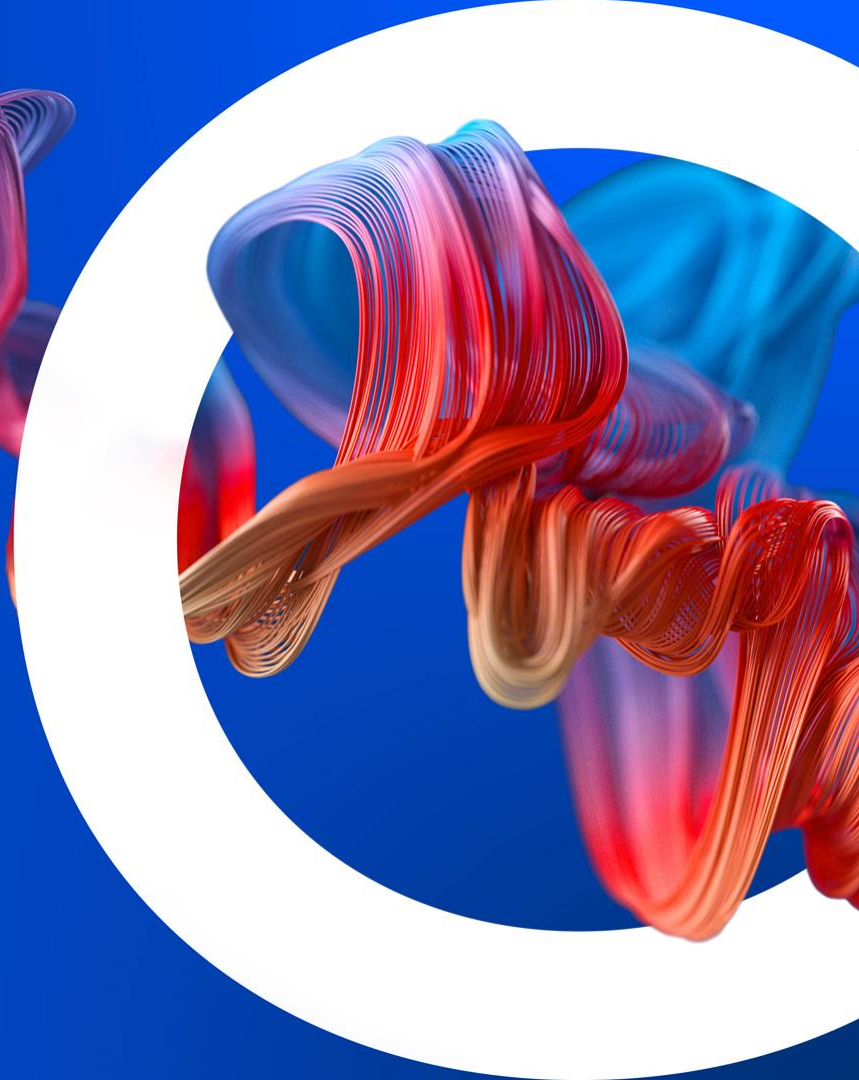
DDoS最前線
DDoSトラフィックの変化と課題

2024/01/18

ノキアソリューションズアンドネットワークス合同会社



自己紹介

- 名前: 石井俊行 (Ishii Toshiyuki)
- 所属: ノキアソリューションズ&ネットワークス合同会社
  IP製品部門 シニアソリューションアーキテクト
- Janog参加歴: Janog21(2008年)@熊本～
- Email toshiyuki.ishii@nokia.com

目次

1. 概要
2. DDoSの変化と現在
3. DDoS対策の最適解とは？
4. まとめ・議論

1.概要

なぜ Nokia が DDoS?

End To Endでモバイル/固定/ISP/データセンタ/エンタープライズあらゆるネットワークソリューションを提供しています

DDoSトラフィックに対してはフローコレクターをベースとしたインターネット観測技術を開発し、また10年以上にわたり世界各国のコラボレーション企業と協力しながらインターネットトラフィックの実情を分析しています

1.概要

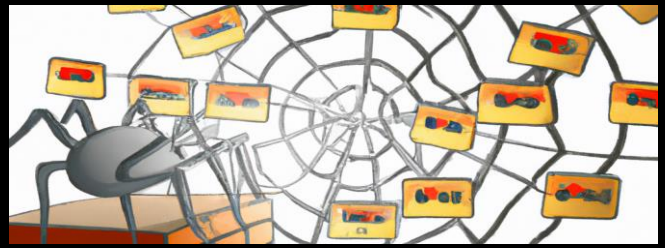
どうやってDDoS観測をしている？
1:自発的に探す(Nokia開発)

Deepfield Genome

世界中のすべての IPv4 とアクティブな IPv6 をクロール

Deepfield Secure Genome

Deepfield Cloud Genome®

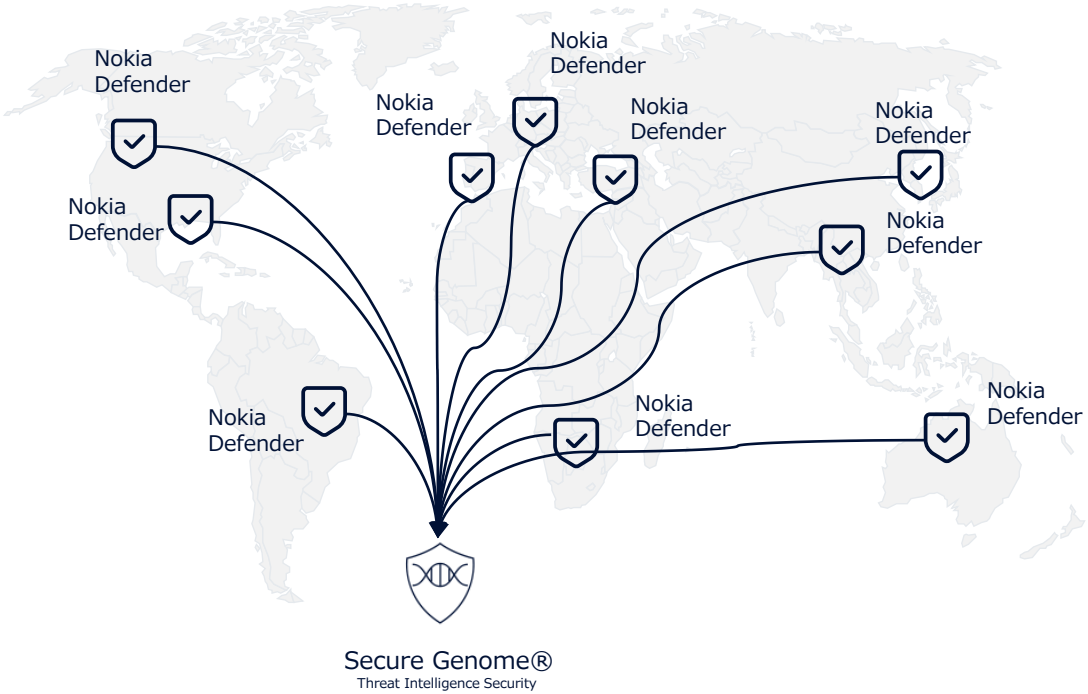


OTT サービス、アプリケーション、CDN、ISP、サーバー、ホスティング、既知のボットネット
CVE 、誤設定、脆弱なサーバー、アプリケーション、デバイス
IoT デバイスの種類、侵害されたサーバー、アクティブなボット メンバー
などを検出

