マルチホーム DDoS 対策を実現する経路制御技術について『DDoSテストベッド』のご紹介

2015年7月3日

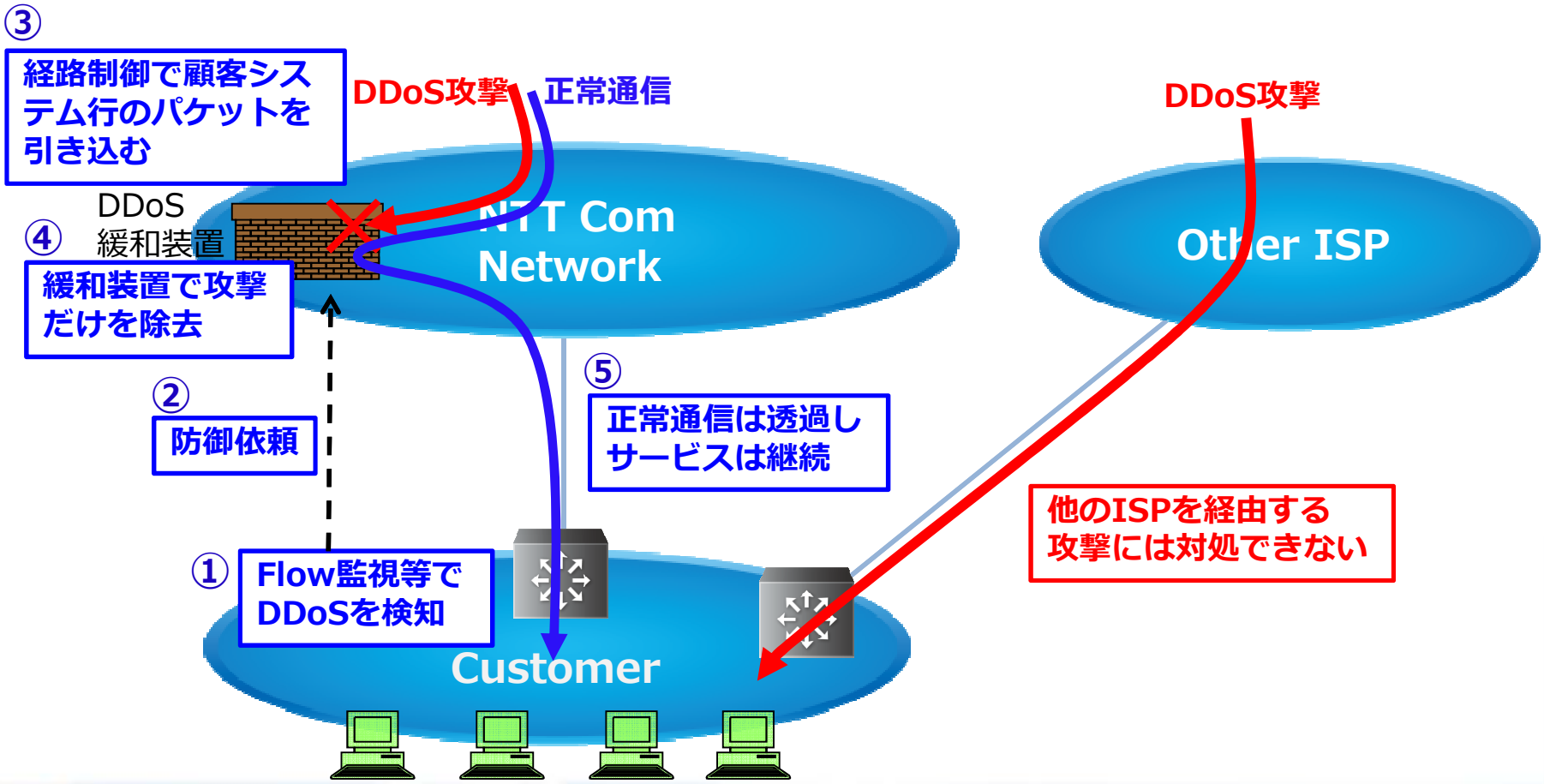
NTTコミュニケーションズ株式会社
技術開発部

脅威を増すDDoS攻撃の傾向

日時	継続時間	攻撃対象	影響内容
2013年3月	4日間	Spamhaus/Cloudflare	300Gbps以上の攻撃 3月22日には、ロンドン、アムステルダム、フランクフルト、香港のIXがトラヒック輻輳が発生、欧州全体に影響
2014年2月	不明	Cloudflareの顧客	NTP増幅攻撃により、400Gbps弱の攻撃
2014年5～6月	14日間	K-optcom社 eo光　DNSサーバ	Web閲覧、メール送受信などに時間がかかる、または表示不可
2014年7月	5日間以上	K-optcom社 eo光　DNSサーバ	Web閲覧、メール送受信などに時間がかかる、または表示不可
2014年6～7月	28日間	セガ 「ファンタシースターオンライン2」サービス	当該期間は、サービス停止 6月27日から、一次サービスを再開
2014年6月	数時間	Evernote	400Gbps以上のDDoS攻撃を受け、サービスに支障が出た 金銭要求
2014年6月	半日	Feedly	Evernoteとほぼ同時にDDoS攻撃を受け、サービス停止 金銭要求。米国ISP等の協力により、サービス復旧
2014年8月	数時間	PlayStation Network (PSN)	ネットワークに接続障害。サービス利用停止
2014年12月	不明	北朝鮮（STAR-KP）	9時間半にわたり北朝鮮がインターネットから孤立

