ISPにおけるDoS/DDoS攻撃の検知・対策技術

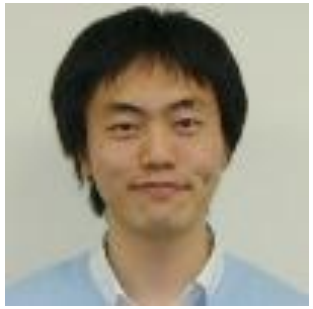
InternetWeek 2013 S2:DDoS攻撃の実態と対策
2013/11/26 (火) 13:00-15:30

NTTコミュニケーションズ株式会社 西塚要

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

自己紹介

- 西塚要

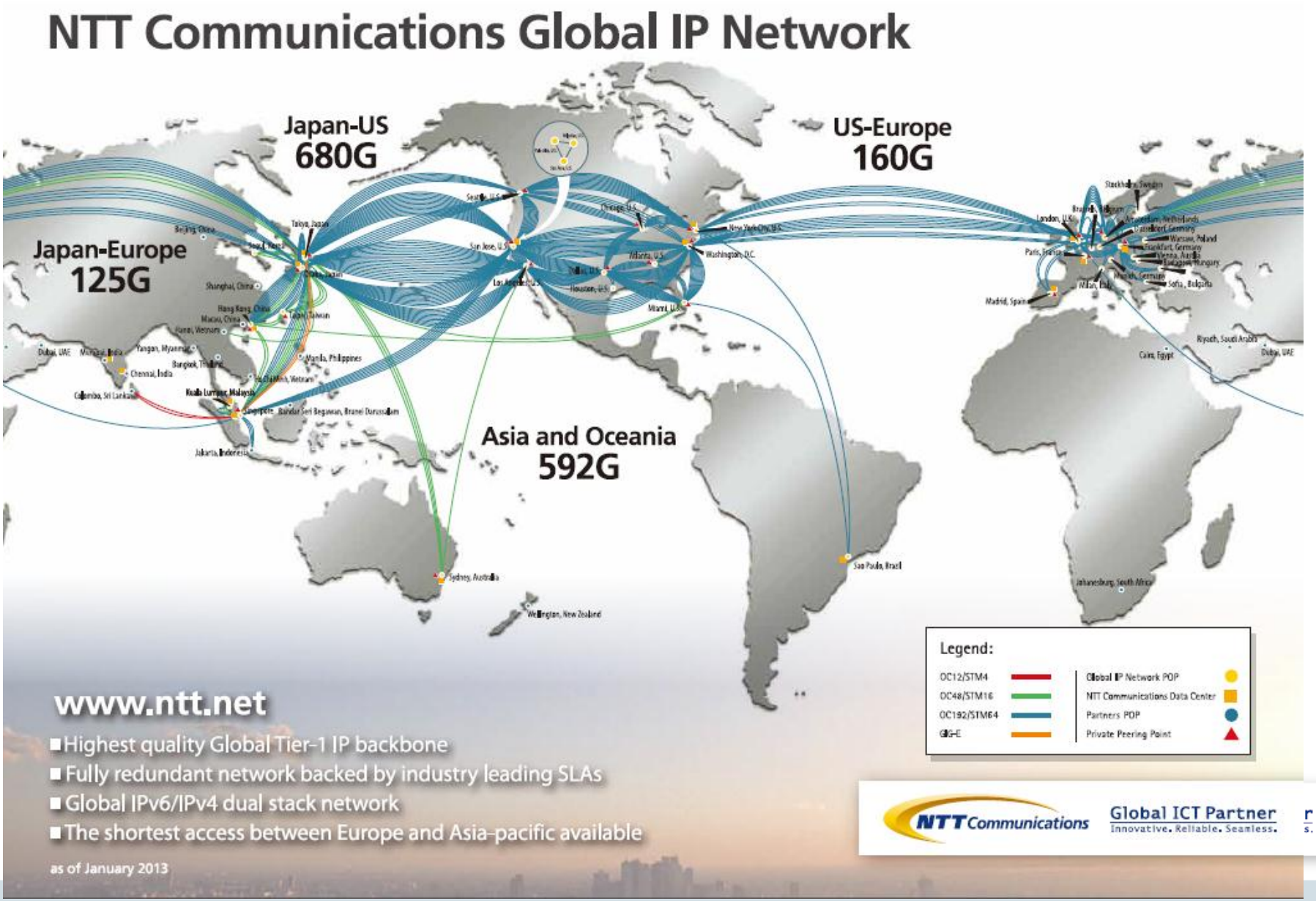


- 2006年 NTTコミュニケーションズ入社。
- OCNアクセス系ネットワークの設計に従事した後、中・大規模ISP向けのトータル保守運用サービスを担当。
- 現在、顧客基盤を守るためのDDoS対策ソリューションの開発に従事。

- 対外活動
  - JANOG28 実行委員長
  - JANOG30 会場運営委員長など

キャリアにおける Dos/DDoS対策の取り組み

アジア圏最大規模のTier1ネットワーク



SAMURAI 登場

高度なトラフィック監視
DDoS攻撃検出・対策を実現する
トラフィック解析ツール

SAMURAIが実現するDoS/DDoS対策

- 攻撃の検知
  - xflow技術を基にした検知
    - ✓ 特定の攻撃パターンによる検知
    - ✓ 過去のトラフィック学習による検知