1.概要

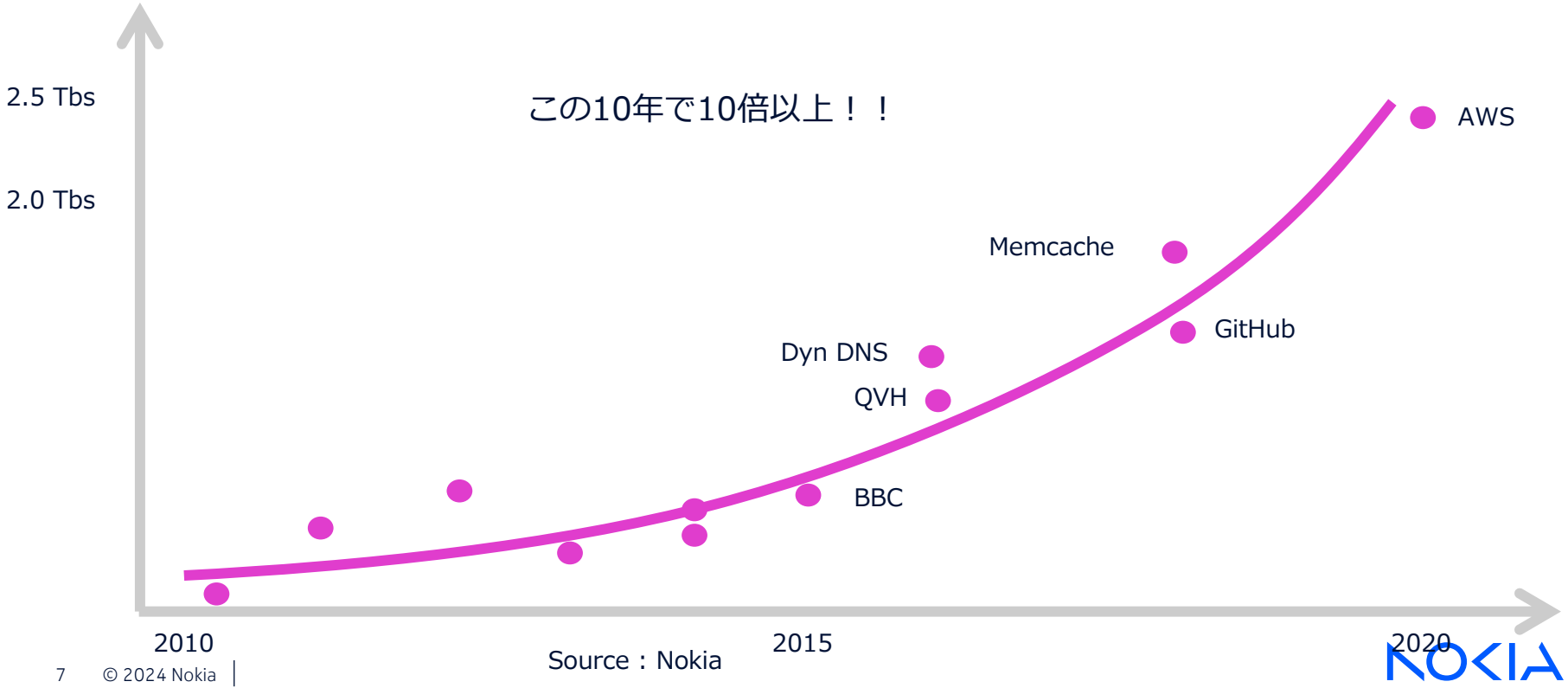
どうやってDDoS観測をしている？
2:世界中の協力企業から情報を集める

- 任意メンバーシップ (オプトイン)
- プライバシーと匿名性を念頭に置いて構築
  - EU GDPRなど
- 攻撃のメタデータ/特性を追跡
  - 攻撃元 IP、上位ベクトルなど
  - 匿名性を保証するため、攻撃を受けている IP は除外
- Nokia Deepfield Secure Genome を強化し、世界中の DDoS トラフィックを発信するボットネットを特定



2.DDoSの変化と現在

DDoSトラフィックの変遷



Source：Nokia

2.DDoSの変化と現在

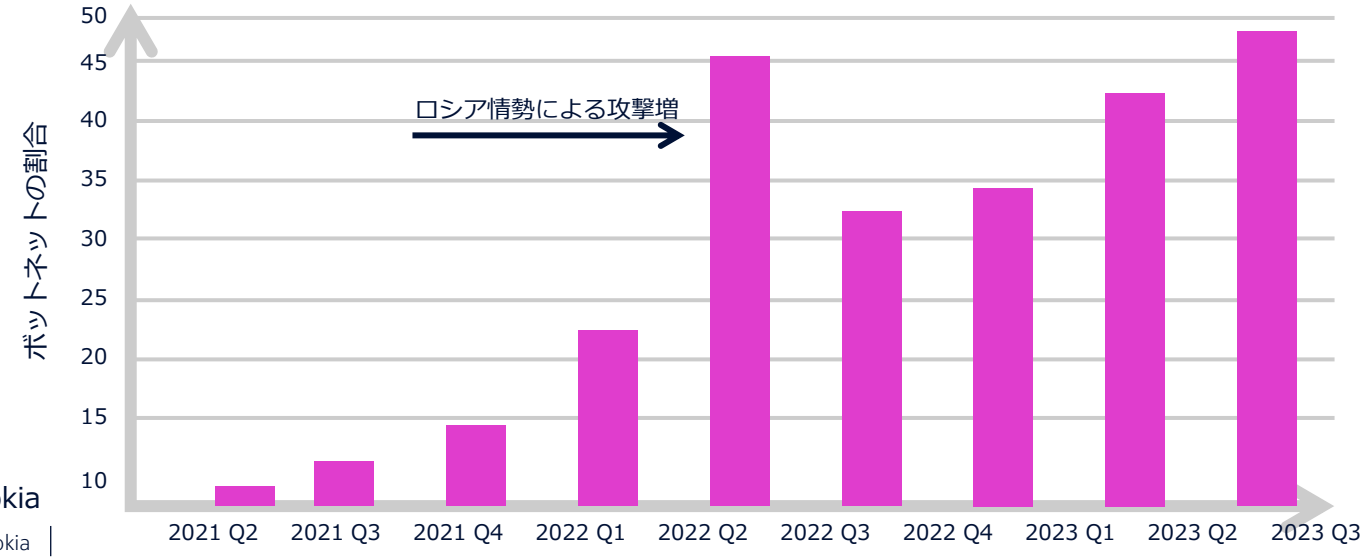
問題点:Botnet

2002年-2022年
DDoS の大部分はなりすまし
ヨーロッパ/アジアなどのホスティングプロバイダーからの送信
NTP/DNS サーバーを悪用など

2023年
ボットネットが DDoS ボリュームの大部分を占める

攻撃に占めるボットネットからの DDoS の割合

ほぼ50%!!!

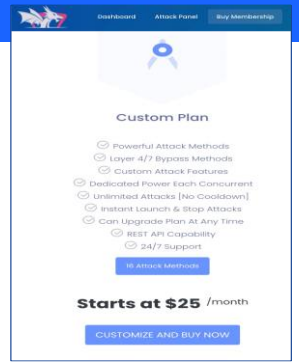


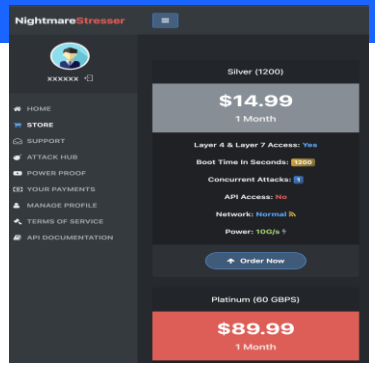
Source：Nokia

2.DDoSの変化と現在

問題点:IoT

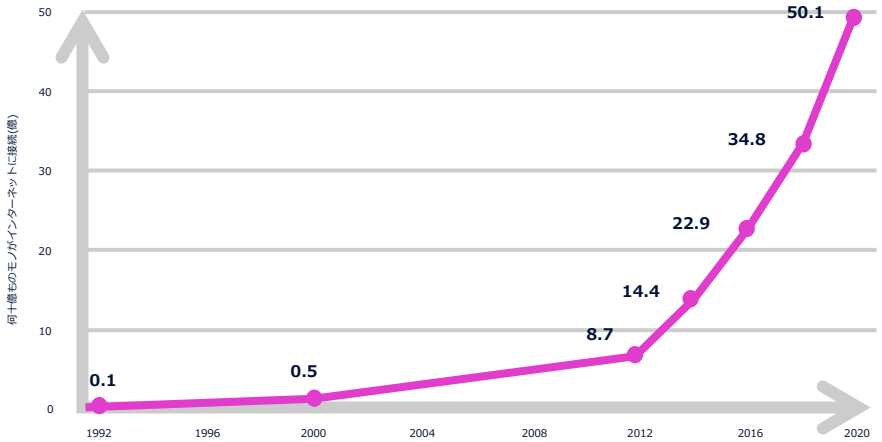
デバイスの急激な増加
ハイジャックに対して非常に脆弱
DDoS闇市場価格の崩壊を促進