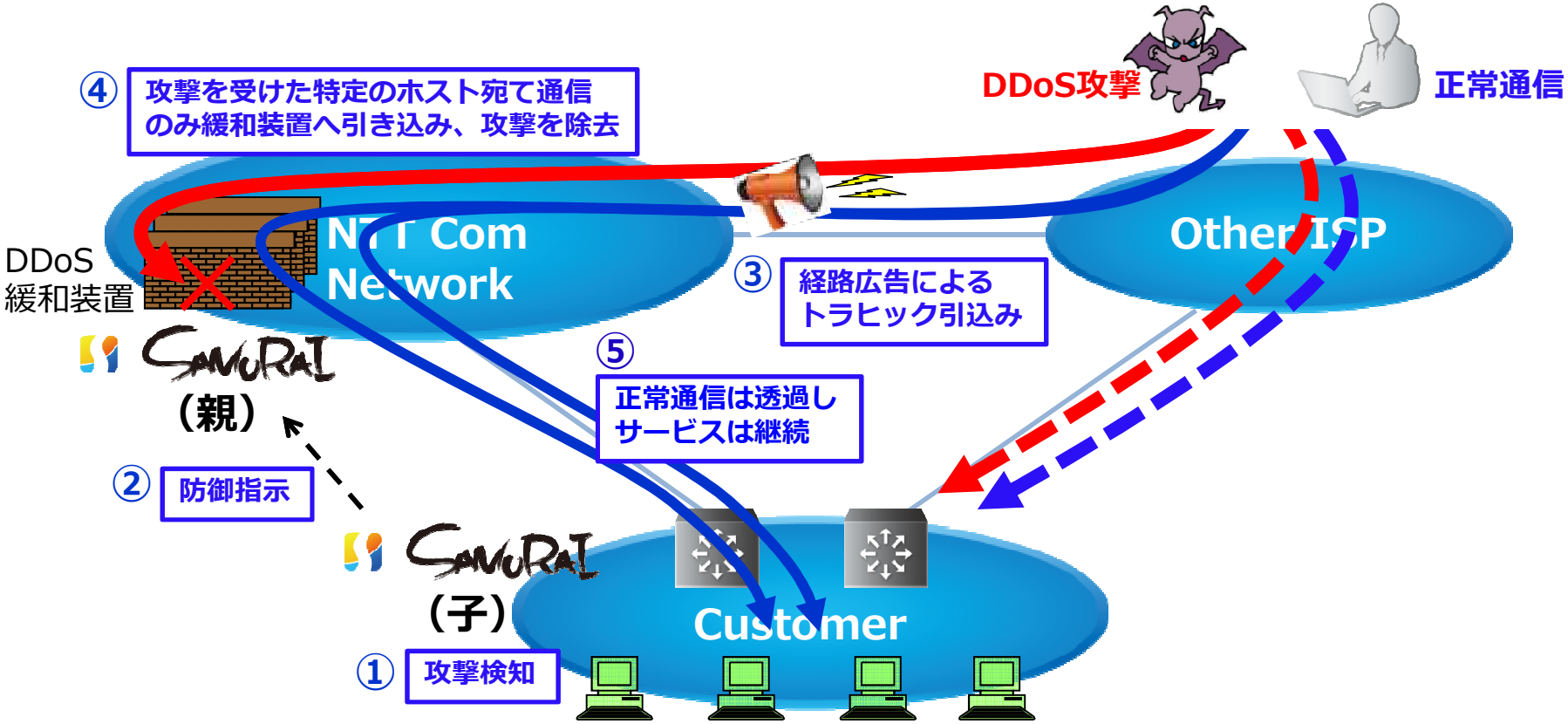
従来のDDoS防御サービスの課題

・お客さまからの防御依頼に基づき、弊社ネットワークを通るDDoS攻撃を緩和
・マルチホームユーザに対して、他のISPを経由する攻撃に対処できない



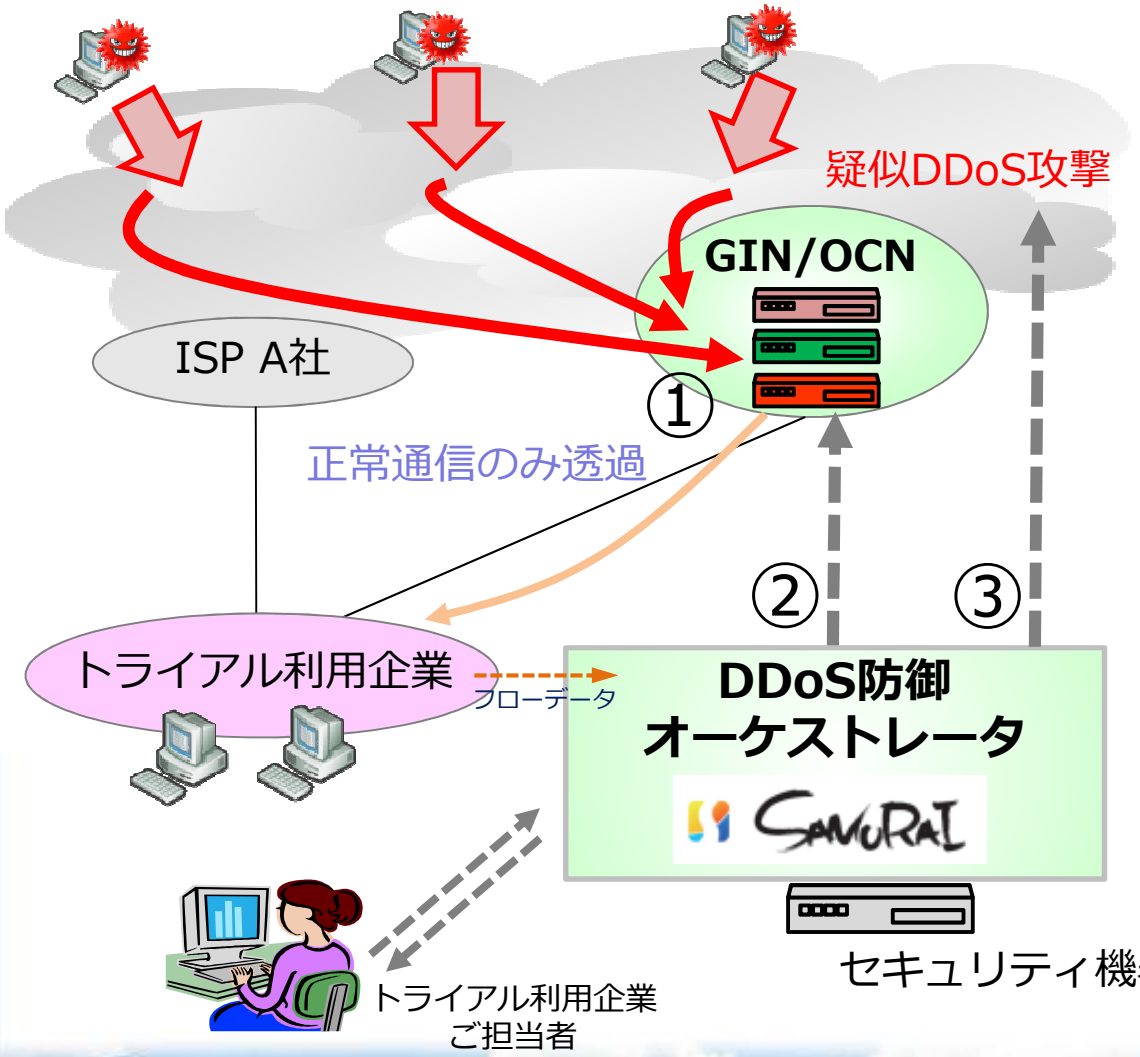
マルチホームユーザをDDoSから守る仕組みを開発

・BGP経路制御により、他ISP経由のトラヒックをNTTCom Networkに引き込み
・トラヒック迂回による正常通信への影響を最小限に抑える
・緩和装置のマルチベンダ化により攻撃タイプに応じたDDoS緩和を実施
・NTTCom NetworkでDDoS緩和/正常通信透過によりマルチホームユーザを防御



