によると、2014年2月頃から攻撃が観測されている
- 2015年現在、多少落着きつつあるものの、依然として攻撃は観測され続けている



[3] https://indico.dns-oarc.net/event/21/contribution/29/material/slides/0.pptx

攻撃の影響範囲

- ランダムサブドメイン攻撃による影響は、DNS権威サーバのみならず、キャッシュサーバにも及ぶ
  - CPU負荷上昇
  - NW帯域の圧迫
- キャッシュサーバ側でも何らかの防御策を講じる必要がある



有効な防御策(の1つ)

- キャッシュサーバ側で攻撃対象ドメイン名の応答制御を行う方式
  - ただし、正規ドメイン名は救い、攻撃利用ドメイン名のみ制御するよう注意する必要がある
    - ✓ www.example.comの応答は正規ドメイン名として正しい応答を行う
    - ✓ *.www.example.comは偽の応答を返す

- 課題
  - 制御対象の攻撃利用ドメイン名の特定が困難
    - ✓ 通常のDNSサーバ監視では個々のドメイン名までは見ないため、異常が発生した際に、どのドメイン名を制御すれば良いか分からない

本発表では、効率的に攻撃に利用されているドメイン名を特定する技術を紹介する

攻撃検知手法のアイデア

- ランダムサブドメイン攻撃を検知するためには、ゾーンごとの出現サブドメイン数を数えればよい
  - サブドメイン数が多いゾーンは攻撃されているという発想

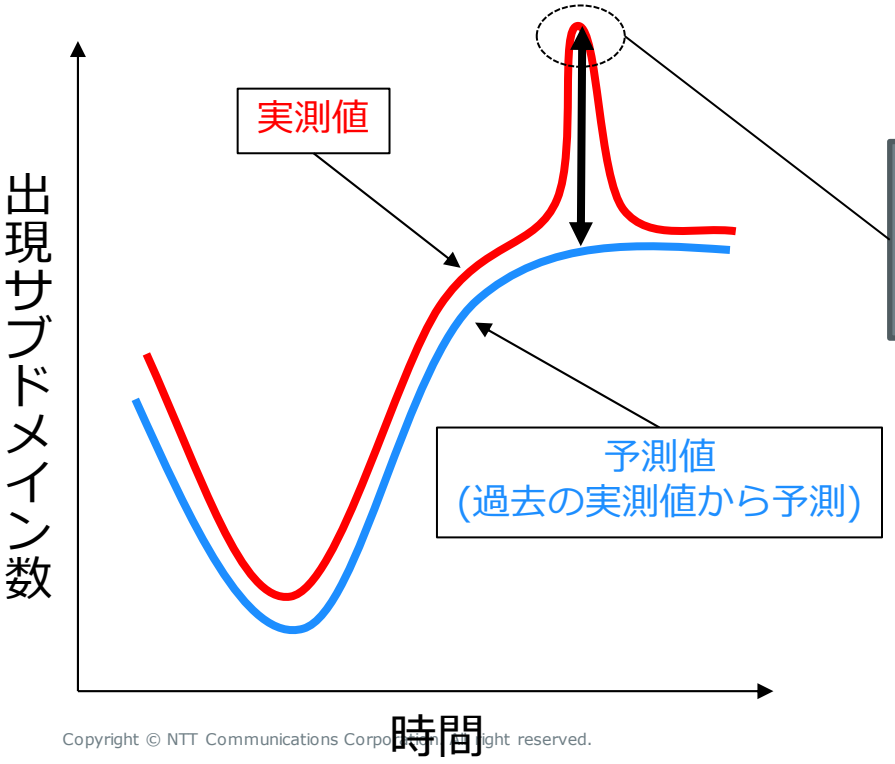
- ただし、単純な閾値検知では誤検知が発生する可能性が高い
  - GoogleやAmazonなどは大量のサブドメインを運用
  - その他にもアンチウィルスソフトウェアベンダ、Webホスティング事業者など、大量のドメイン名を運用している事業者は多く存在

ということで

- 誤検知回避のため、サブドメイン数の時系列変化を分析する
  - 攻撃の場合、出現サブドメイン数が急増するはず
  - 非攻撃の場合、出現サブドメイン数の増減幅は小さいはず