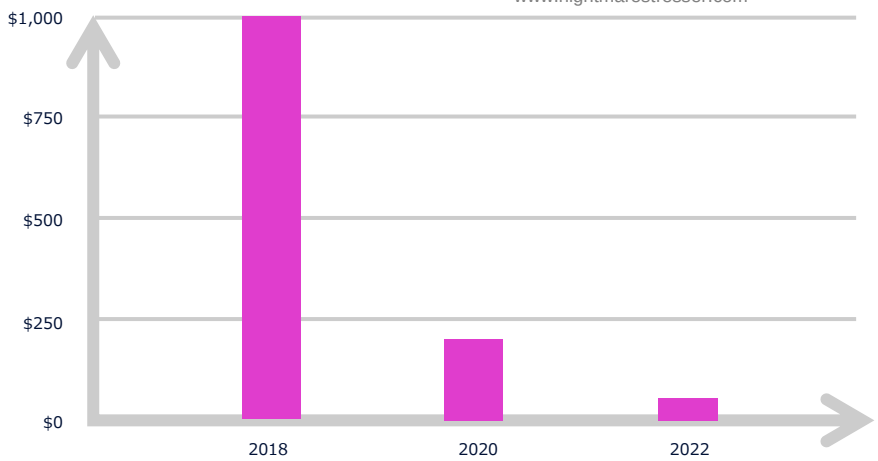


www.nightmarestresser.com

IoTデバイス数



https://www.comptia.org/content/research/sizing-up-the-internet-of-things



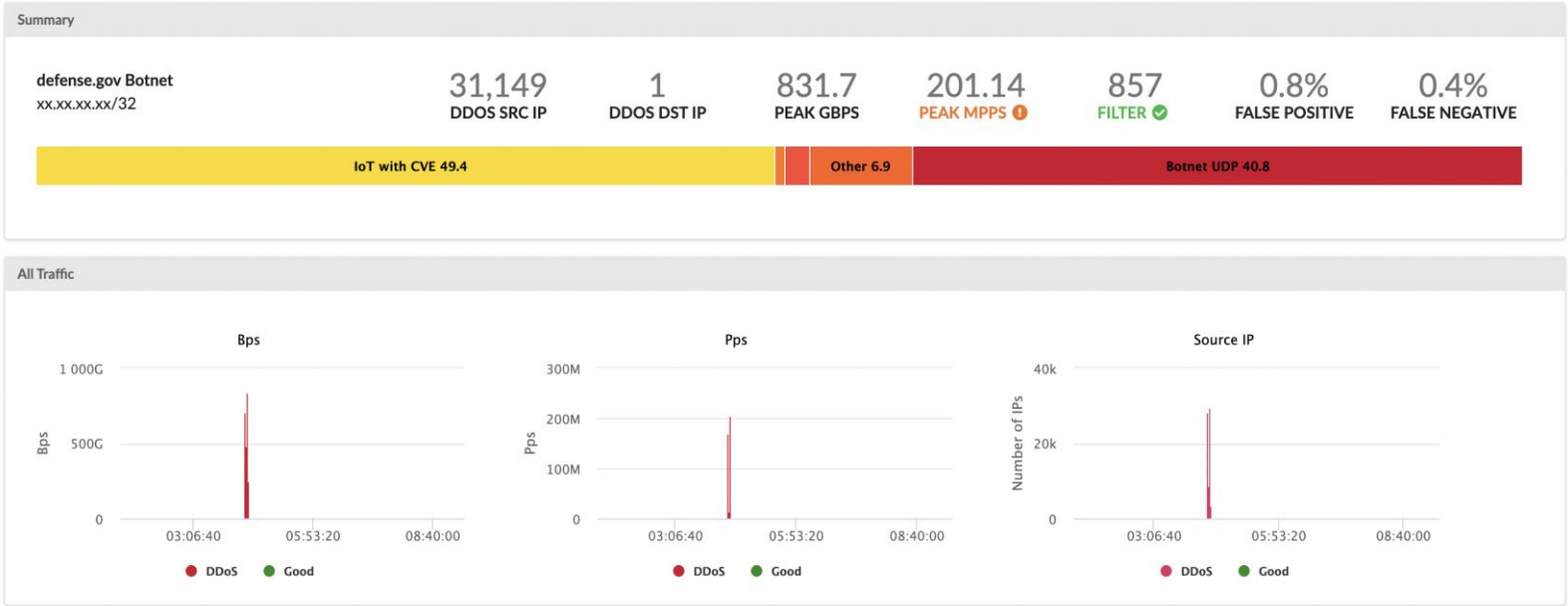
www.zero.bs blog

DDoS 導入にかかる 1 日あたりの平均料金

2.DDoSの変化と現在

問題点:IoT

IoTデバイスによる攻撃例
31,000 台の IoT デバイスからの 830 Gb/s 攻撃
~40% がエンドユーザネットワークから
瞬間で攻撃が終わってしまっている

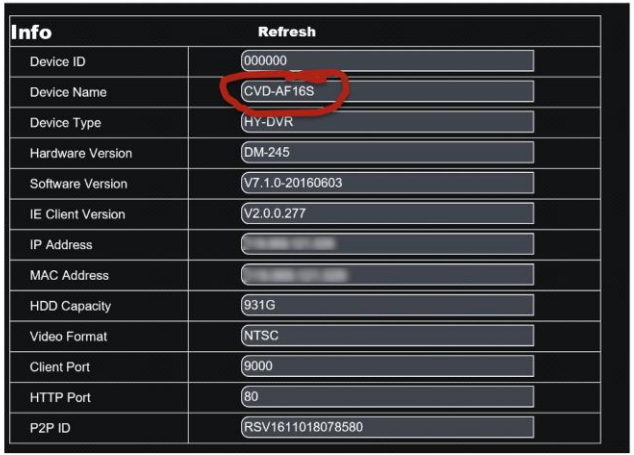


Source：Nokia

2.DDoSの変化と現在

問題点:IoT

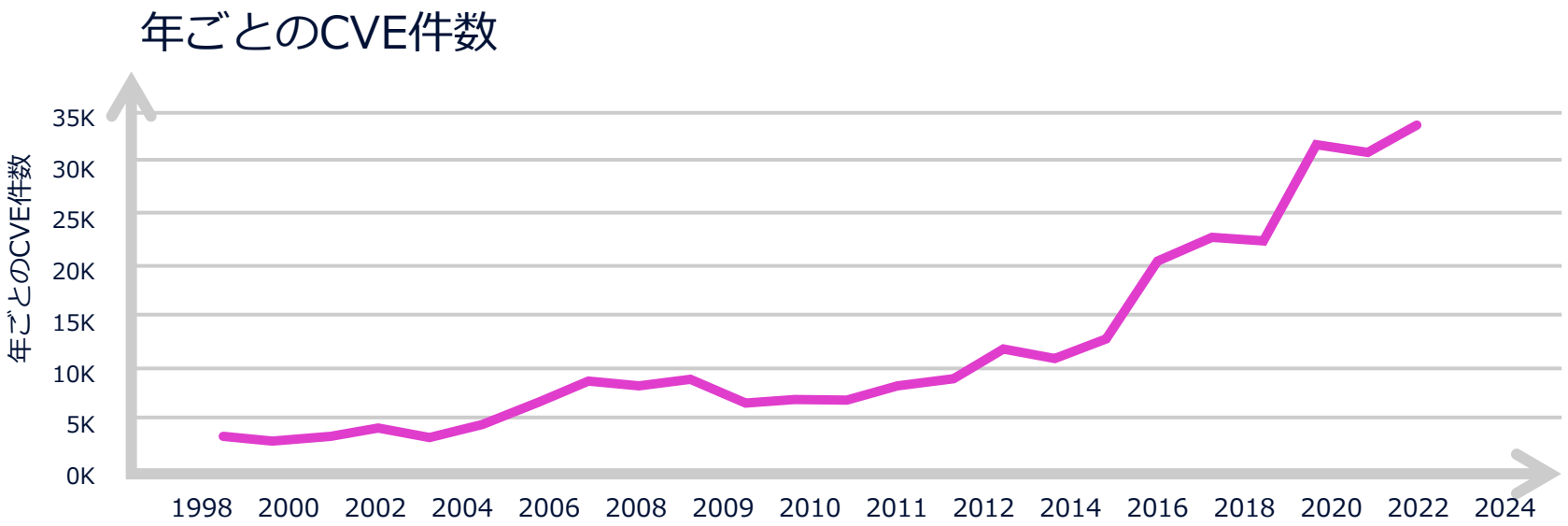
例:セキュリティ保護されていない IoTデバイスを簡単に発見可能
2016 ファームウェアを実行 - 悪用されやすいモデル番号からCVEを見つけることが可能
CVE から GitHub エクスプロイト コードをゲットし使用すると、ボットが作成