DDoSテストベッド トライアルを開始 1/2

～6月8日よりスタート！～



■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テストベッドトライアルを開始 2/2
～トライアルにご参加いただいた組織 (6/5現在)～

順不同 敬称略

■DDoS緩和装置ベンダ様

ARBOR NETWORKS

A10 Networks

radware

■ユーザ参加企業様

internet mf

#show△net
> Go to the next decade

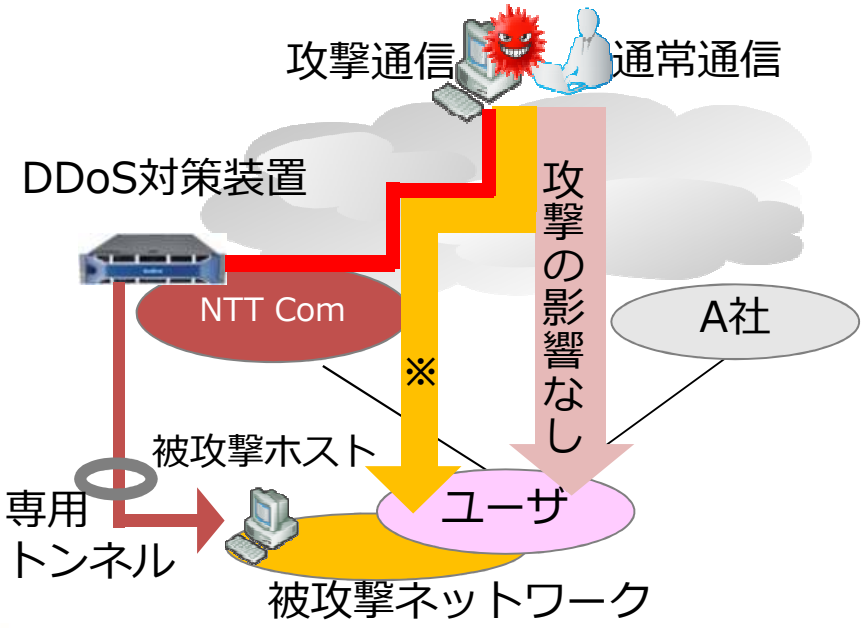
愛媛CATV

mixi

OKIT

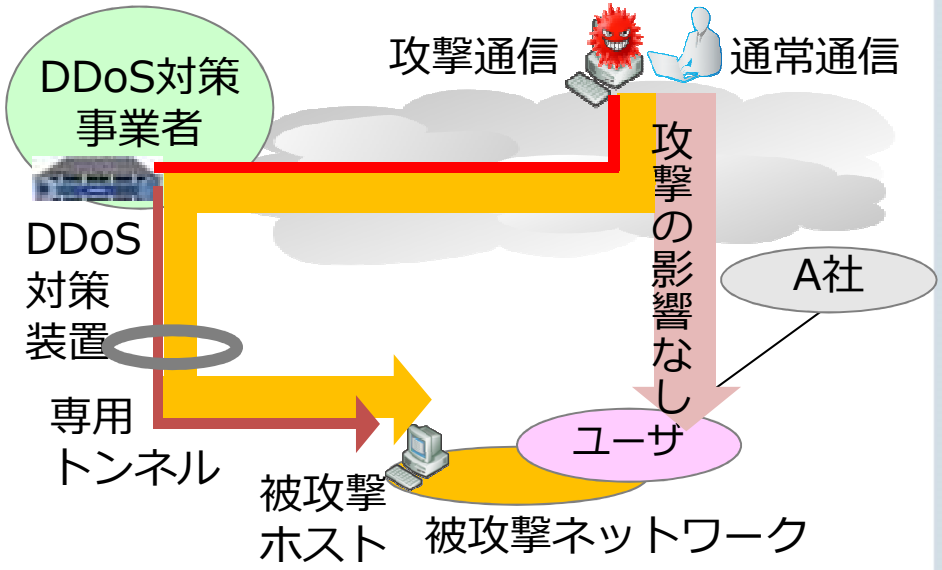
DDoS攻撃の引き込みのトラフィック制御方式

■新方式 (NTT Com)