  - 高度な解析
    - ✓ DNS Amp 攻撃を例に。

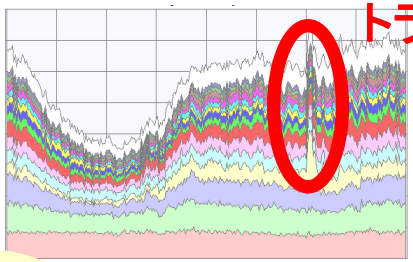
- 防御
  - 攻撃規模に合わせた3段階の手法
    - ✓ BH(BlackHole) ルーティング
    - ✓ フィルタリング
    - ✓ 防御装置との連携
  - 新しい防御手法
    - ✓ 顧客への攻撃の実例から

攻撃の検知について

トラフィックの解析と異常検知

SAMURAI

-アプリケーション解析/アドレス解析
-異常検知



トラフィック情報の収集
(flowデータ)

海外ISP

お客様サーバ

お客様
ネットワーク

国内ISP

海外ISP

異常トラフィック検知（不正トラフィック検知）

(1) 攻撃パターンにマッチした際の攻撃検知

DDoSトラフィックパターン	概要
DNS	大量のクエリーなどによるDNSの攻撃トラフィック
ICMP	大量のPingなどによるICMPの攻撃トラフィック
IP Fragment	IPフラグメントトラフィック
IP Private	プライベートIPアドレストラフィック
Protocol 0	Protocolの指定がないトラフィック
TCP Flag 0	TCPでTCP Flag指定がないもの
TCP RST	TCP RSTトラフィック
TCP SYN	TCP SYNトラフィック