2.DDoSの変化と現在

問題点:脆弱ソフトウェア

報告されたIoT エクスプロイトの数は引き続き大幅に増加



Source : https://cve.mitre.org/

2.DDoSの変化と現在

問題点:世界情勢

サービスプロバイダーは知らず知らずのうちに地政学的紛争に巻き込まれる可能性がある

「DDoS攻撃」世界で5倍に急増、親ロシアのハッカー集団「キルネット」関与か

2022/09/13 13:30　ウクライナ情勢

この記事をスクラップする

政府のオンラインシステム「e—Gov（イーガブ）」や企業のホームページで、大量のデータを送りつけられてシステムがまひする「DDoS（ディードス）攻撃」が原因とみられる障害が相次ぎ、親ロシアのハッカー集団が関与を主張している。ロシアがウクライナ侵略を始めた時期から、同様の攻撃は全世界で5倍に増えたとの調査もあり、専門家は警戒を呼びかけている。（藤亮平）

イスラエル・ハマス衝突でサイバー空間も戦場に　ハッキングで“偽の核攻撃アラート”　SNSはデマだらけ

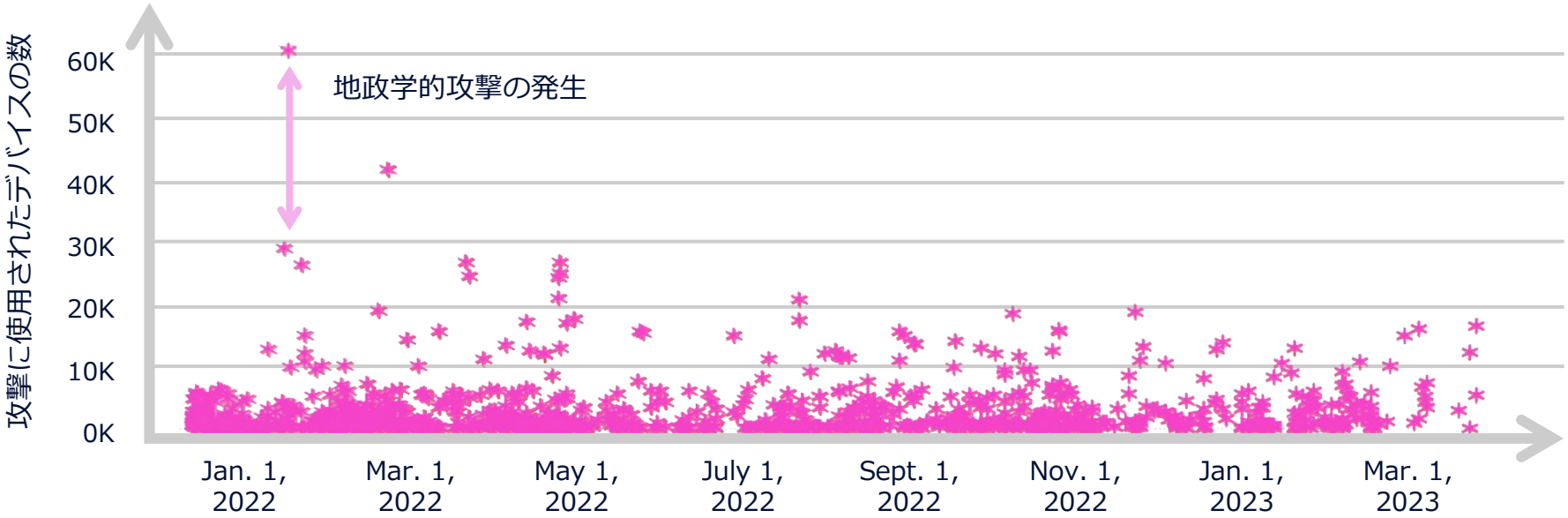
2023年10月18日 08時00分 公開

パレスチナ自治区ガザのイスラム勢力ハマスとイスラエルの戦闘が、サイバー空間でも激化している。イスラエルの警報アプリから偽の核攻撃警報が発信され、双方が大規模なDDoSなどの攻撃に見舞われ、SNSに投稿された偽情報は瞬く間に拡散する。