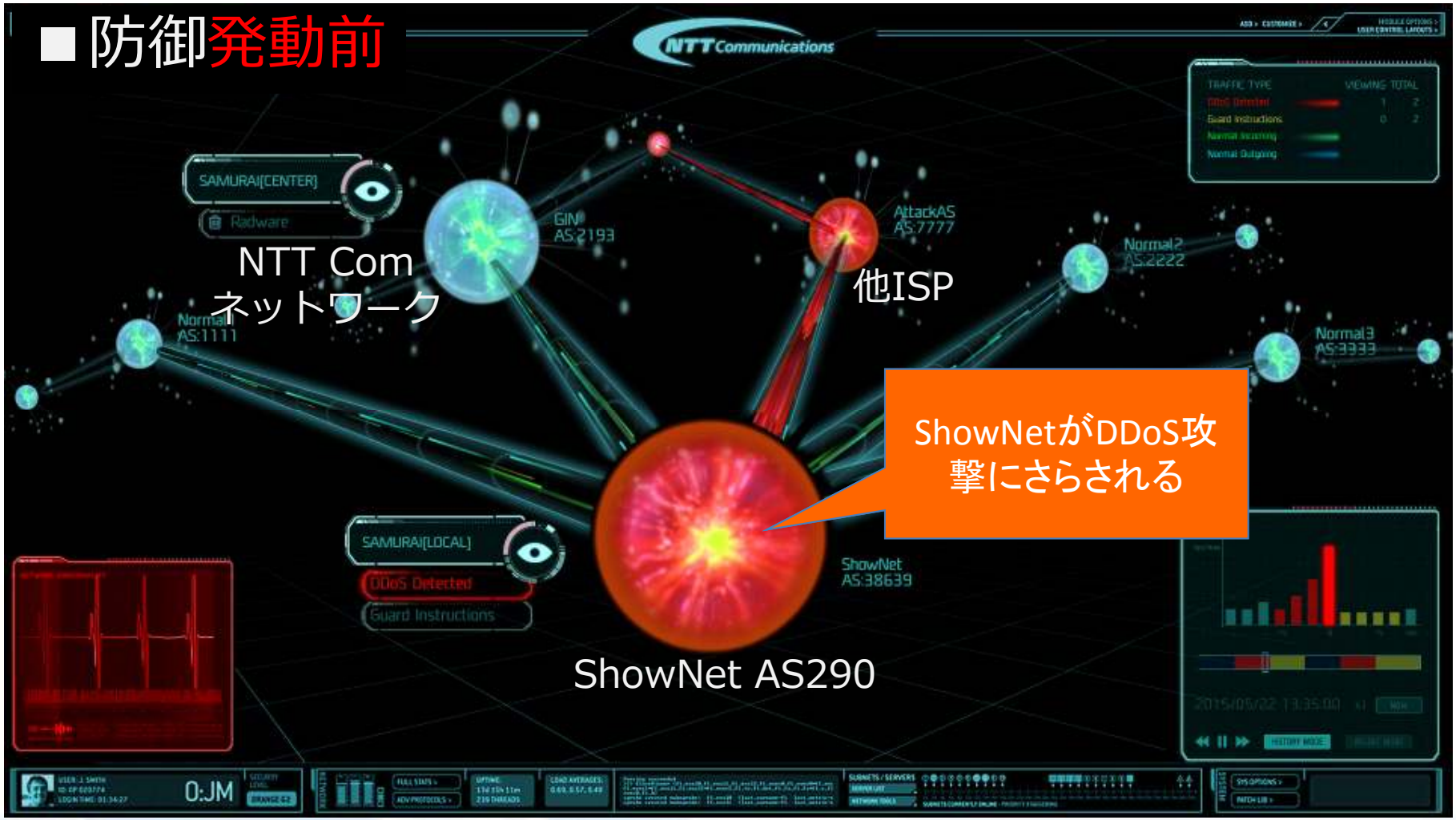
○ NTT Comが引き込んだトラフィックをコム回線でお客様へ直接転送 ⇒ **遅延増加は微小**

■従来方式 (DDoS対策事業者)