(2) トラフィック学習による異常トラフィック検知

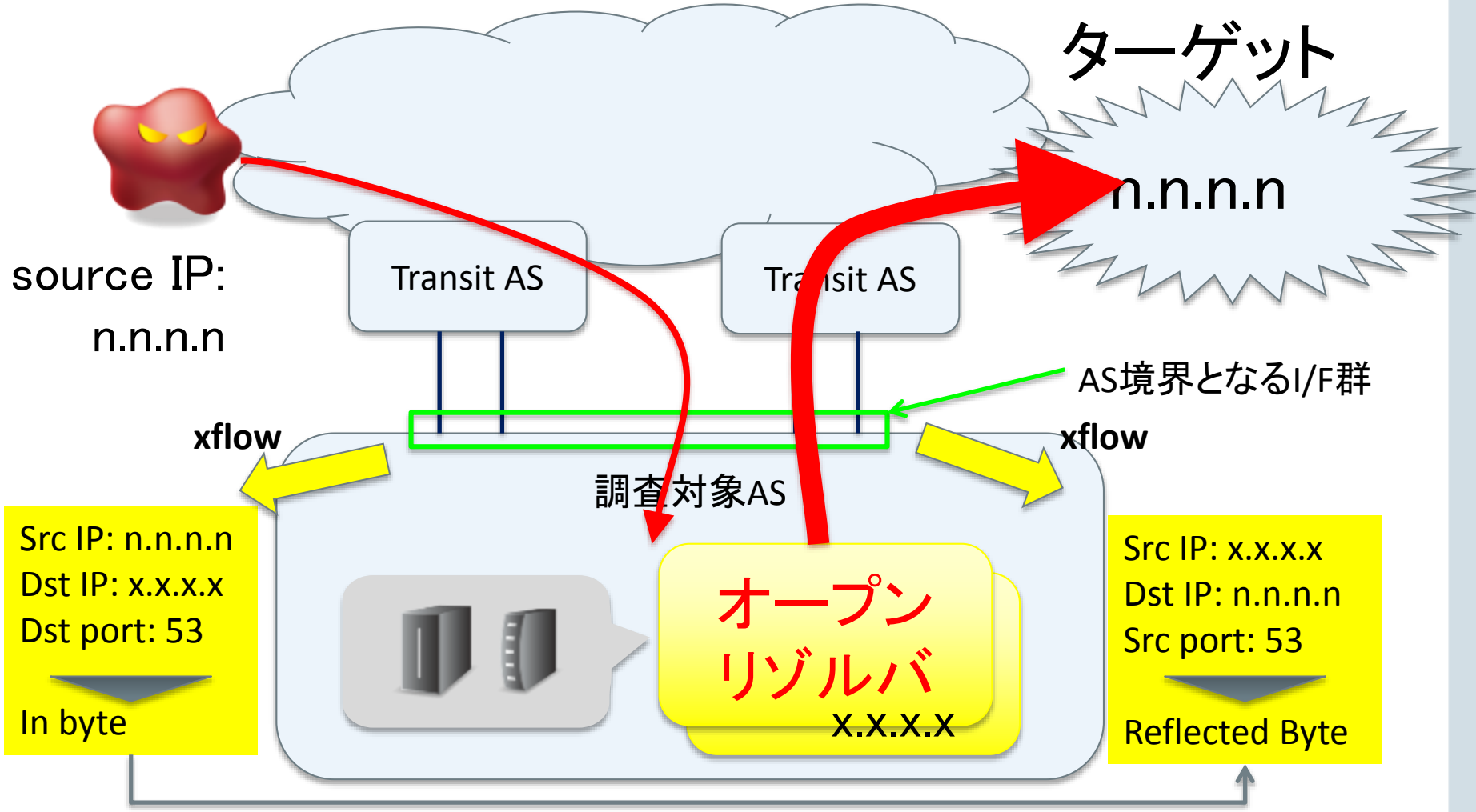
過去のトラフィックを学習し、大きく外れた値となった際に異常トラフィックとして検知します。

xflow技術による
DNS Amp攻撃の解析

モチベーション

- OpenResolverProject.org などで与えられるオープンリゾルバのリストについて、「本当に攻撃に利用されているのか」を解析する。
- 上記のリストに載っていないが実はオープンリゾルバになっているIPアドレスが無いかを調べる。
- 対象:SAMURAIを導入していただいている顧客

