DDoS対策に関するテスト話

2016.01.21 16:00～17:30
JANOG37 meeting BoF, どんなテストしてる? (続)

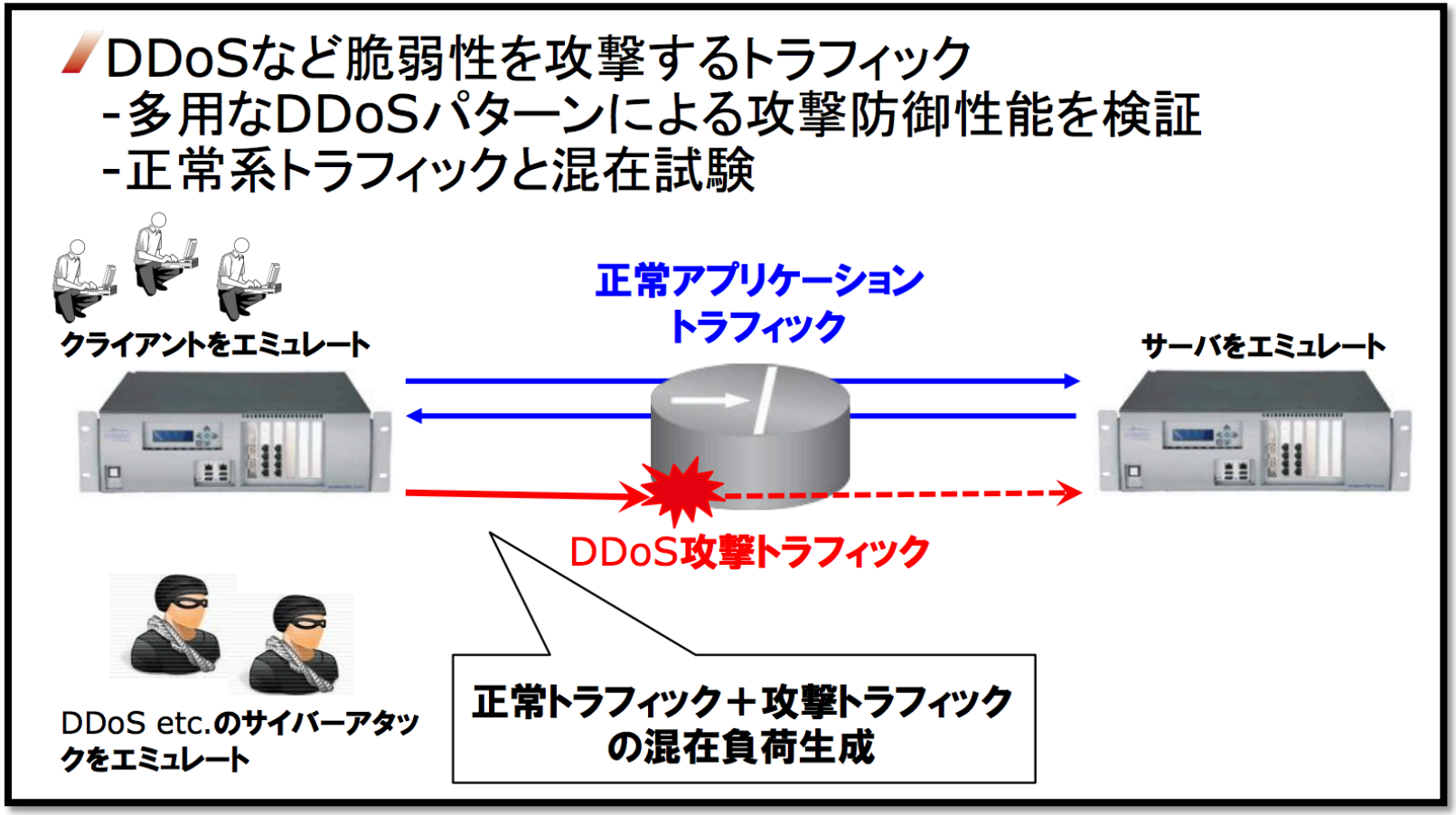
NTT コミュニケーションズ
技術開発部
池田賢斗

自己紹介

- 2014年 NTTコミュニケーションズ入社
- DDoS対策ソリューションの開発や、
  xFlow関連技術の開発に従事
- JANOG33 (学生時代)、JANOG36 のスタッフ活動
- wakamonog の 運営委員