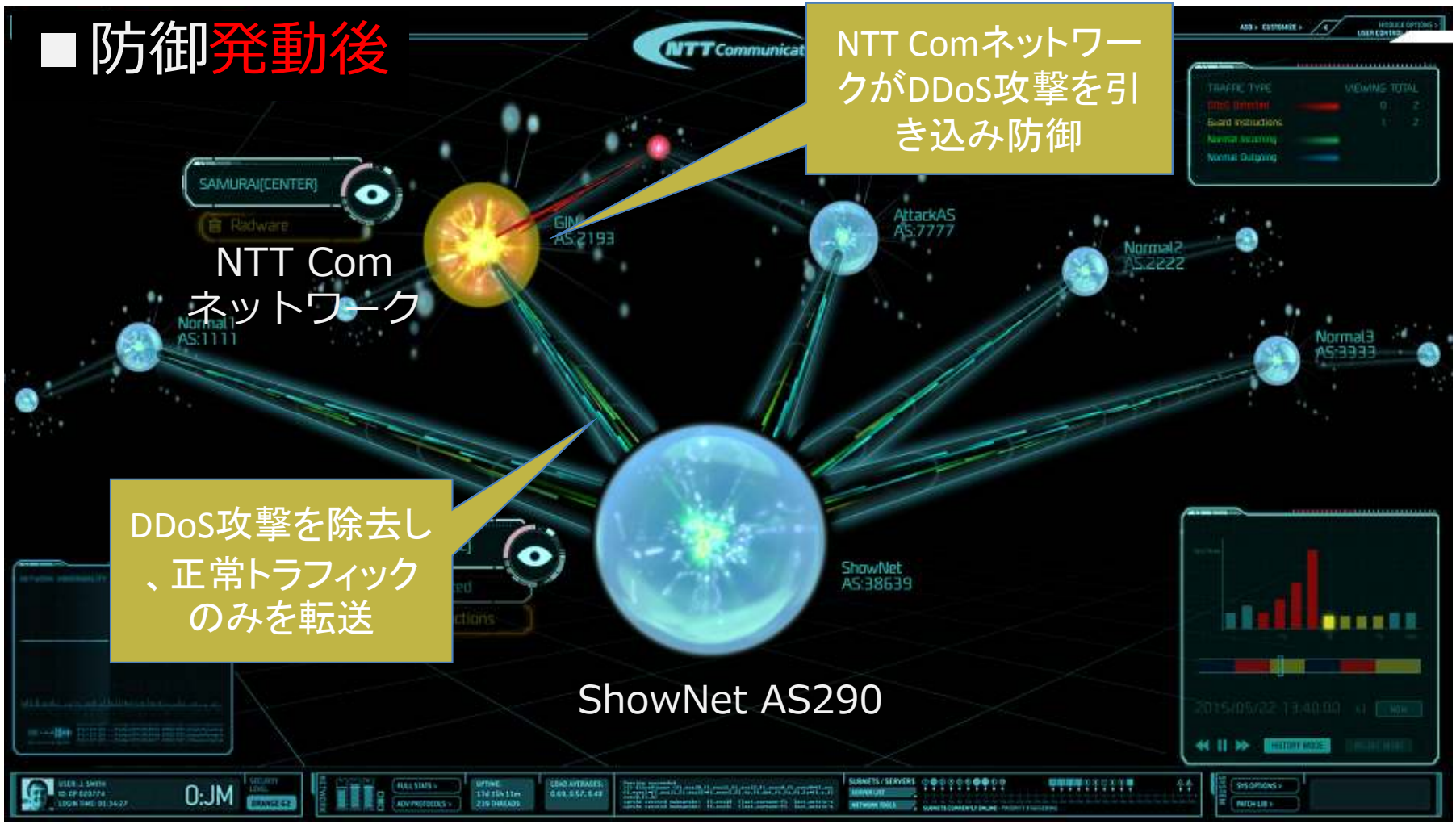


× 引き込んだ通信をトンネル経由で戻す場合、ネットワークの往復時間だけ**遅延が増加**

防御状態可視化 - ShownetNOCにて展示
