News Release

NTT Communications

2015 年 6 月 4 日

独自開発の経路制御技術を採用した
DDoS 防御オーケストレータシステムのトライアルを開始
～国内通信事業者として初めて、マルチホーム対応 DDoS 対策サービスの実現性を検証～

NTT コミュニケーションズ(略称：NTT Com)は、DDoS 攻撃[*1]を検知・解析・防御する DDoS 防御オーケストレータシステム[*2]において、インターネットを利用する全ての企業や事業者に対する DDoS 防御を可能とする機能拡張を目指し、複数のセキュリティ事業者と共同構築した検証環境にて、2015 年 6 月 8 日よりトライアルを開始します。

本トライアルでは、DDoS 防御時に発生する正常通信の遅延などの影響を極小化する、NTT Com が独自開発した経路制御技術を利用しています。インターネットを利用する全ての企業や事業者を対象としたマルチホーム[*3]対応 DDoS 対策サービスに関するトライアルは国内通信事業者として初めてとなります。

１．背景・目的

DDoS 攻撃の頻度や規模は年々増大しており、インターネット回線の輻輳が企業に大きな損失を与えています。しかし、多くの企業において、多様化・複雑化する DDoS 攻撃に対して、迅速で適切な対策がなされていません。また、ISP/データセンター/クラウド事業者においてもサービス利用者に有効な DDoS 対策を提供できておらず、DDoS 攻撃への防御・対策が企業や事業者全体にとって喫緊の課題になっています。

加えて、複数の ISP とのインターネット接続を持つ場合、これまでは接続 ISP 単位で DDoS 対策を導入する必要がありましたが、ISP ごとにサービスレベルの差があることにより、一元的な対応・管理が困難で、システム運用が煩雑になる、対策までに時間を要するなどの課題も顕在化しています。

これらの課題を解決するため、NTT Com は、インターネットを利用する全ての企業や事業者を対象とした DDoS 防御オーケストレータシステムのマルチホーム対応を含む機能拡張に向けて、機能面・運用面を評価するトライアルを開始します。

