

IDC フロンティア ネットワークサービス

DDoS 対策

1. サービス概要

IDC フロンティア ネットワークサービス DDoS 対策(以下本サービス)は、IDC フロンティアのバックボーンネットワーク上に設置された DDoS 検知防御システムにより、お客様ネットワークに対するトラフィックを常時引込により監視し、DDoS 攻撃を検知した場合、自動的に不正トラフィックのフィルタリングを実施します。

- お客様ネットワークへの流入前にフィルタリングするので、お客様通信機器に負荷を与えません
- 悪意のあるトラフィックのみに対して選択的に遮断します
- DDoS 攻撃検知、フィルタリングまで自動的に行われます(振り舞い検知による動的フィルタリング)
- 10 ギガビットクラスの攻撃にも対応可能です
- クラウドサービスご利用のお客様もご利用可能です

2. サービス提供内容

2.1 サービスタイプ

本サービスでは、以下3種類の品目をご用意しております。

品目	内容	契約単位
アクセスレポート	・ フロー情報のレポートを提供します。	1 契約回線単位 (ポリシー、設定値が変わる場合は、別契約となります)
ガード [スタンダード]	・ 当社標準ポリシーに基づいて、複数の検知種別に対応する DDoS 検知防御サービスを提供します。 ・ 検知種別、設定値は、当社指定とさせていただきます。	セルフクラウドの場合 20IP アドレスが 1 単位 (ポリシー、設定値が変わる場合は、別契約となります)
ガード [カスタム]	・ お客様環境への導入時にモニタリング(エージング)を実施し、計測されたデータを基に検知種別攻撃毎に任意のポリシーの設定が可能です。	

2.2 サービス仕様

検知/対策ポリシー

ネットワーク上での振り舞いをチェックし、統計学的に分析することで悪意あるアクセスを検知し、該当するトラフィックを遮断するためのシグネチャ(フィルター)を自動生成する動的シグニチャで DoS/DDoS 攻撃を緩和、防御いたします。さらに静的なシグネチャを併用することで、アプリケーションレベルの攻撃や既知の脆弱性に対する防御も可能となります。

説明	アクセスレポート	ガード [スタンダード]	ガード [カスタム]
推奨帯域	全帯域	全帯域	全帯域
提供内容	フロー情報レポート	DoS / DDoS 攻撃防御	DoS / DDoS 攻撃防御 (個別)
Behavior DoS protection	-	動的シグネチャ	個別設定*1
SYN Protection	-	推奨値	
DNS Protection	-	推奨値	
HTTP Mitigator	-	-	
Connection limit	-	-	
Packet Anomalies	-	推奨値	
Black/White list	-	-	
通知ポリシー ^{*3}	-	防御後及び障害時通知(メール) ^{*2}	個別設定 *3

*1: bps または pps 単位で任意の値で設定可能です。初期導入時にトラフィックをモニタリングのうえ、推奨値をご提示致します。
その他の検知種別攻撃については、個別相談とさせていただきます。

- *2: DDoS 攻撃防御後に、予めご登録いただいたメールアドレスに自動送信メールにて通知します。
- *3: 「ガード[カスタム]」をご利用の場合は、ご要望に応じて当社スタッフから電話でご連絡することも可能です。

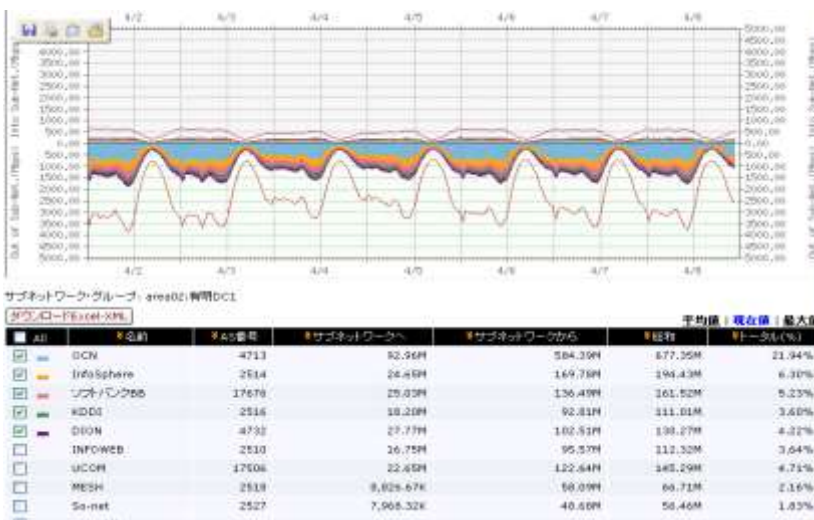
アクセスレポート

解析されたデータは、グラフによるレポートとして、カスタマーポータルにてお客様にご提供いたします。

※ フロー情報レポートの保存期間は 1 年間です。

アクセスレポート 検知項目説明

項目	概要
Host Total Traffic	インターネットからデータセンターに対する通信のうち、1 つの IP に流入するトラフィックの総量
UDP Flooding	UDP パケットを大量送信し帯域や機器リソースを飽和させる
TCP RST Flooding	TCP RST パケットを送信し、セッションを強制的にリセットする
ICMP Misuse	ICMP パケットを大量送信し帯域や機器リソースを飽和させる
TCP SYN Flooding	TCP SYN パケットを送信し、セッションを強制的にリセットする