～ShowNetが他ISPを経由してDDoS攻撃を受ける～



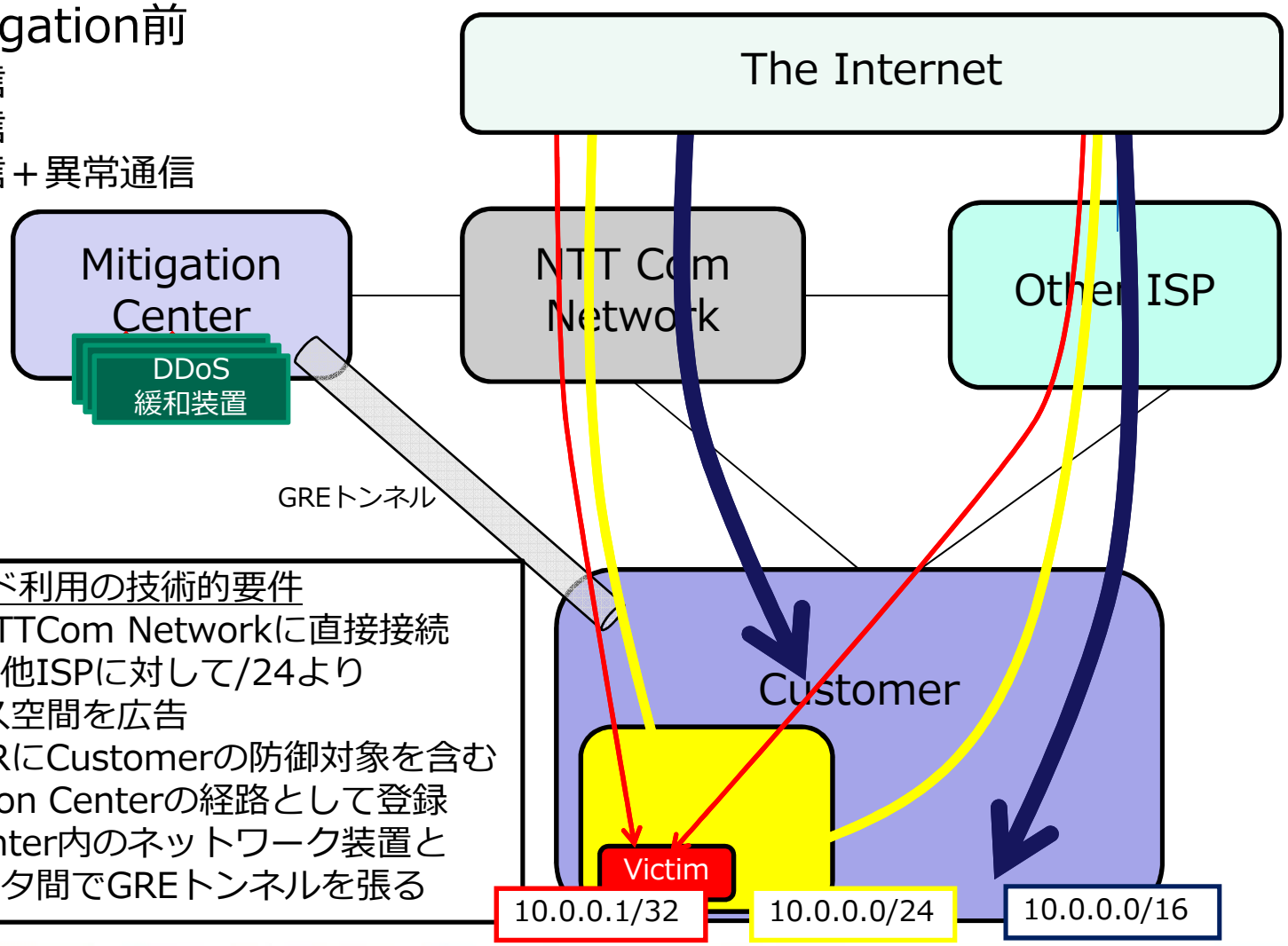
防御状態可視化 - ShowNOCにて展示中！
～NTT Comネットワークが攻撃を一元的に防御～