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

前回のBoFでの小岩さんの発表資料



http://www.janog.gr.jp/meeting/janog36/download_file/view/166/196

本発表ではこの部分に関する実例を共有し、
Bofのネタ提供ができればと思います

DDoS軽減専用装置の検証実例

■ 今回ご紹介するPJの主な目的

- 複数のDDoS軽減専用装置に対して横並び検証を実施することで各製品毎の弱み・強みを評価し、商用サービスへの製品選定時の参考情報とする
  - ➢ 商用サービスへの導入のための検証ではないことをご留意ください

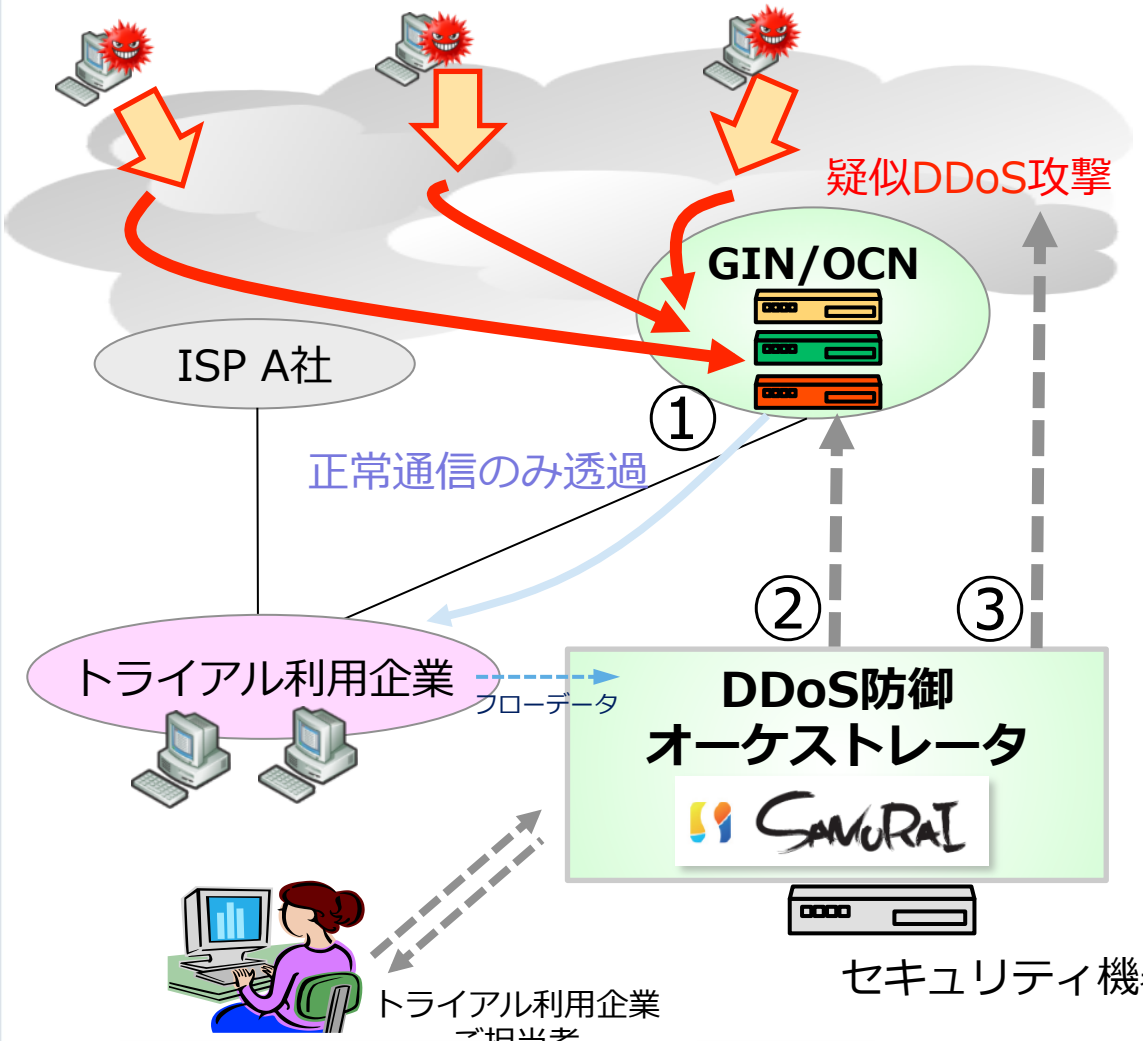
- 複数のDDoS軽減専用装置のAPIに関する検証を行い、DDoS防御オーケストレータシステムの開発を行なう