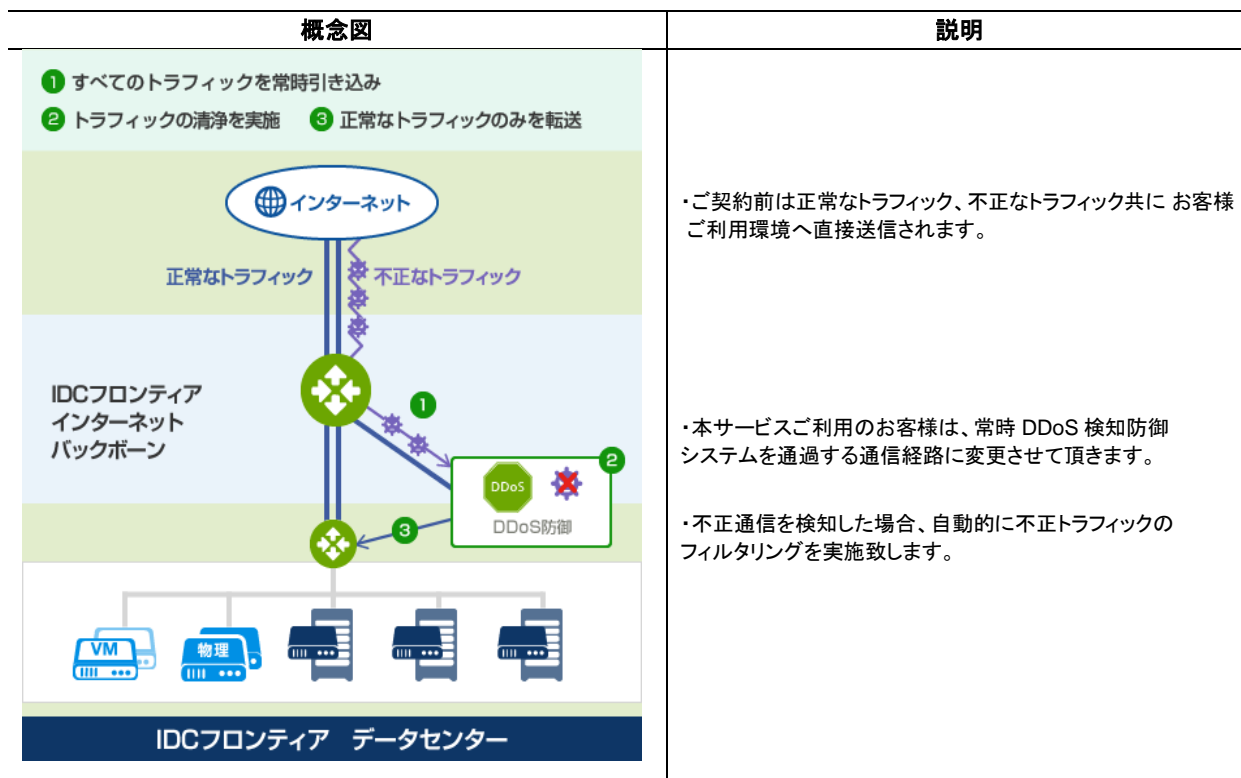


2.3 ご利用可能データセンター/クラウドサービス

本サービスをご利用可能なデータセンターおよびクラウドサービスは下表のとおりです。

サービス	リージョン(ゾーン) /DC	アクセスレポート	ガード [スタンダード]	ガード [カスタム]
クラウド	セルフクラウド	EAST リージョン (白河ゾーン)	○	○
		EAST リージョン (東京ゾーン)	○	○
	マネージドクラウド	EAST リージョン	○	○
		WEST リージョン	○	○
データセンター	福島白河 DC	○	○	
	東京有明 DC1	○	○	
	東京新宿 DC	○	○	
	大阪吹田 DC	○	○	
	アジア・フロンティア	○	○	
	北九州 DC	○	○	
	東京新川 DC	○	○	
	東京日本橋 DC	○	○	
	東京虎ノ門 DC	○	○	
	神奈川横浜 DC	○	○	