2.DDoSの変化と現在

問題点:世界情勢

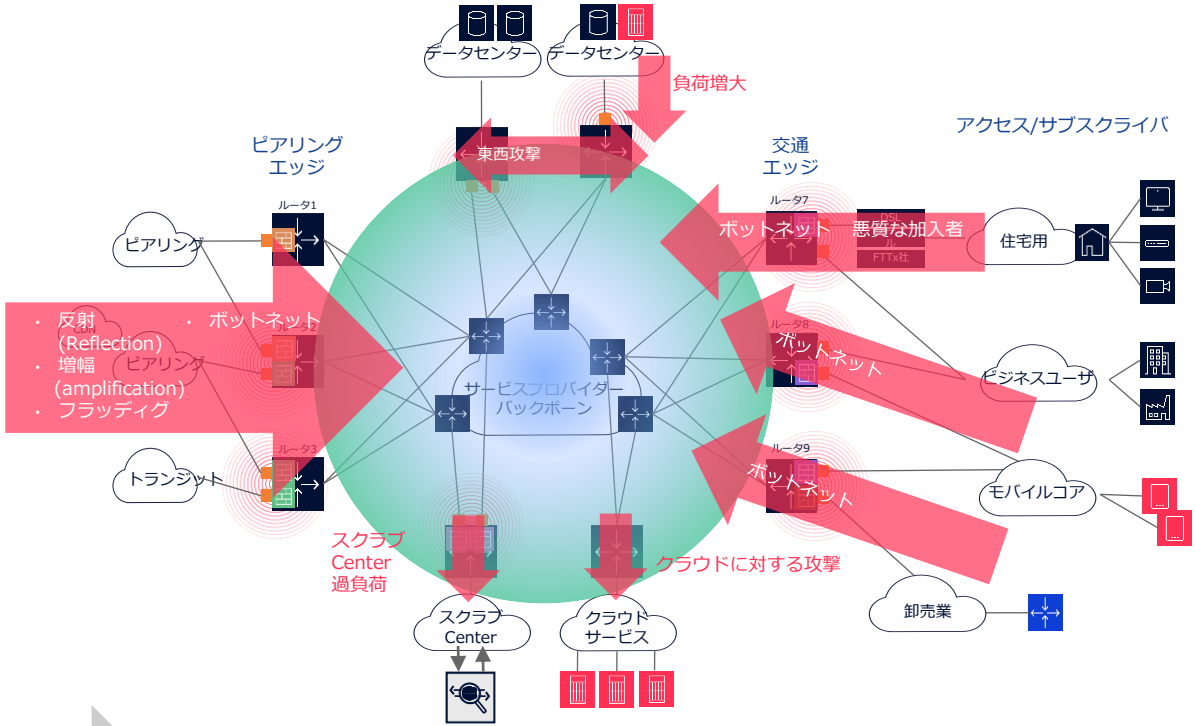
攻撃に使用されたデバイスの数



Source：Nokia

2.DDoSの変化と現在

問題点:360度、あらゆる箇所の攻撃が観測されている

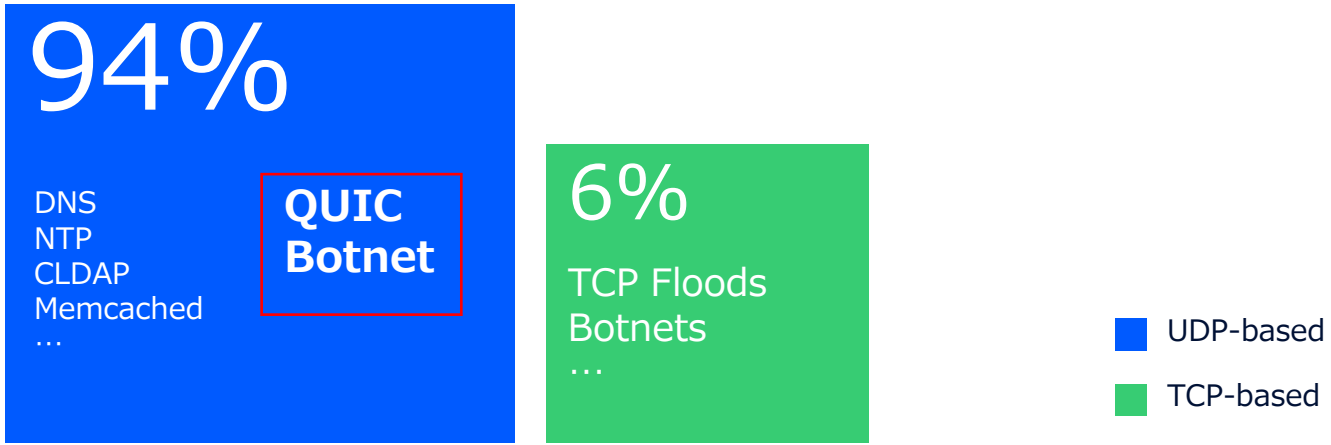


できるだけネットワークの入り口で安価に高度な防御が必要

2.DDoSの変化と現在

問題点:DDoSの内訳

UDPベースの攻撃が90%以上



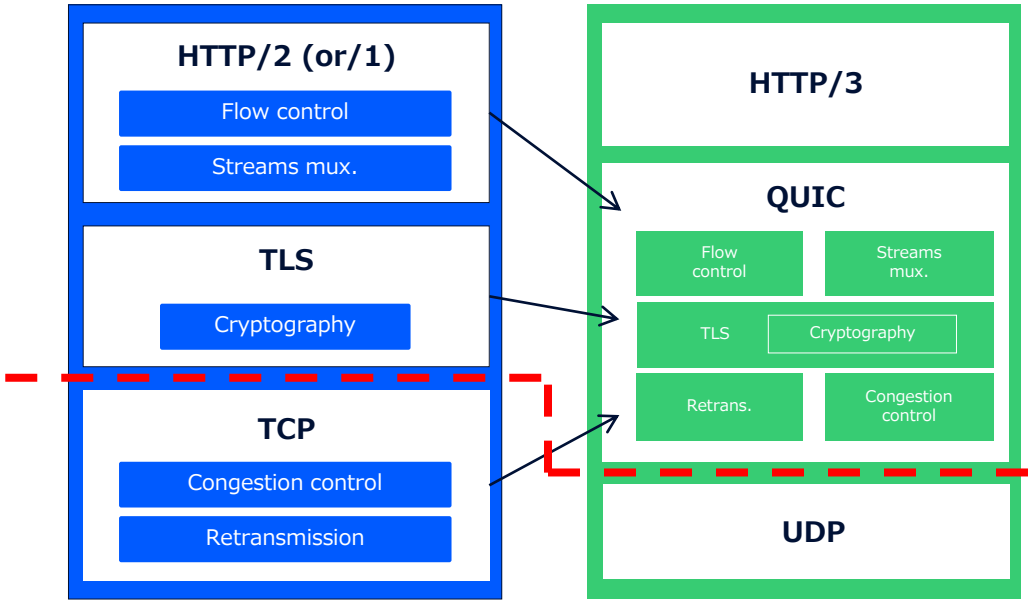
Source: Nokia

昔から傾向は変わらず投げつけるだけで攻撃可能ため
(コネクションレス/TCPよりシンプル/なりすませる)
しかし現在Botnet / QUIC、両方の割合が上位を占め始めている

2.DDoSの変化と現在

問題点:QUIC?

UDPベースの攻撃が90%以上



遅延を削減

- 0-RTT コネクション確立

帯域最大化

- 信頼性の高いストリーム間でヘッドラインブロッキングなし
- 多重化
- ACK(シグナル)削減

クライアントモビリティ

- トランスポート層でのコネクションレス型
- アプリケーション層での接続指向 (ランダムな 64 ビット接続 ID によるスティッキー性)

セキュリティとプライバシーの向上

?

2.DDoSの変化と現在

QUIC?

セキュリティ/プライバシーについてはまもられているか？

ハッカーが侵入したり隠れたりしやすくなる

ますます大規模なボットからの攻撃の可能性

一般的なルータでは UDP/443 のみをブロック可能、、、

暗号化されたUDP+ポート番号不明 DDoSが主流に？

2.DDoSの変化と現在

QUIC?

QUICの中身はどうなってみえるか？

Client Hello 例

```
> Internet Protocol Version 4, Src: 172.253.122.91, Dst: 192.168.1.88
v User Datagram Protocol, Src Port: 443, Dst Port: 60839
    Source Port: 443
    Destination Port: 60839
    Length: 1204
    Checksum: 0x2e6e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  > [Timestamps]
    UDP payload (1196 bytes)
v QUIC IETF
  v QUIC Connection information
      [Connection Number: 0]
    [Packet Length: 1196]
  v QUIC Short Header
      0... .... = Header Form: Short Header (0)
      .1.. .... = Fixed Bit: True
      ..0. .... = Spin Bit: False
    Remaining Payload: d84a2436f9b44a49fdef2012bd0d6bdcf0d3f2104a42465fa
```

```
v Extension: server_name (len=12)
    Type: server_name (0)
    Length: 12
  v Server Name Indication extension
      Server Name list length: 10
      Server Name Type: host_name (0)
      Server Name length: 7
      Server Name: [redacted]
```

L4よりは上の階層だがDPI、L7 ACLがかけられる機器であればなんとか対応はできる？

2.DDoSの変化と現在

QUIC?

TLS Encrypted Client Hello によるさらなる暗号化

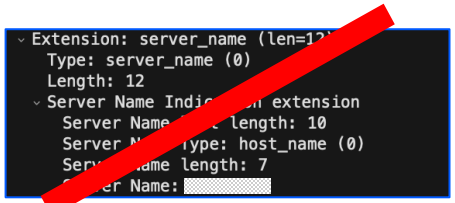
https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni

~~コネクション追跡~~ ~~TLS プロファイル~~ ~~URL フィルタリング~~ Payload inspection ?

TLS Encrypted Client Hello

Abstract

This document describes a mechanism in Transport Layer Security (TLS) for encrypting a ClientHello message under a server public key.



どうする?

送信元の識別と中身(L4レベル)に基づくパケット フィルターしかない(か？)

3.DDoS対策の最適解とは？

ネットワーク境界でのいままでの防御方法まとめ
インライン型:DPI、Firewall、IPS、etc

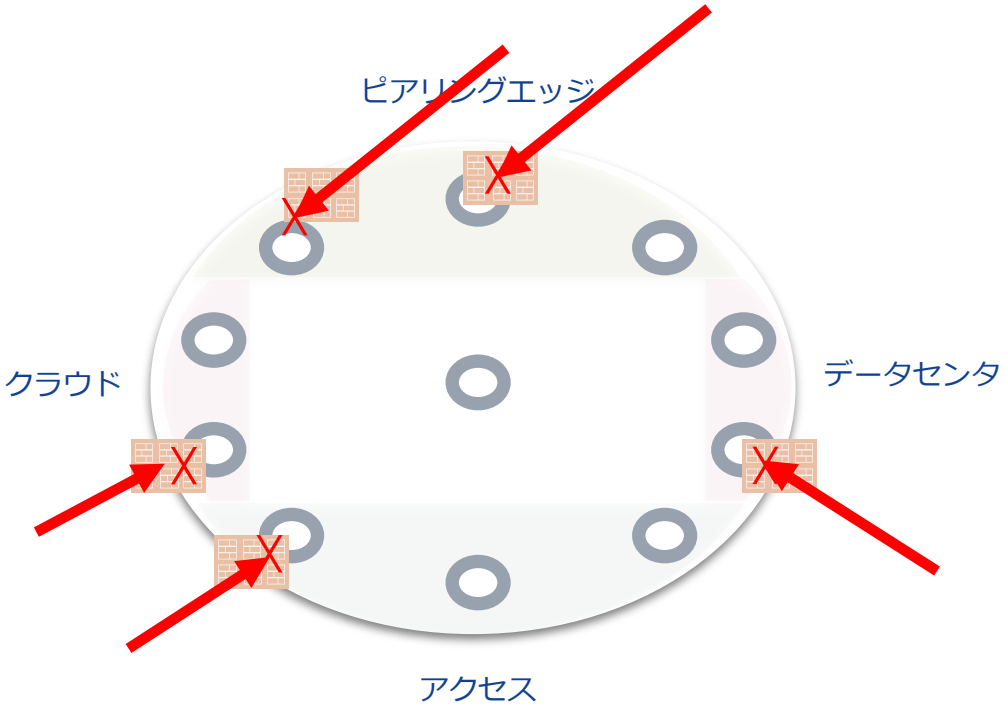
手法:ユーザネットワークの入り口に防御装置をおいてトラフィックをSignatureベースで解析