  ※ DDoS防御オーケストレータシステムについて
  <http://www.ntt.com/release/monthNEWS/detail/20150604.html>

- 開発したシステムを実網上に構築し、複数企業でトライアルを実施する

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

（参考）DDoSテストベッド トライアルを実施中



■３つの特徴

①NTT Com独自の経路制御技術
- DDoS攻撃をGIN/OCNに引き込み一元的に防御

②適切な防御手段の選択
・マネジメントポータルから状況に応じた防御手段を選択

③擬似攻撃発生による試験実施
・トライアル利用企業が自社への擬似DDoS攻撃が可能
・利用企業が自ら試験シナリオを作成・実行し有効性を評価

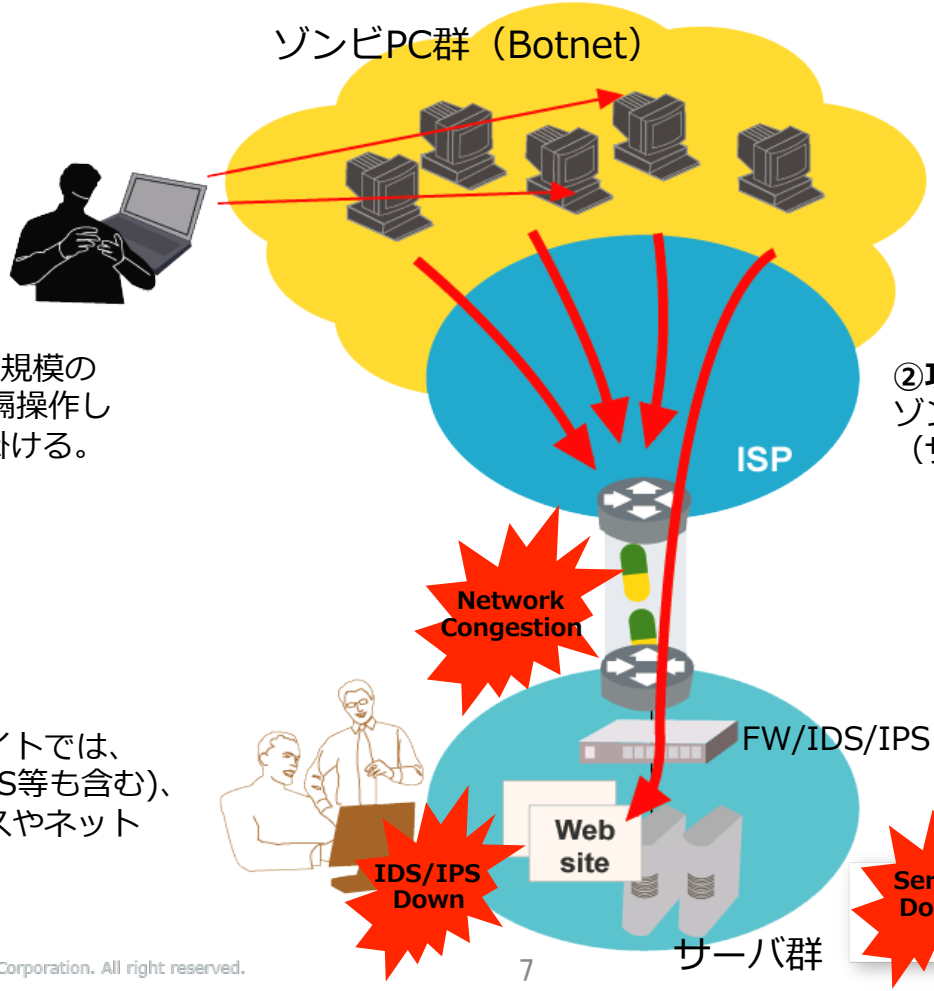
セキュリティ機器ベンダ提供のDDoS緩和装置

DDoS対策に関する
事前知識の共有

DDoS攻撃とは

DDoS攻撃とは

DDoS（Distributed Denial of Service：分散サービス妨害）攻撃は、インターネット上に存在する大量のコンピュータから一斉に特定サイト（WEBサーバなど）や企業のネットワークへ不正パケットを送出し、サーバ/システム負荷、ネットワーク輻輳を招き、サービスを停止させてしまう攻撃です。
ここ数年でDDoS攻撃が大規模化・複雑化しており、事前のセキュリティ対策が不可欠になりつつあります。