xflowを用いた手法



比較して、倍率をAmp強度と定義

解析の詳細は当日会場にて！

xflow技術によるDNS Amp攻撃の解析結果

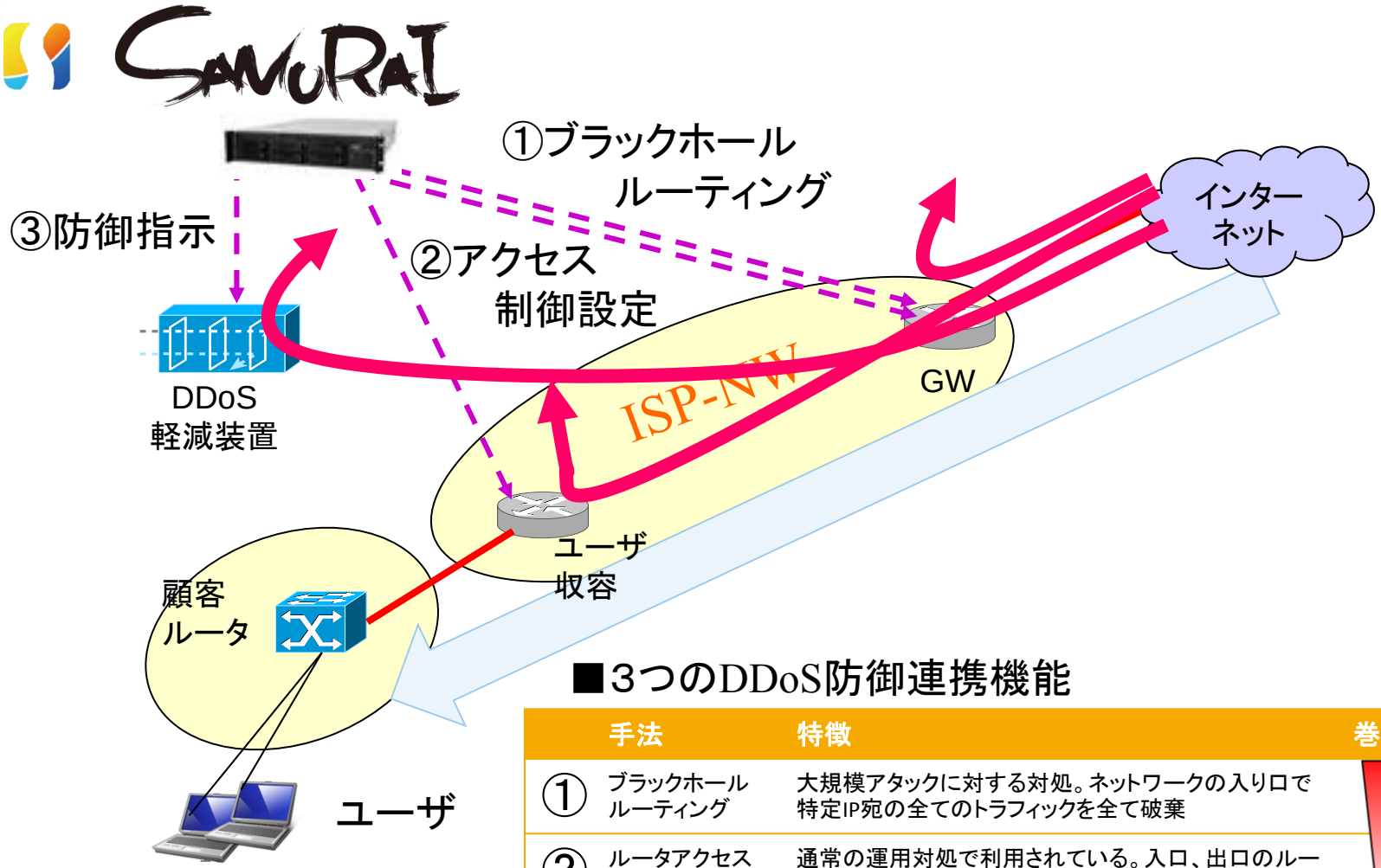
- xflow情報の解析により、オープンリゾルバのリストから「実際に攻撃に使われているホスト」の絞り込みが可能