DDoSを止める

課題

非対称トラフィックに未対応、Signature/ルールで発見できないものに未対応

トラフィック増加に対して各装置も対応しないと行けない

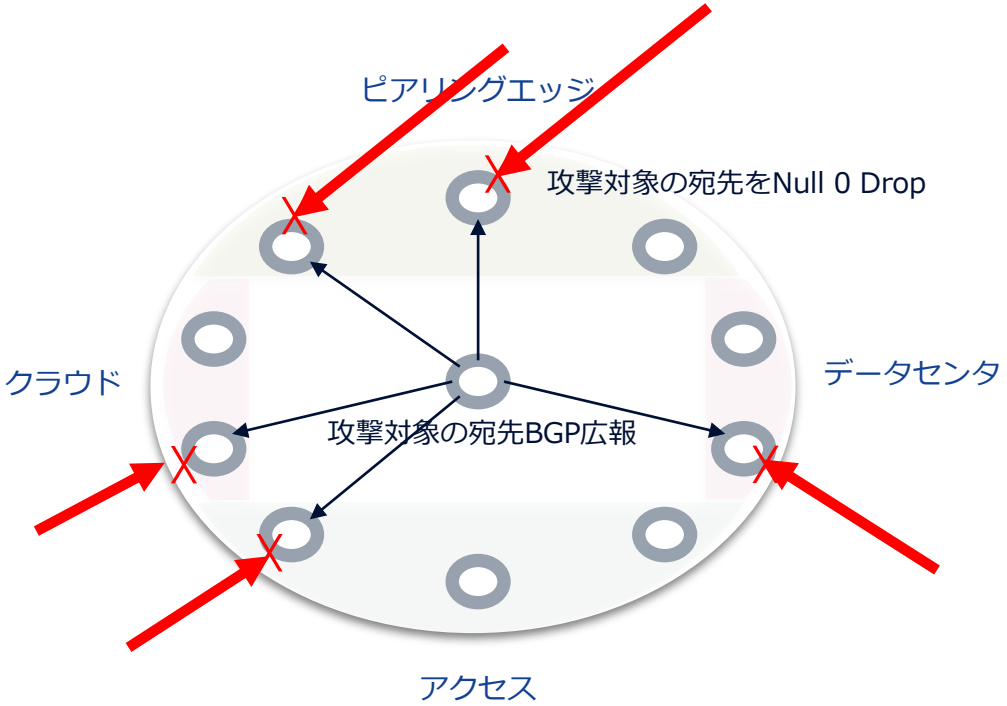


3.DDoS対策の最適解とは？

ネットワーク境界でのいままでの防御方法まとめ
RTBH(Remotely Triggered Black Hole Filtering)