①攻撃命令
インターネット上の数十万規模のゾンビPC（Botnet）を遠隔操作しWEBサーバ等に攻撃を仕掛ける。

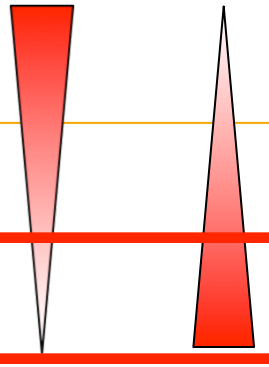
②攻撃パケット送信
ゾンビPC（Botnet）から、特定サイト（サーバ）への大量のパケット送信。

③DDoS被害の発生
DDoS攻撃対象となったサイトでは、サーバ高負荷（FW/IDS/IPS等も含む）、NW輻輳が発生してサービスやネットワークがダウン。

DDoS防御のトレードオフ

- DDoS対策において、精度-費用間のトレードオフが存在する
- DDoS防御の精度
  - False positive：通常トラフィックを誤って攻撃トラフィックと判断して遮断してしまうこと
  - False negative：攻撃トラフィックを誤って通常トラフィックと判断して通してしまうこと

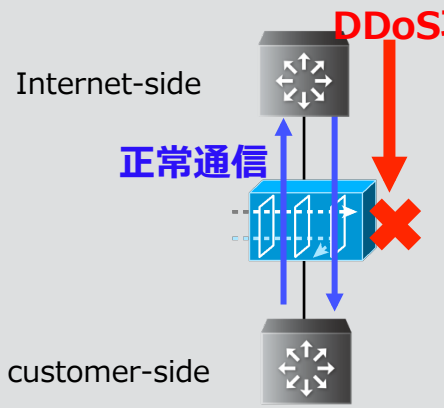
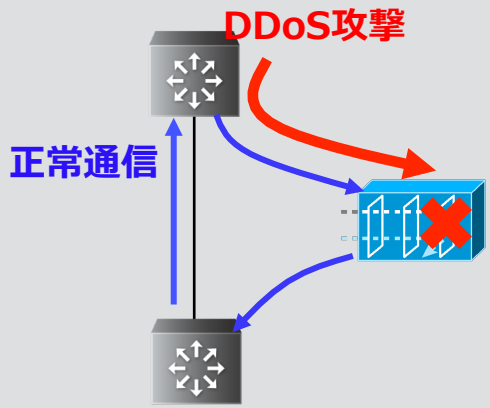
	手法	特徴	巻込	費用
①	ブラックホールルーティング	大規模アタックに対する対処。特定IP宛の全てのトラフィックを全て破棄		
②	アクセス制御設定	ルータ等におけるACL設定にてIP+Portの組み合わせでパケットを破棄		
③	DDoS軽減専用装置	きめ細やかなDDoS対処が可能。DDoS軽減専用装置にトラフィックを通して防御実施		



NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

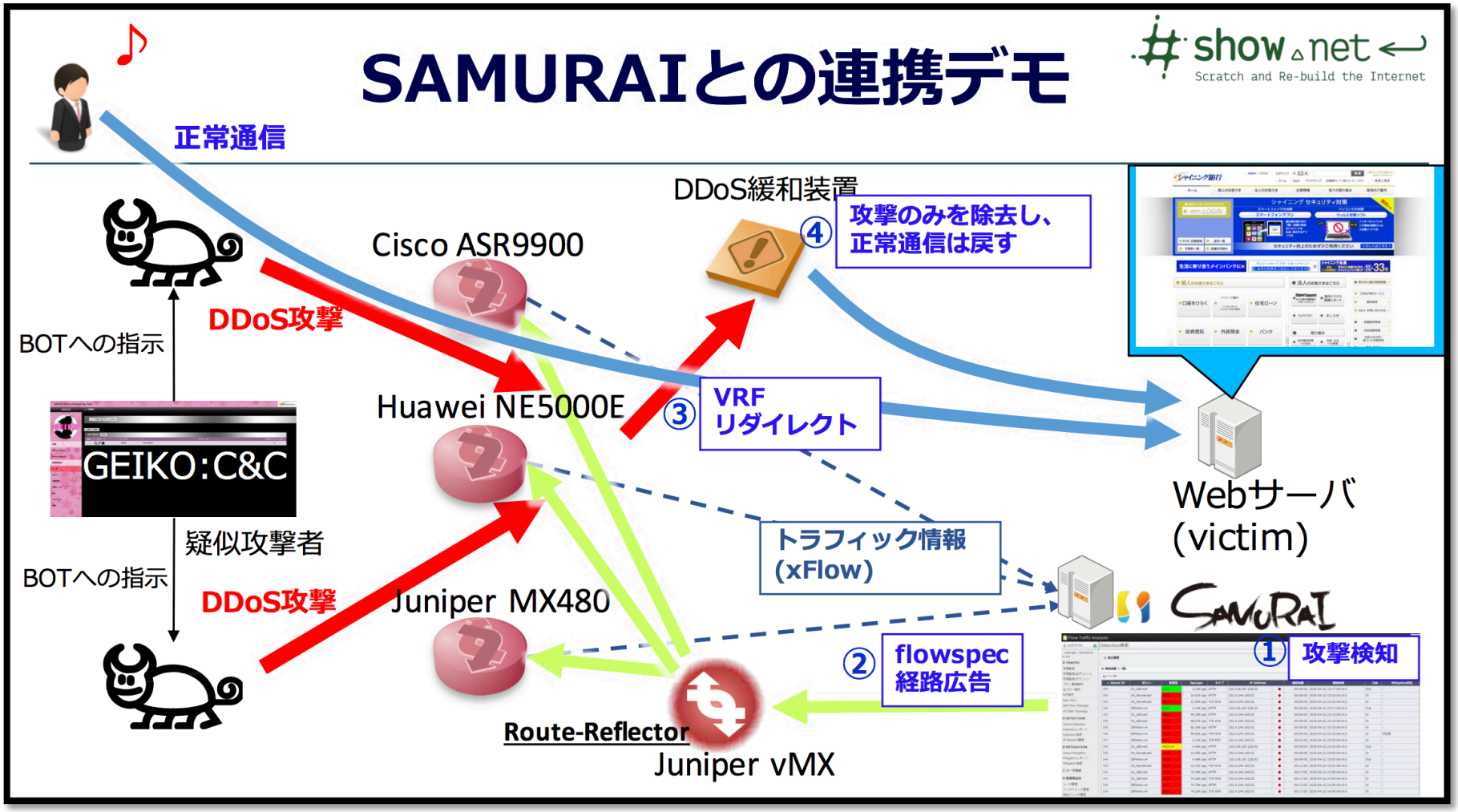
DDoS軽減専用装置を利用した防御

■ 主な構成

	インライン構成	オフランプ構成
構成		
防御期間	常時	flow情報などにより検知をし、一時的にトラフィックを引き込んでいる間のみ
トラフィック制御	特になし	BGP等を用いてトラフィックを引き込む GREトンネル等を利用して、元のNWに戻す
検知	DDoS軽減専用装置	flow技術による検知やユーザ申告など
防御	DDoS軽減専用装置	DDoS軽減専用装置
収容可能ユーザ	少ない	多い