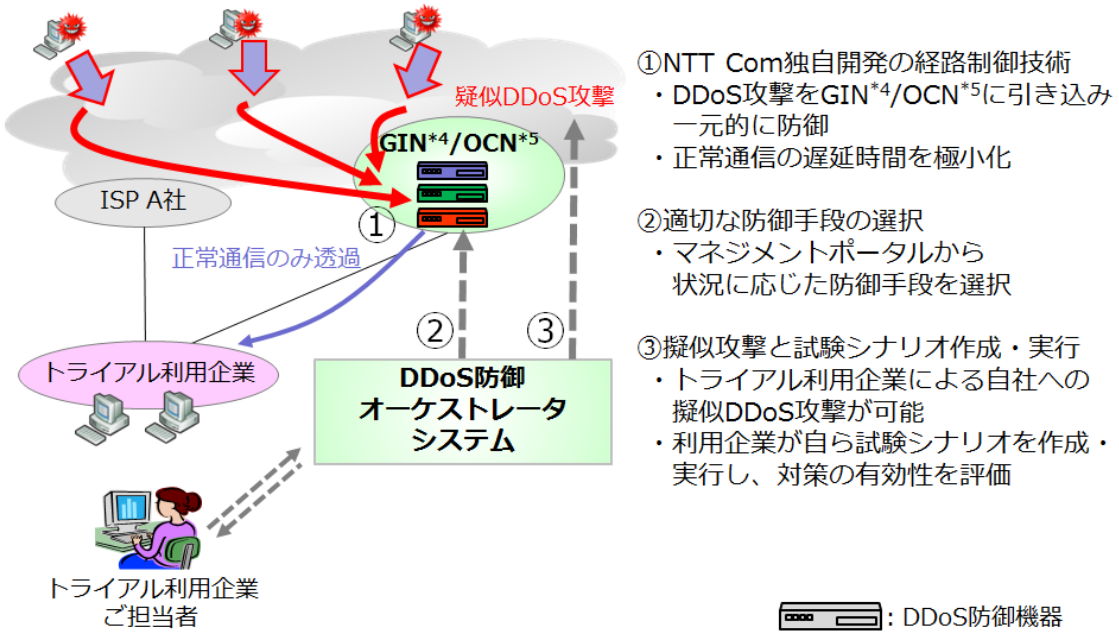
2．トライアルの概要

複数のセキュリティ事業者と共同構築した検証環境にて、関連技術のトライアルを行います。（詳細は別紙 1 参照）

新技術の有効性を検証するとともに、付随する技術的懸念事項の洗い出し、サービス化を見据えてお客さま視点での運用性の評価を行うことを目的としています。

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

トライアルの構成



① NTT Com 独自開発の経路制御技術

NTT Com が独自開発した特許出願済みの経路制御技術により、世界中に展開するインターネット網(GIN*4/OCN*5)内の最適な位置で、攻撃対象宛のトラフィックのみをピンポイントに DDoS 防御機器に引き込み、DDoS 攻撃以外の正常な通信の遅延を極小化することが可能です。

② 適切な防御手段の選択

DDoS 防御機器のマルチデバイス化を実現しています。トライアル利用企業には、DDoS 防御機器を制御するマネジメントポータルが提供され、デバイスごとに異なる機能を意識することなく、適切な防御手段を選択できます。

③ 擬似攻撃と試験シナリオ作成・実行による対策の評価

NTT Com が提供する DDoS 攻撃ポータルから、擬似的な攻撃を発生させることが可能です。トライアル利用企業自身で試験シナリオを作成・実行し、DDoS 防御オーケストレータシステムの有効性を評価していただきます。

3. トライアルへの参加企業名（順不同）

○セキュリティ事業者

A10 Networks 社

Arbor Networks 社

日本ラドウェア株式会社

○トライアル利用組織
インターネットマルチフィード株式会社
Interop Tokyo 2015 ShowNet
株式会社愛媛ＣＡＴＶ
株式会社オキット
株式会社ミクシィ
※組織名掲載を許可して頂いた組織のみを掲載。
※50 音順

4．今後の展開

本トライアルが完了次第、DDoS 攻撃を検知・解析・防御する独自開発 DDoS 防御オーケストレータシステムを機能拡張し、より高度な DDoS 対策サービスの提供を予定しております。

*1: Distributed Denial of Service 攻撃。コンピュータネットワークを通じて行う攻撃の一種。複数のネットワークに分散する大量のコンピュータから、一斉に特定のネットワークやサーバなどへ不要なパケットを送出し、通信容量やサーバの処理許容量をあふれさせることでサービスを停止させてしまう攻撃。

*2: NTT Com で独自開発したトラフィックの可視化および DDoS 攻撃を検知・解析・防御するシステム。
通称「SAMURAI」。NTT Com のネットワークサービスのオプションとして 2009 年より提供しているトラフィック解析ツール<http://www.ntt.net/service/traffic.html>にて活用されており、2015 年 3 月より、NTT Com が提供するクラウドサービスにおいて基盤を守るためにも活用されています。

*3: 複数の ISP とインターネット接続を持つこと。

*4: 国際インターネット接続サービス「グローバル IP ネットワーク」
サービス紹介サイト　<http://www.ntt.net/>
*5: 法人向けインターネット接続サービス
サービス紹介サイト　<http://www.ocn.ne.jp/business/>

（別紙 1）**DDoS 防御検証環境の詳細**

NTT Com では、通信事業者やセキュリティ事業者とともに DDoS 防御オーケストレータシステムの新しい機能や効果の評価･検証に参加して頂けるトライアル利用企業を募集しています。

本トライアルへの参加期間中、トライアル利用企業が実際に DDoS 攻撃を受けた場合、DDoS 防御オーケストレータシステムを利用した防御および対処が可能です。

■トライアルにおける各社の役割

【NTT Com】

- DDoS 防御オーケストレータシステムの提供
  - フロー技術を利用したトラフィック解析・DDoS 攻撃検知機能
  - DDoS 防御機器を制御するマネジメントポータル
  - 擬似的な攻撃を発生させる DDoS 攻撃ポータル
- 経路制御関連の技術支援

【セキュリティ事業者】

- NTT Com の DDoS 防御オーケストレータシステムと連携する DDoS 防御機器の提供
- DDoS 防御機器に関する技術サポート

【トライアル利用企業】

- トライアル利用企業への影響や DDoS 対策の有効性を評価

■トライアルの内容

①トライアル利用企業が、DDoS 攻撃ポータルを使って自社システムへの疑似攻撃を実施
②マネジメントポータル上で DDoS 対策を選択し、防御を実施
③対策の有効性を評価