攻撃検知手法の詳細

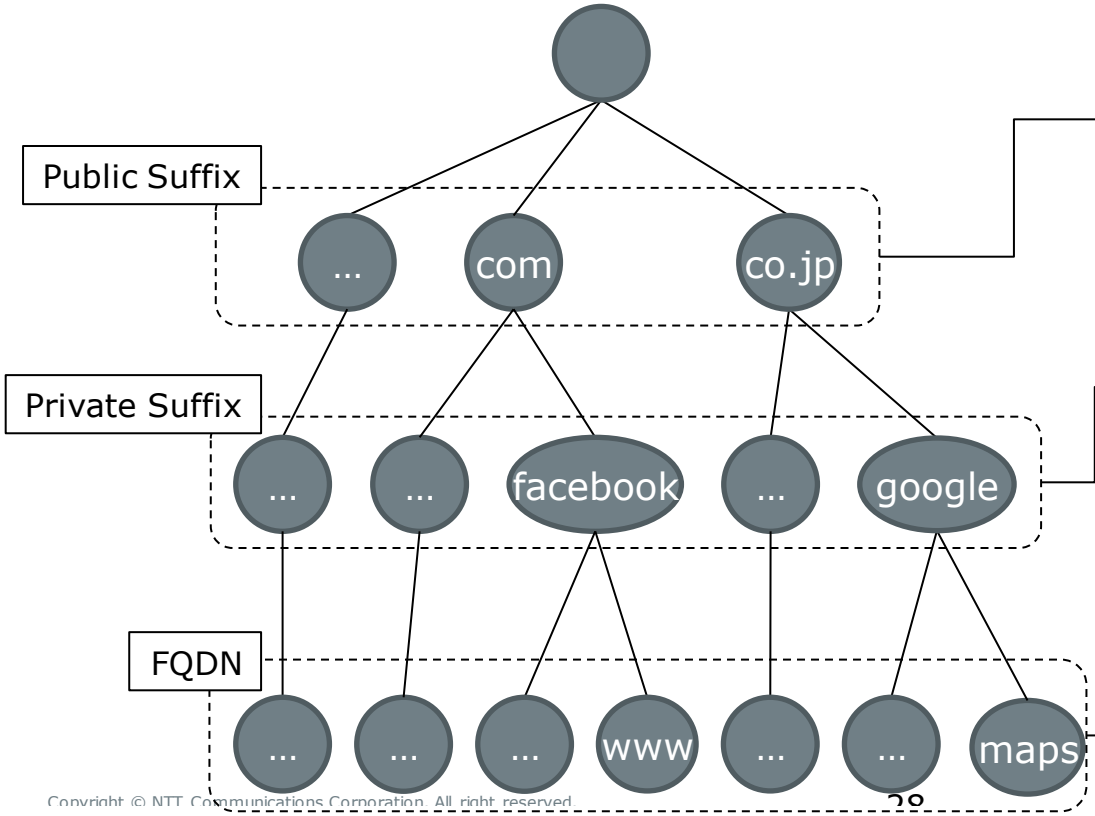
- ゾーンごとに出現サブドメイン数の時系列情報を保持しておき、次回出現数の予測値を計算
- 実測値と予測値に大きな乖離があった場合、攻撃として検知する
- ただし、全ゾーンの時系列分析は計算機の資源(CPU/メモリ)的に厳しいため、効率的な計算方法を検討する必要がある



出現サブドメイン数の予測値と実測値が閾値以上のとき、攻撃ありと判定する

(前職で)開発した技術(1/2)

- DNS木構造に基づくDNSトラフィック統計情報保持・参照技術
  - ユーザのインターネットサービス利用動向把握を目的とした技術
  - 国/分野、事業者、サービスごとにパケット数、利用ユーザ数などのトラフィック統計情報を算出