手法:BGP経路広報
攻撃対象の境界ルータでドロップ

課題
宛先ベースでのDDoS防御となるため
悪意のないユーザのトラフィックにも
影響がある



3.DDoS対策の最適解とは？

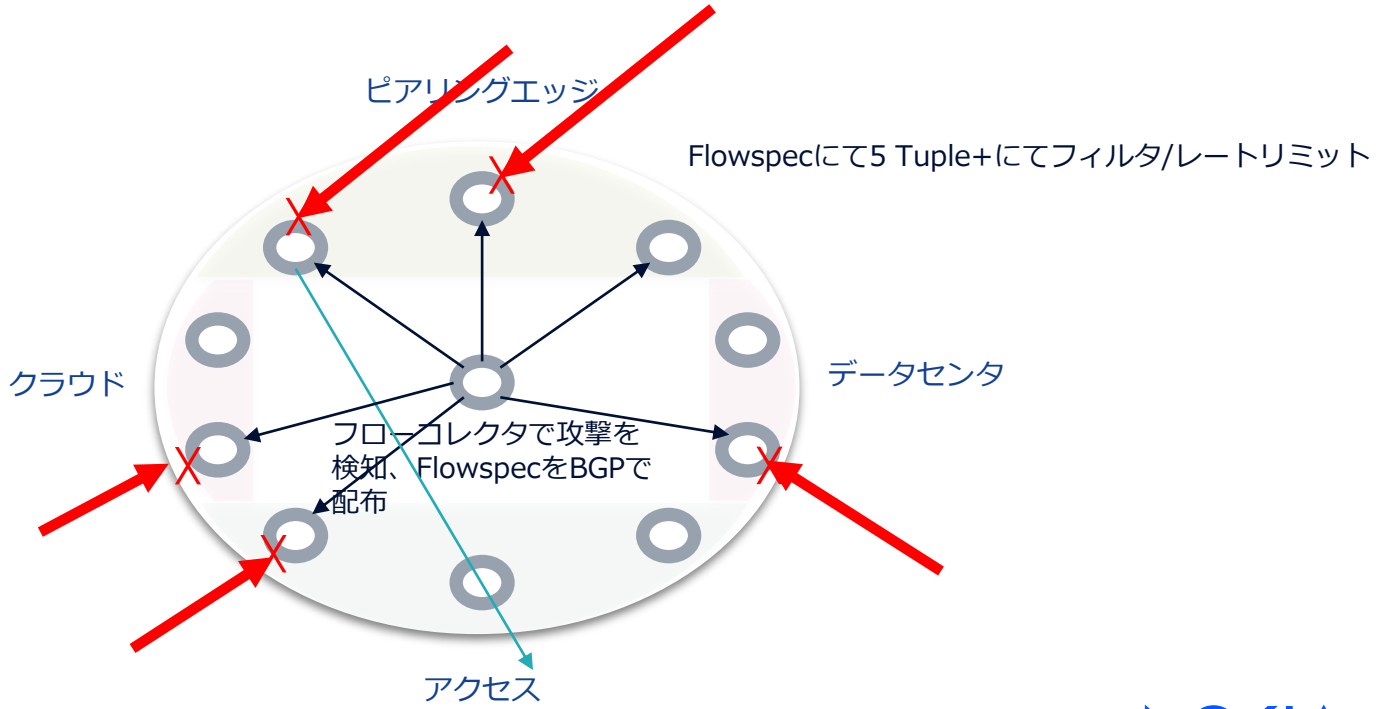
ネットワーク境界でのいままでの防御方法まとめ
Flowspec

手法:Flowspec

FlowコレクターよりBGP flowspecによりドロップ、Rate Limit

課題

RTBHよりきめ細かい制御(5 Tuple+でのACL)が可能だが防御する装置での対応及びスペックに依存



3.DDoS対策の最適解とは？

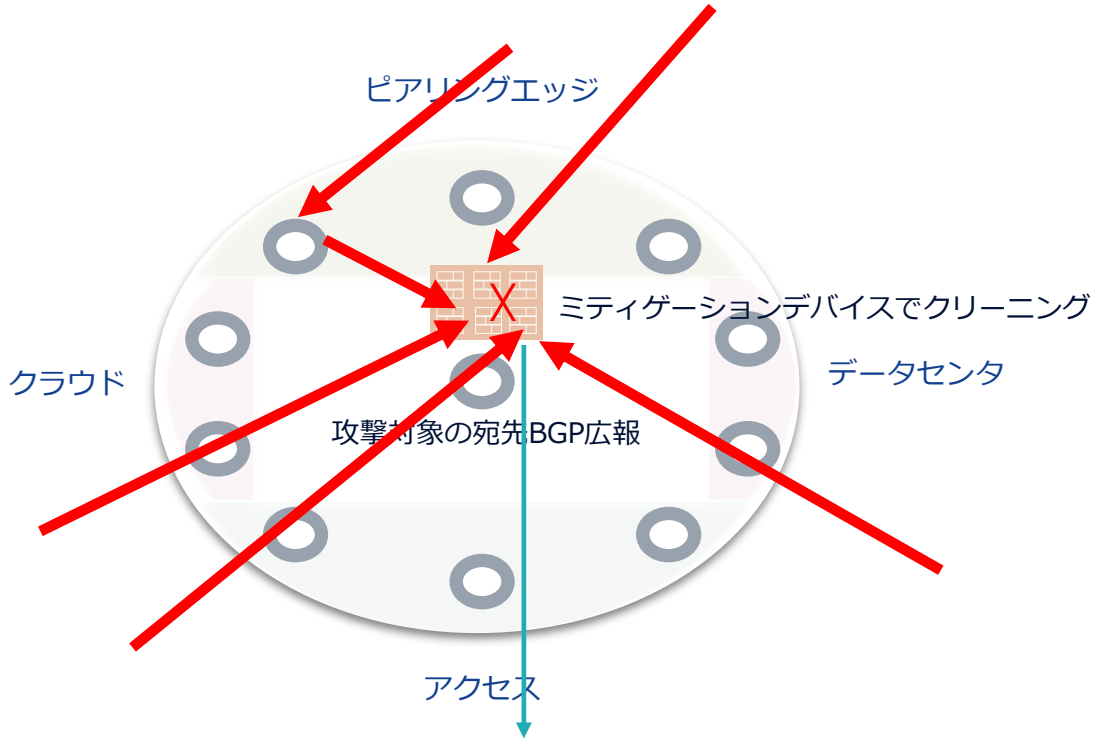
ネットワーク境界でのいままでの防御方法まとめ
ミティゲーションデバイス

手法:トラフィックをミティゲーションデバイスにRedirectしDDoSトラフィックをクリーニング

課題

DDoSチェックをしたいトラフィック量が多くなればなるほどミティゲーションデバイスの容量が大きくなる=コスト増

DDoSトラフィックをミティゲーションデバイスまで持ってこなければならずその分の帯域が無駄になる



3.DDoS対策の最適解とは？

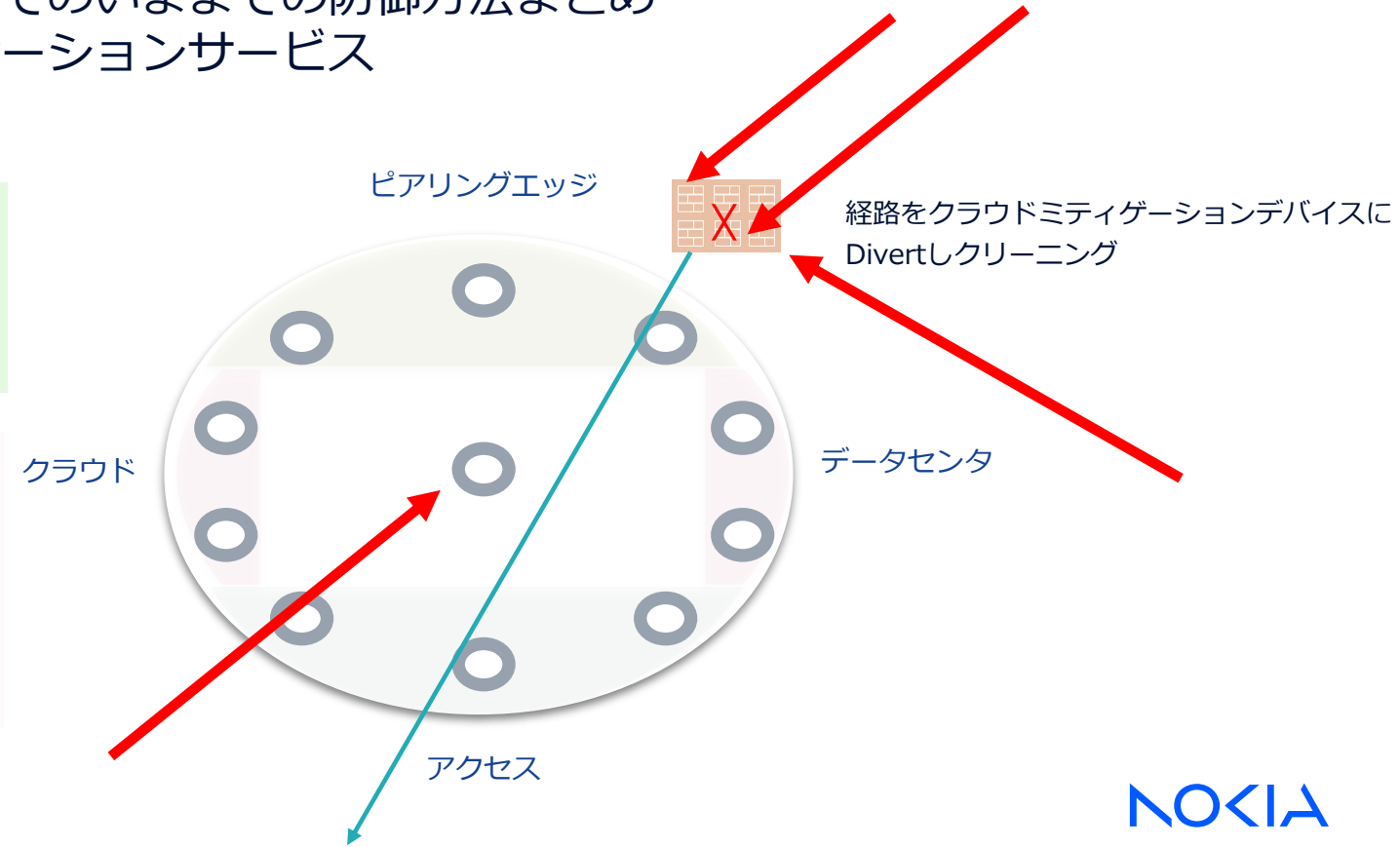
ネットワーク境界でのいままでの防御方法まとめ
クラウドミティゲーションサービス

手法:トラフィックをクラウドミティゲーションデバイスにRedirectしDDoSトラフィックをクリーニング

課題

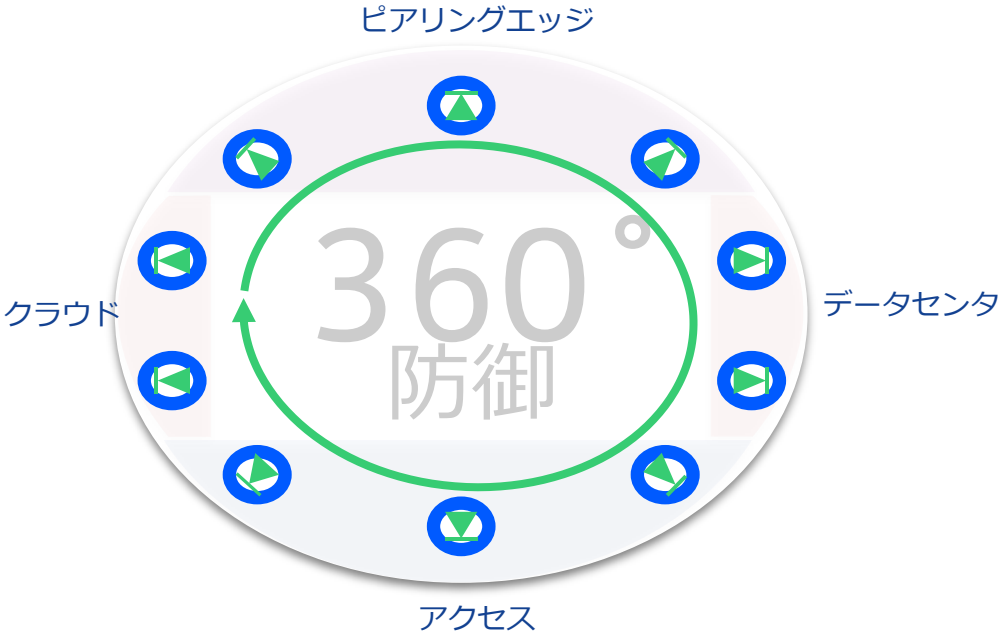
経路情報などをDivertするためクリーニングしたいトラフィックを寄せる必要がある

アクセス側など網を通っていかなければならないものは対応できない



3.DDoS対策の最適解とは？

理想は安価に高度にこうしたい
が今後のBotnet/QUICへの対応はどうすべきか？



必要な要素

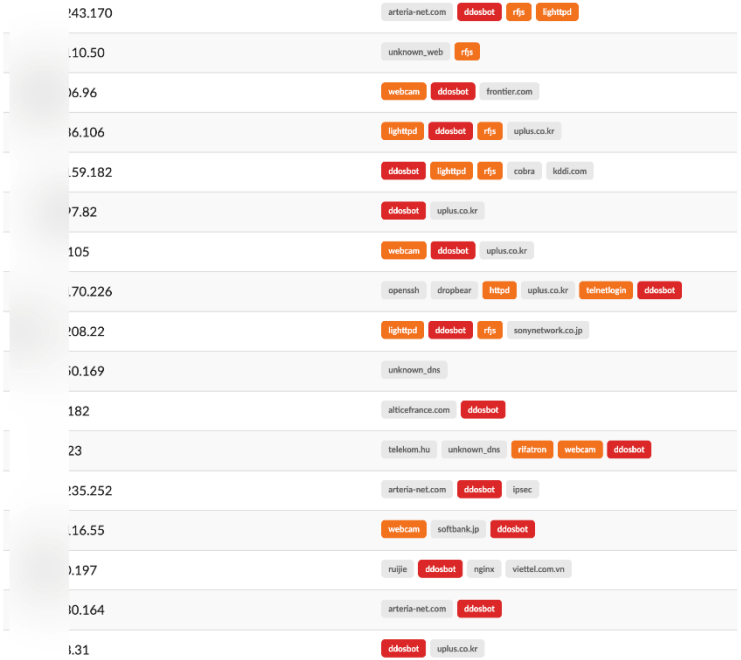
- DDoS検知方法と精度
- エッジ装置での防御力

3.DDoS対策の最適解とは？

ネットワーク境界での防御方法
DDoS検知:例)Nokia Deepfield Genomeの検知アプローチ

閾値ベース(bps/pps) やベースラインで検知するのではなく該当IPアドレスがどのような属性を持っているかを日々収集しその属性をもっているトラフィックが来た場合にはDDoSとして検知