構成によって、使用できない機能があるDDoS軽減装置も

(参考)flowspecを用いたオフランプ型DDoS緩和の例



http://www.janog.gr.jp/meeting/janog36/download_file/view/160/216

検証の実例のご紹介

ご紹介する検証の概要

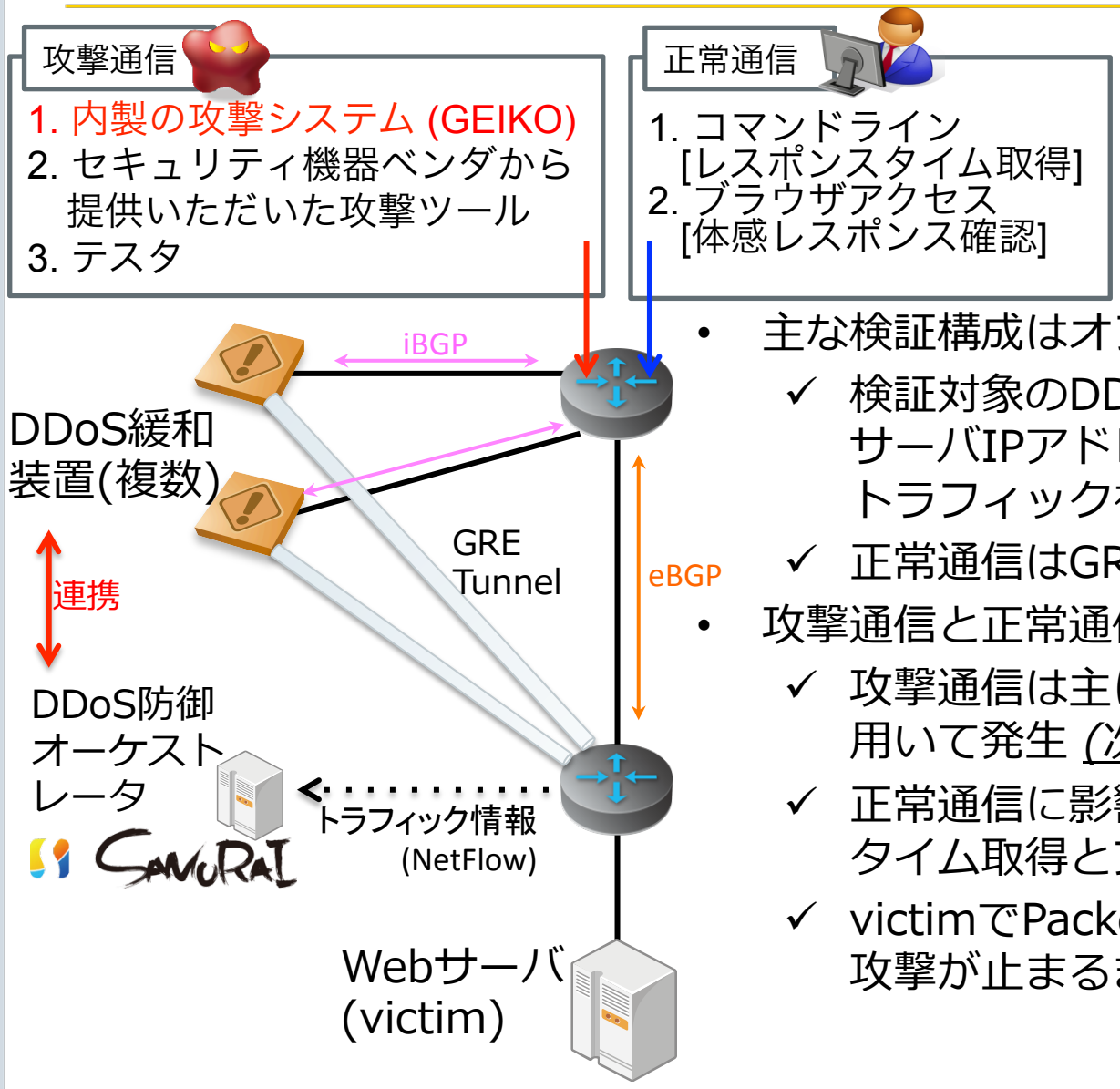
■ 主な検証構成はオフランプ構成
- DDoS攻撃の検知
- BGP経路広告によるトラフィック迂回
- DDoS軽減装置による攻撃トラフィックの除去
- GREトンネルによるトラフィック戻し