Public suffix	パケット数	下位ノード数	・・・
co.jp	・・・	・・・	・・・
com	・・・	・・・	・・・
・・・	・・・	・・・	・・・

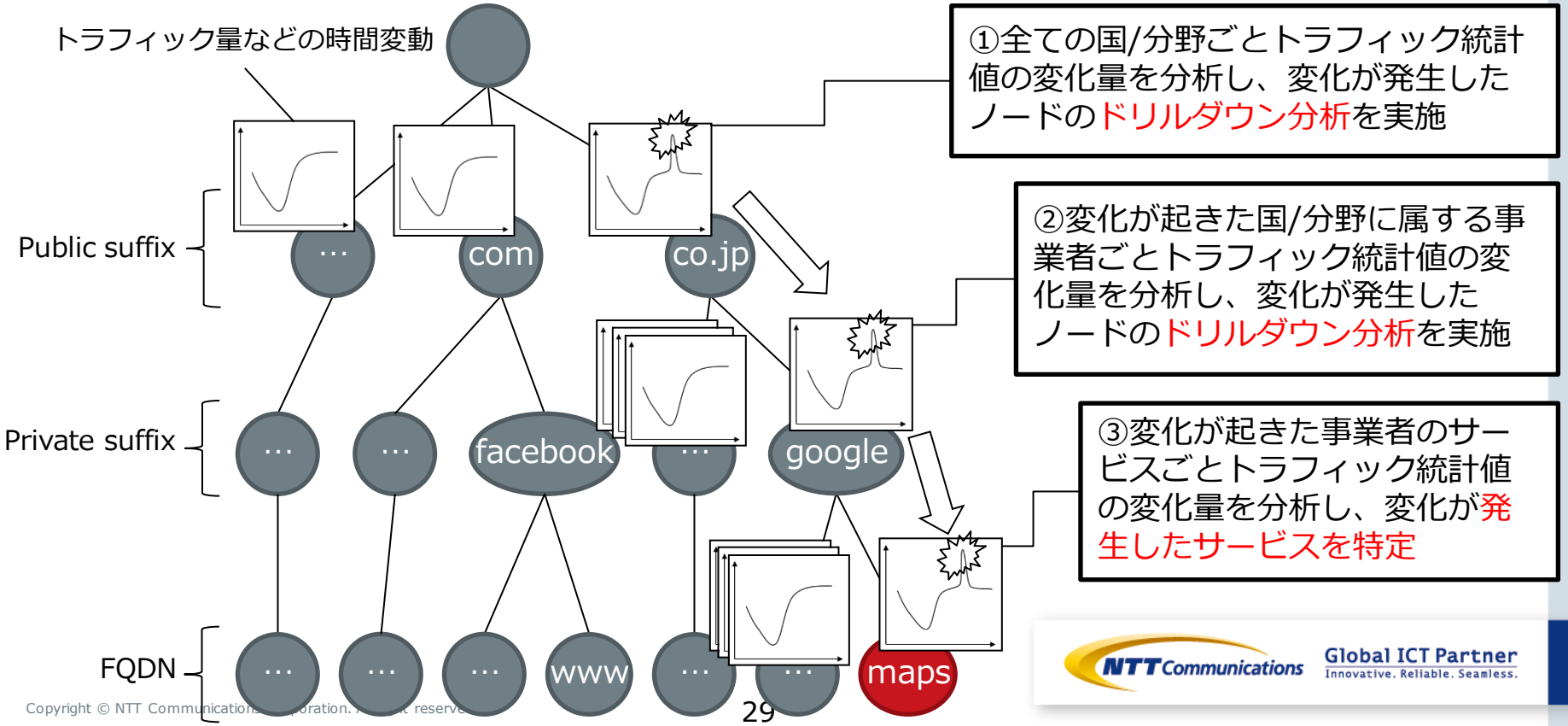
Private suffix	パケット数	下位ノード数	・・・
google.co.jp	・・・	・・・	・・・
facebook.com	・・・	・・・	・・・
twitter.com	・・・	・・・	・・・
・・・	・・・	・・・	・・・

FQDN	パケット数	下位ノード数	・・・
maps.google.co.jp	・・・	・・・	・・・
www.google.co.jp	・・・	・・・	・・・
www.facebook.com	・・・	・・・	・・・
search.twitter.com	・・・	・・・	・・・
・・・	・・・	・・・	・・・