NTT Comによる攻撃トラフィック制御方式 (1/2)
～引き込み制御＆防御 発動前～

■ DDoS Mitigation前

正常通信
正常通信
正常通信＋異常通信

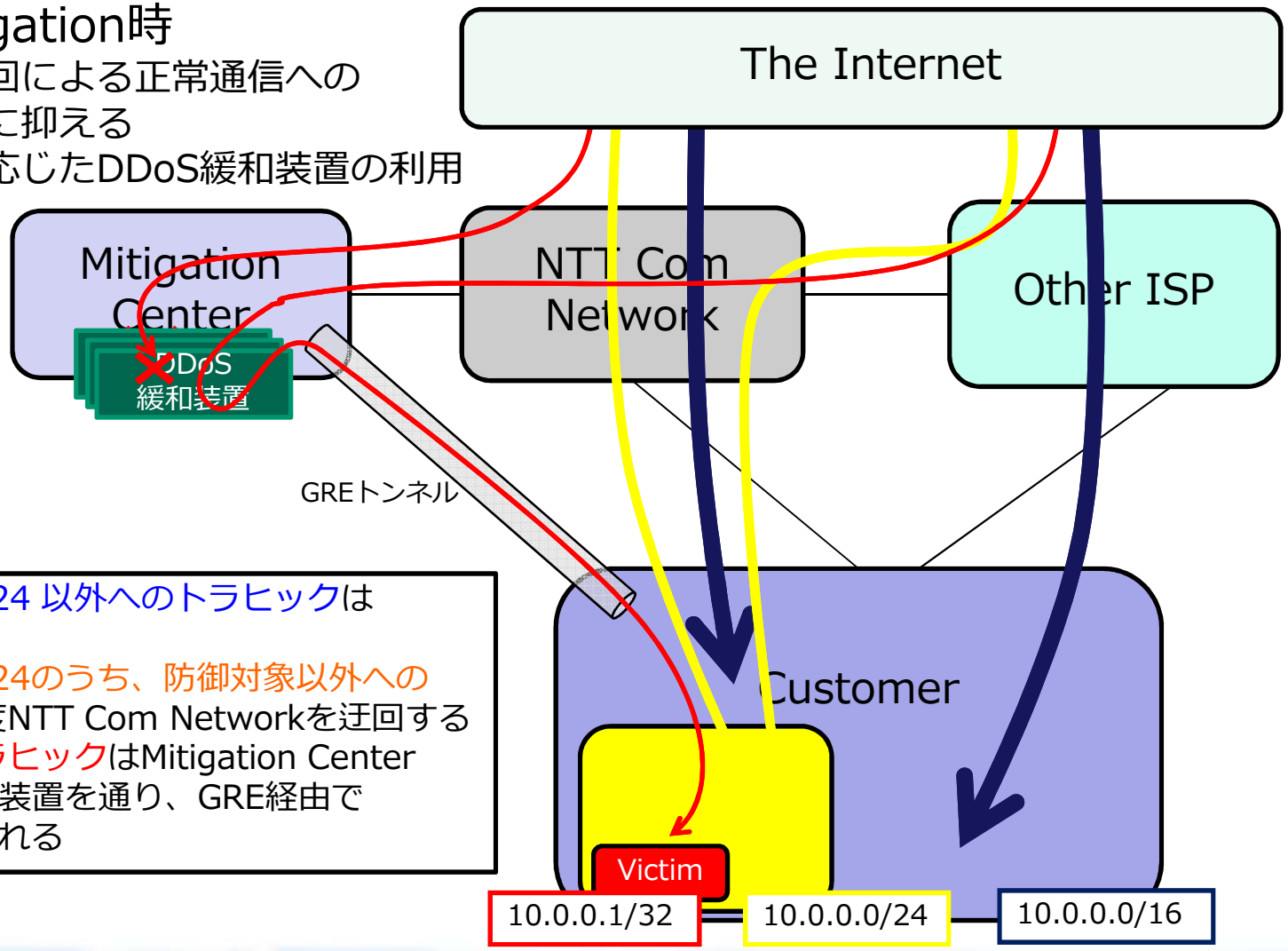


DDoSテストベッド利用の技術的要件
- CustomerはNTTCom Networkに直接接続
- Customerから他ISPに対して/24より大きなアドレス空間を広告
- NTTComのIRRにCustomerの防御対象を含む経路をMitigation Centerの経路として登録
- Mitigation Center内のネットワーク装置とCustomerルータ間でGREトンネルを張る

NTT Comによる攻撃トラフィック制御方式 (2/2)
～引き込み制御&防御 発動後～

■ DDoS Mitigation時

- トラヒック迂回による正常通信への影響を最小限に抑える
- 攻撃タイプに応じたDDoS緩和装置の利用



- ■ 防御対象を含む/24 以外へのトラヒックは通常時通り
- ■ 防御対象を含む/24のうち、防御対象以外へのトラヒックは一度NTT Com Networkを迂回する
- ■ 防御対象へのトラヒックはMitigation CenterおよびDDoS軽減装置を通り、GRE経由でCustomerへ運ばれる