の4つの技術の検証が必要 (本発表では除去機能の検証について)

■ 本PJの検証の流れ
- ラボ試験
  - ✓ 上記の検証に加え、API制御に関する開発を行なう
- 実網試験
  - ✓ 検証用のASを用いて実網上で試験を行なう。
    主にトラフィックの迂回・戻しの検証を重点的に
- 他社様との共同検証

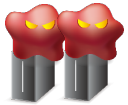
NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

ラボ検証の概要



- 主な検証構成はオフランプ型
  - ✓ 検証対象のDDoS緩和装置からvictimサーバIPアドレスの経路広告を行いトラフィックを引き込む
  - ✓ 正常通信はGRE経由で戻す
- 攻撃通信と正常通信の混在通信で試験を行なう
  - ✓ 攻撃通信は主に内製の攻撃システムを用いて発生 *(次ページで説明)*
  - ✓ 正常通信に影響がないことを、レスポンスタイム取得とブラウザアクセスにより確認
  - ✓ victimでPacket Captureを行い、攻撃が止まるまでの時間を測定

内製の攻撃システム (GEIKO) の概要

- GEIKOの構成
  - GEIKO:C&C 
    - ✓ Webポータルから(複数の)GEIKO:BOTに攻撃の開始/終了の指示を行なう
      - ➢ 使用するGEIKO:BOT・攻撃の種類・攻撃対象の選択が可能
  - GEIKO:BOT 
    - ✓ GEIKO:C&Cから指示を受け、攻撃を行なう
      - ➢ 現在26種類のDDoS攻撃を選択可能 (主に攻撃頻出度の観点から選定)
      - ➢ BOTの追加や攻撃ツールの追加は、Ansibleを用いて実施