- また、同一手法により、リストが無くても、「攻撃に使われている可能性のあるホスト」の検出が可能

※ただし、オープンリゾルバかどうかの最終的な判断には、flow情報だけから機械的に判別するのではなく、他の情報と組み合わせることを推奨

DoS/DDoS攻撃に対する防御について

3つのDDoS防御方式

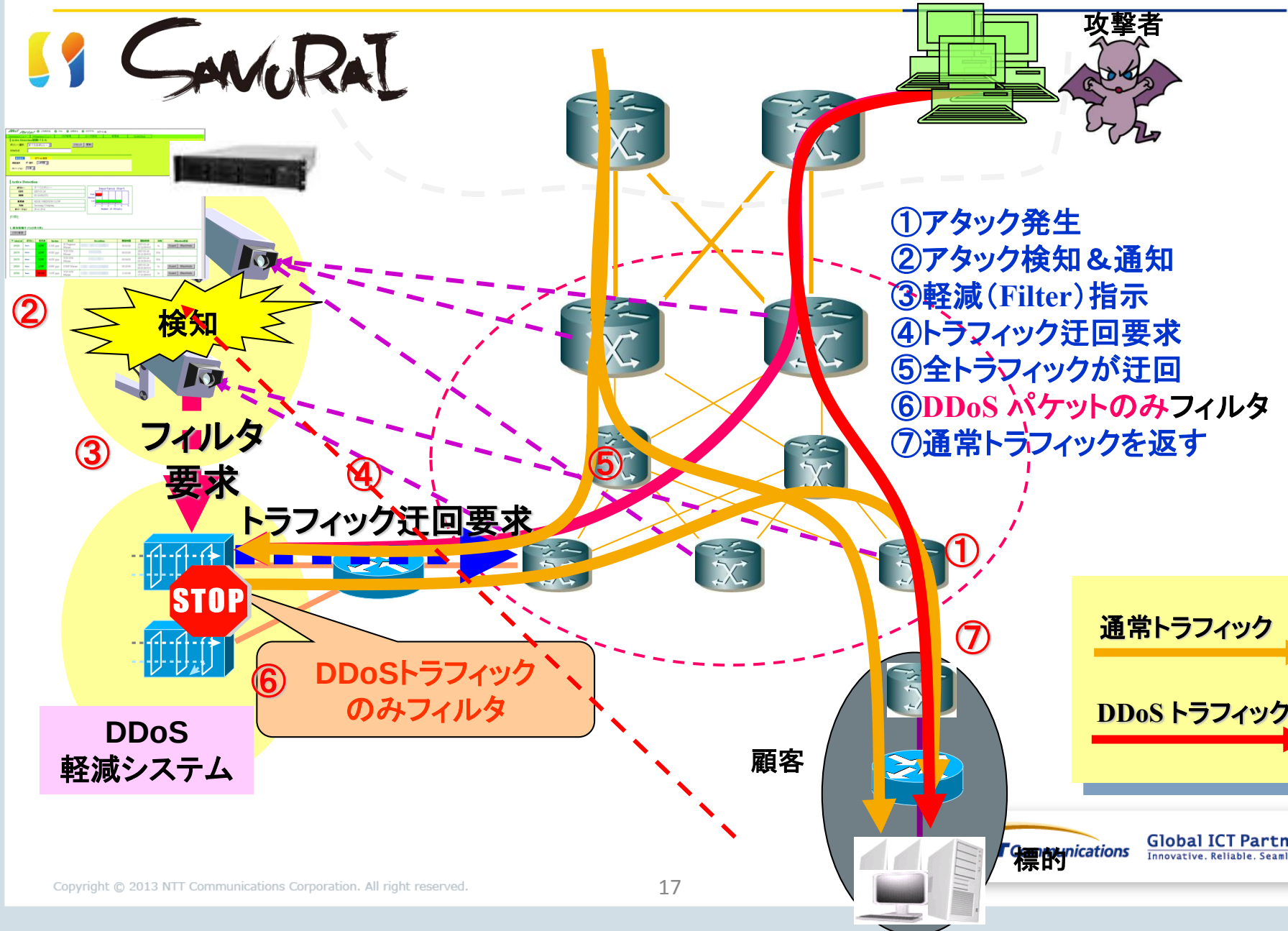


■3つのDDoS防御連携機能

	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。ネットワークの入り口で特定IP宛の全てのトラフィックを全て破棄		
②	ルータアクセス 制御設定	通常の運用対処で利用されている。入口、出口のルータでACL設定にてIP+Portでパケットを破棄		
③	防御システムへの防御指示	きめ細やかなDDoS対処が可能。DDoS軽減専用装置に指示を送り、トラフィックを吸い込み防御実施		

16

DDoS軽減装置との連携



新しい防御手法
～顧客への攻撃の実例から

ここから先は当日会場にて！