*private suffixはpublic suffixの1つ下位のラベルまで含めたドメイン

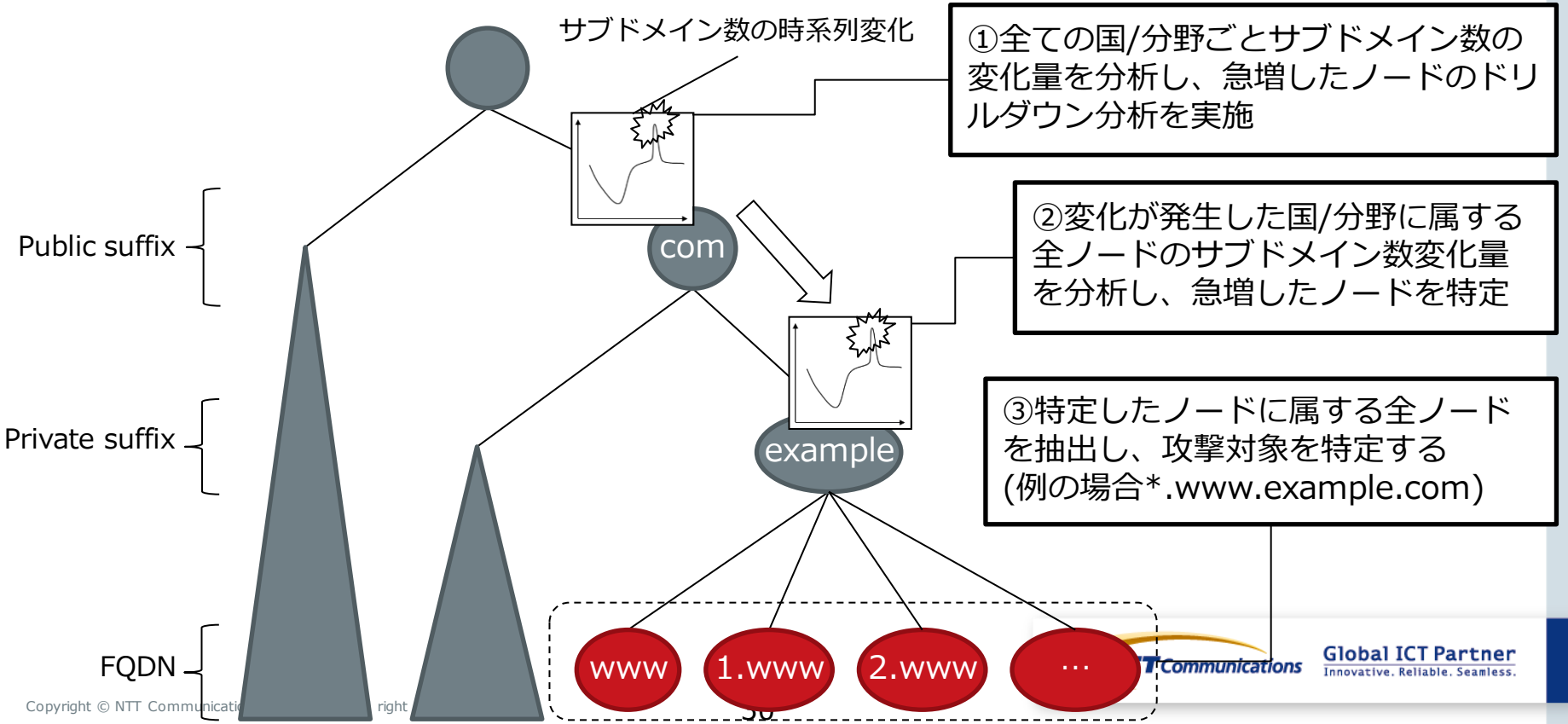
(前職で)開発した技術(2/2)

- DNSツリー構造に基づくDNSトラフィック変化検知技術を開発
  - トラフィック統計情報の時系列分析とDNS木構造のドリルダウン分析により、効率的なトラフィック変化分析が可能