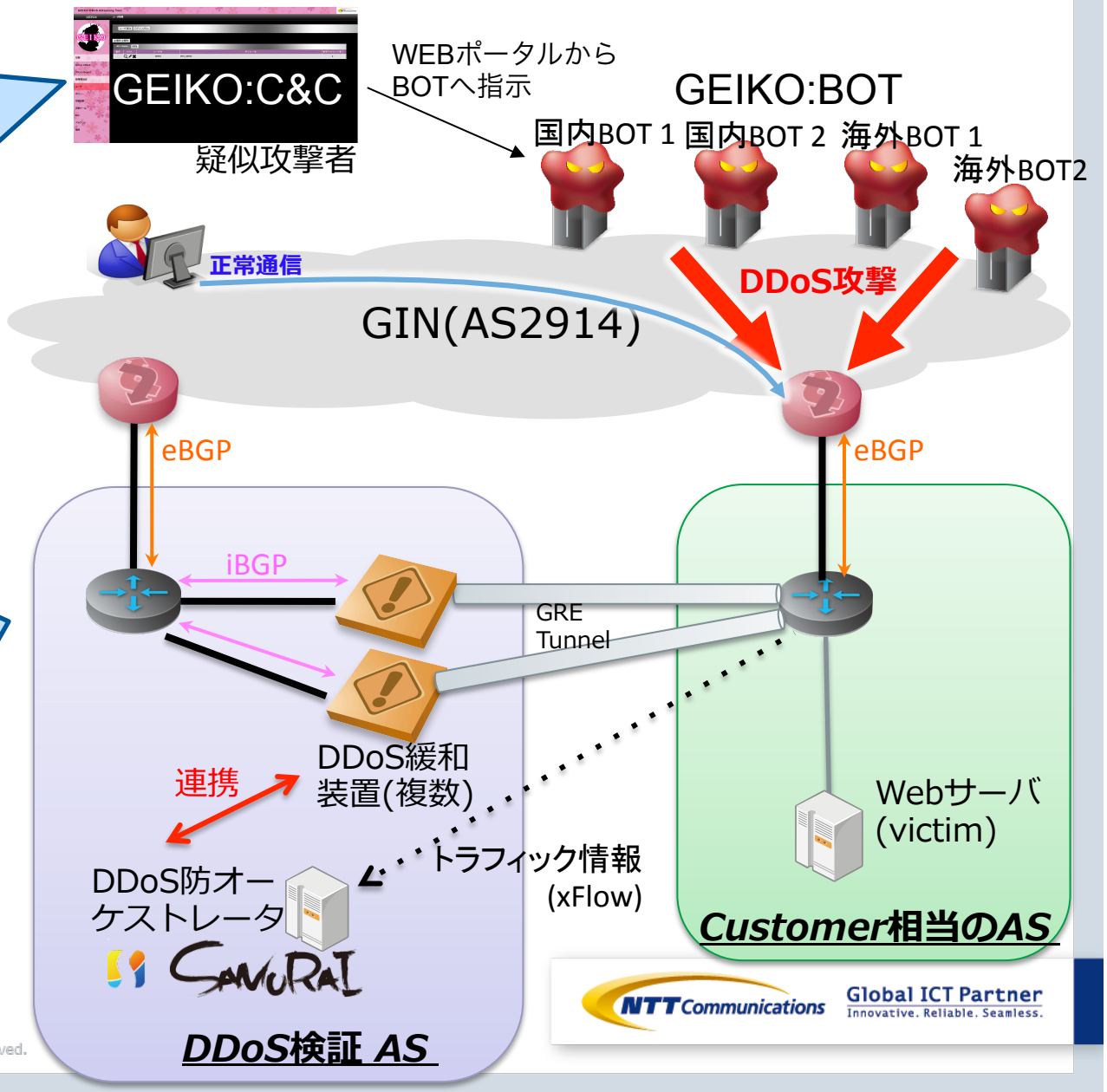
- 内製の攻撃システムを用いるモチベーション
  - 実網上での検証に拡張可能 (次ページ)
  - 公開されている攻撃ツール (ペネトレーションテストツール) に対してアンテナを高く持つきっかけとなる
  - テスタで足りない攻撃があった場合に対応可能
  - 低コスト

実網検証環境の概要

内製の攻撃発生システムを構築し、国内外の自社拠点にGEIKO:BOTを配置
↓
GINに影響がない範囲で実網上でDDoS対策関連の検証を実施可能

オフランプ型で実網上に検証環境を構築

防御対象アドレスの経路広告をGINに行なうことで、DDoS軽減装置への引き込みが可能



NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

実網検証環境の活用例

- トラフィックの引き込み・戻しの検証を実網上で実施
  - BGP経路の伝搬の検証
  - DDoS緩和装置のMTUに関する検証を実網上で実施
    - ✓ DDoS緩和装置とCustomerがGIN上でGREトンネルをはる場合、GREのMTUを1500にすることが可能
    - ✓ 通常のGREのMTUは1476となるが、GINのバックボーンはMTUが大きく設定されているためGREのMTUを拡張可能
      → トラフィック戻しの際のフラグメントを防ぐことが可能
- GeoIPベースの緩和(除去)機能の検証を実施
  - 国内外に配置したBOTを用いることにより検証を実施
- 他社様との共同検証を実施

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

まとめ・BoFで議論したい内容

- オフランプ型DDoS緩和の場合、
  ①検知 ②トラフィック迂回 ③除去 ④トラフィック戻し
  の4技術に関する検証が必要

本日は主に除去機能の検証についてお話しました

- セキュリティアプライアンスの検証の場合、テスタの使用だけではなく、世の中に出回っているツールのウォッチも重要

- セキュリティアプライアンスは L7機器なので正解データがない
  - 複数種類の攻撃を組み合わせや、それと正常通信の組み合わせを考えるとトラフィックパターンは無数に存在する

  (セキュリティアプライアンスに限らず、)
  L4以上の機器検証を行なう際、みなさまどのような（どこまで）試験を行ってますか？
  →実際に導入してしまい、チューニングをしていくことも必要なのではないでしょうか？

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

ご清聴ありがとうございました