QUICを使用していてもソースアドレスと属性、パケットレングス、TTLなどがあればフィルタが可能



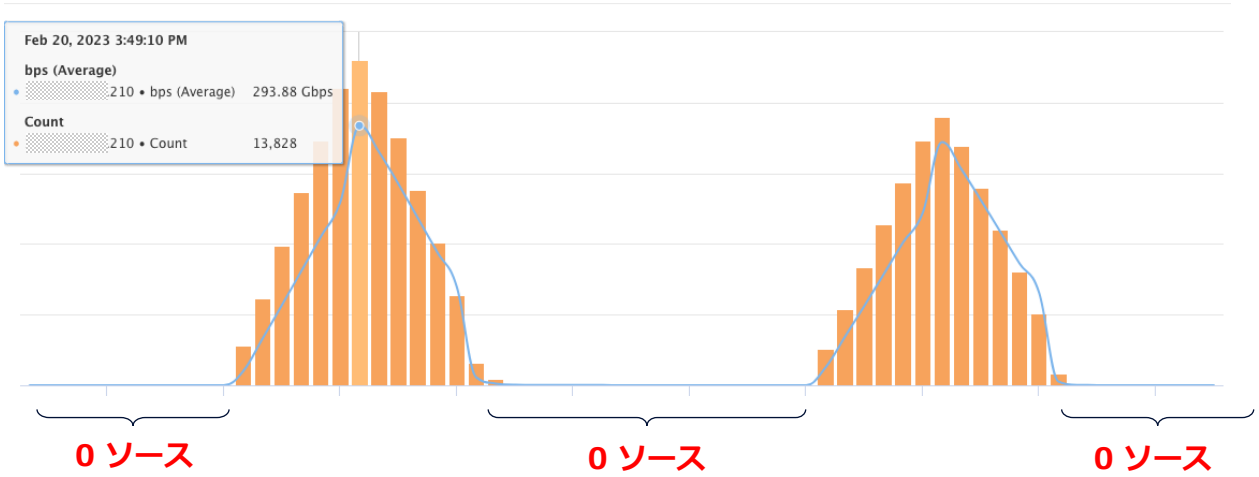
IP アドレス (ターゲット) への DNS 増幅攻撃におけるトラフィック
データ ソース: Nokia DDoS 防御ソリューションを使用する世界サービス/クラウドプロバイダー

3.DDoS対策の最適解とは？

ネットワーク境界での防御方法
DDoS検知後の防御方法:QUIC DDoSの例

UDP 個別ソースの数が数秒で 0 から最大 14,000 まで増加

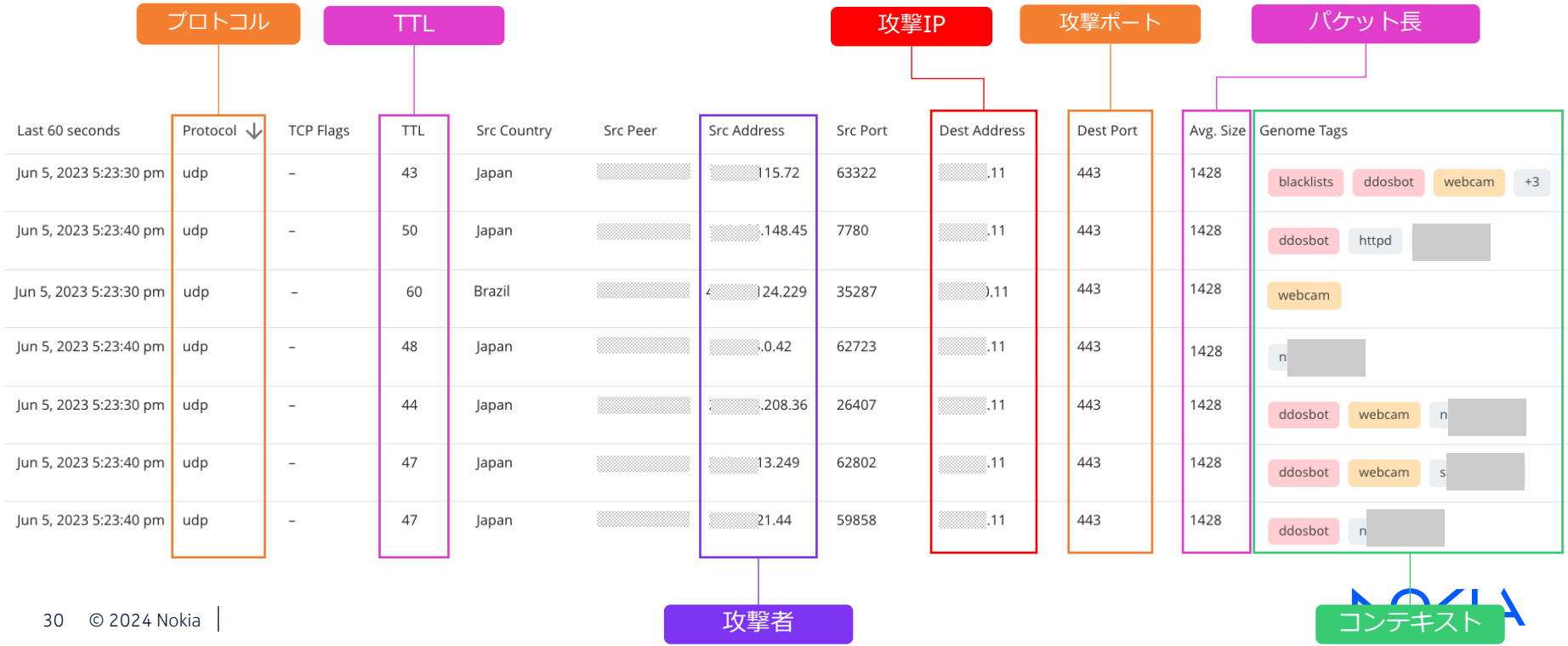
さらに、ソース IP あたりの ソース ポートの数は平均 50 で、これは約 700,000 の UDP 「接続試行」に相当



正当なイベントではないことを判断するにはどうすればよいか？

3.DDoS対策の最適解とは？

ネットワーク境界での防御方法
DDoS検知後の防御方法: QUIC DDoSの例)Nokia Deepfield Genome



Last 60 seconds	Protocol	TCP Flags	TTL	Src Country	Src Peer	Src Address	Src Port	Dest Address	Dest Port	Avg. Size	Genome Tags
Jun 5, 2023 5:23:30 pm	udp	–	43	Japan		115.72	63322	.11	443	1428	blacklists ddosbot webcam +3
Jun 5, 2023 5:23:40 pm	udp	–	50	Japan		.148.45	7780	.11	443	1428	ddosbot httpd
Jun 5, 2023 5:23:30 pm	udp	–	60	Brazil		24.229	35287	).11	443	1428	webcam
Jun 5, 2023 5:23:40 pm	udp	–	48	Japan		.0.42	62723	.11	443	1428	n
Jun 5, 2023 5:23:30 pm	udp	–	44	Japan		.208.36	26407	.11	443	1428	ddosbot webcam n
Jun 5, 2023 5:23:40 pm	udp	–	47	Japan		13.249	62802	.11	443	1428	ddosbot webcam s
Jun 5, 2023 5:23:40 pm	udp	–	47	Japan		21.44	59858	.11	443	1428	ddosbot n

3.DDoS対策の最適解とは？

ネットワーク境界での防御方法
DDoS検知後の防御方法:この情報をもとにACL生成

```
filter ip-filter my-acl
    ....
    entry 5 create
        match protocol Protocol
            src-ip ip-prefix-list Attackers
            dst-ip Target IP
            dst-port eq Target port
            packet-length eq Packet length
            ttl range Distant TTL
        exit
        action drop
    exit
    ....
exit
```

1 Target IP がプロトコル Protocol でどのポート Target port を使用している

2 Attackers と非攻撃者を区別

3 トラフィックの中身に何の問題に対し Packet length や TTL をさらに指定

ルータのACLで止められそう？

3.DDoS対策の最適解とは？

ネットワーク境界での防御方法
とはいえ

- Botnet/QUIC DDoSのソースを見つける一般的な方法は？
- エッジ装置にACLを設定する場合の必要なスケール/パフォーマンスは？
  - ACLをいちいち設定するのは大変。検知->設定->自動化が必要？

4.まとめ・議論

まとめ

- 近年DDoSは変化し特にBotnet/QUIC対策も必要となる
- 既存のDDoS対策では対応できれないケースも出始め、今後も進化が想定される

議論

- 現在どのようなDDoS対策をされていますか？
- 今後進化したDDoS攻撃に対する対策は？


NOKIA