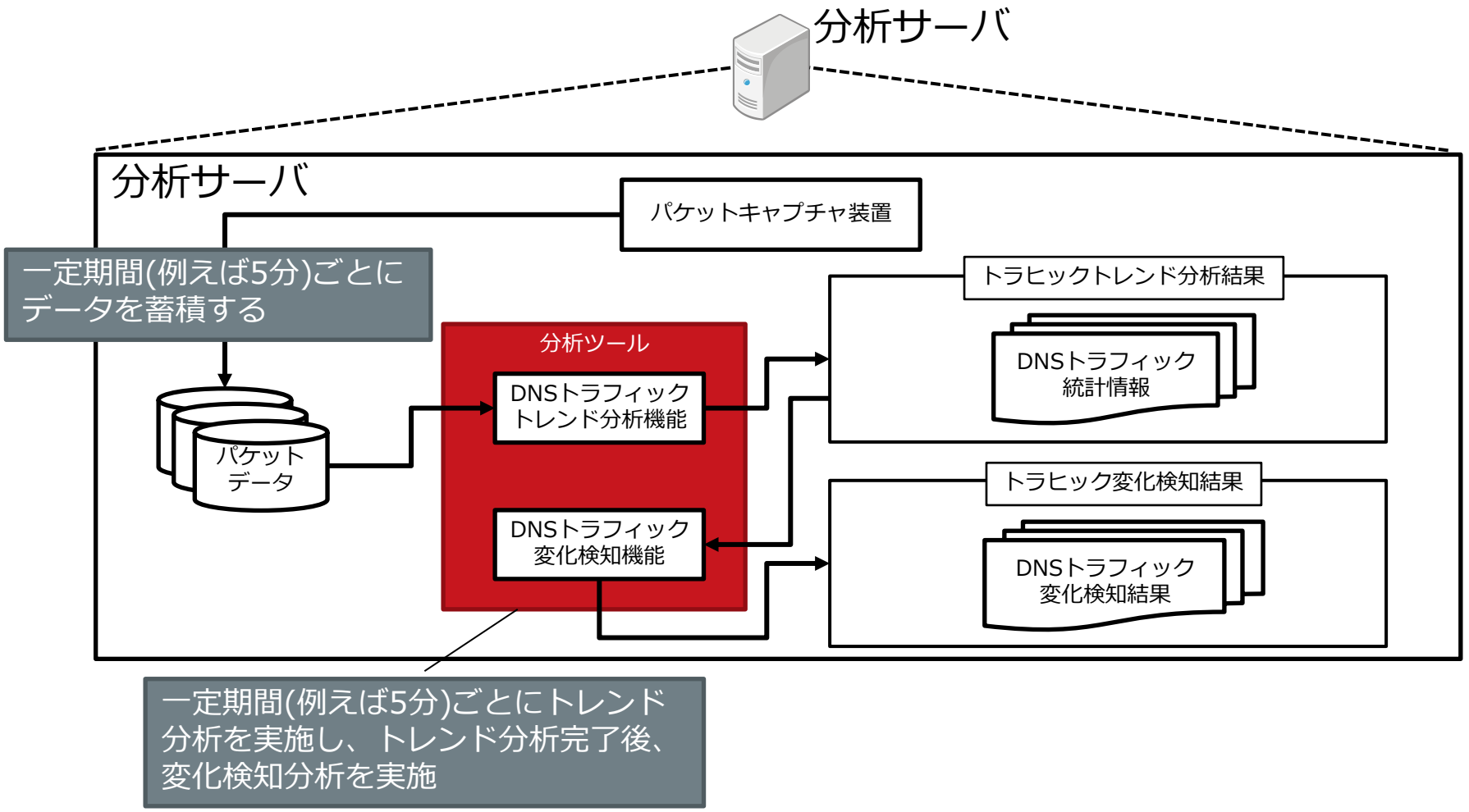


DNSトラフィック変化検知技術を用いた攻撃検知手法

- 攻撃利用ドメイン名検知への適用
  - DNSトラフィック変化検知技術を用いてサブドメイン数監視を行うことで攻撃対象を特定することができる
- 具体的な監視項目
  - Private suffix階層における、サブドメイン数監視



本技術の利用形態



評価結果の簡単な紹介

- 入力データ
  - 攻撃トラフィックと通常トラフィックが両方含まれた、2日分のDNSトラフィックデータ
- 分析環境
  - Linux/Intel Xeon X5650 x 2/192GB ram
    (メモリは若干オーバースペック気味、最低要件ではない)
- 検知精度
  - 2日間で約80回攻撃を検知、誤検知は0(目視で確認)
- 処理性能
  - 1,500万パケット/5分のデータを5分以内に処理可能
    (当然、分析環境に大きく依存)

まとめ

- ランダムサブドメイン攻撃のターゲットは権威サーバであると思われるが、キャッシュサーバにも影響を及ぼす
- キャッシュサーバでの応答制御を行うなど、何らかの対処が必要
- ランダムサブドメイン攻撃の対象ゾーンを特定するための技術を開発
  - DNSの木構造を用いたDNSトラフィック統計情報の時系列分析手法
- 評価の結果、高精度、高効率に攻撃を検知できることを確認