2.4 概念図



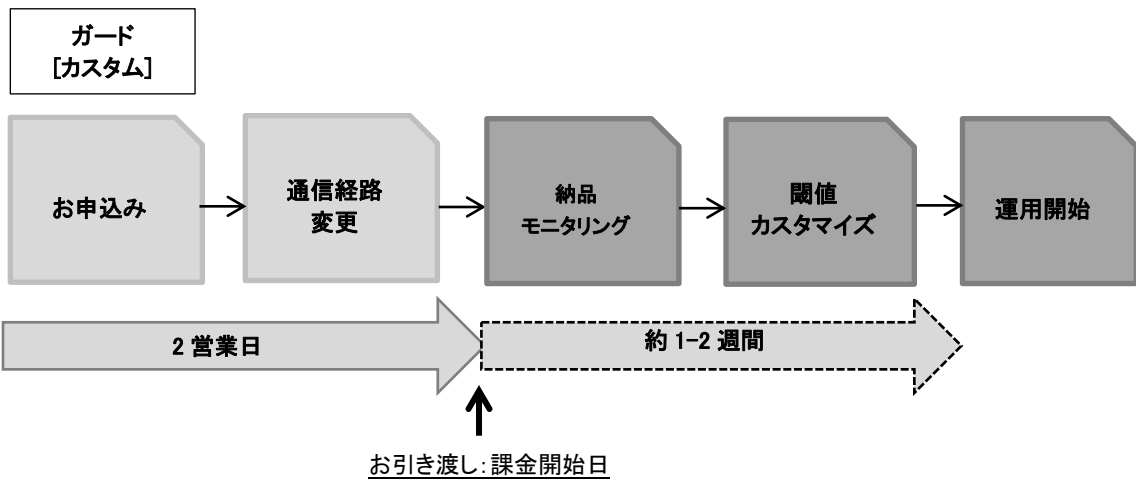
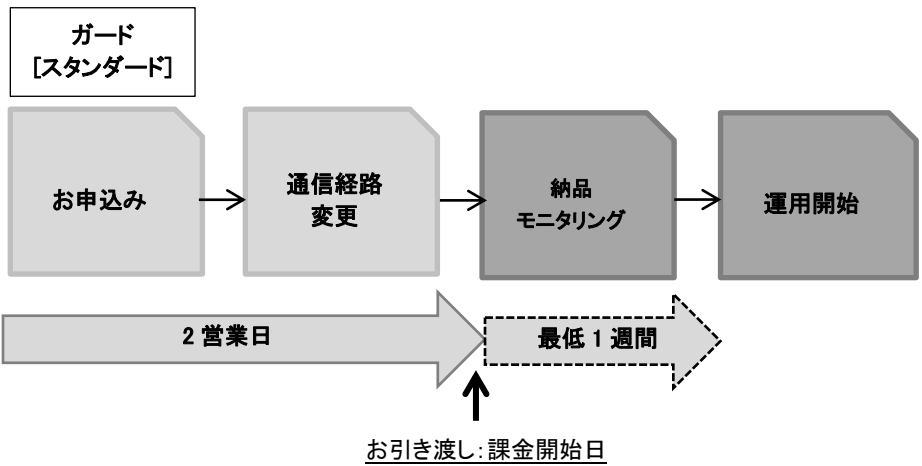
2.5 導入/運用保守

項目	項目	説明	ガード [スタンダード]	ガード [カスタム]
設定/導入	通信経路変更	常時 DDoS 検知/防御システムを通過する通信経路に変更させていただきます。	○	○
	モニタリング	お客様ネットワーク環境を約 1-2 週間モニタリングします。	○	○
	閾値のカスタマイズ	各種ポリシーの閾値やフィルタリング・通知方法の最適値をお客様と協議の上カスタマイズさせていただきます。	—	○
	閾値等の設定	各種ポリシーの閾値やフィルタリング・通知方法を設定します。	○	○
	設定投入	各種ポリシーを DDoS 対策システムに設定します。	○	○
運用	トラフィックサンプリング	お客様トラフィックをサンプリングし、異常を監視します。	○	○
	トラフィックフィルタリング	DDoS 検知時、自動的にフィルタリングを実施します。	○	○
	フィルタリング解除	DDoS 終了判定後、自動的にフィルタリング終了します。(全自動)	○	○
	フィルタリング解除	DDoS 終了判定後のにフィルタリング解除タイミングを協議の上設定致します。	—	○
設定変更	閾値等の変更	閾値やフィルタリング・通知方法の設定を変更します。	—	○

保守/サポート

項目	受付時間	対応時間	ガード [スタンダード]	ガード [カスタム]
障害対応	24 時間 365 日 (電話・メール)	24 時間 365 日	○	○
設定変更	24 時間 365 日 (カスタマーポータル)	平日 9:00-17:00	—	○
各種問い合わせ	24 時間 365 日 (カスタマーポータル)	平日 9:00-17:00	○	○

導入フロー



3. サービスご利用条件

3.1 ご利用条件

- IDC フロンティアのデータセンターサービスまたはクラウドサービスを利用していること。

3.2 ご利用上の制限、及び注意事項

- フィルタリング後、一定期間の経過観察を行ったうえで対策設定を自動解除します。
自動解除を希望されないお客様については、お客様とあらかじめ調整のうえ実施するものとします。
- 本サービスの性質上すべての攻撃通信を防御できるものではない点予めご承知おきください。
- 外部からの攻撃が弊社内で定める閾値(非公開)を著しく超過し、本サービス提供に支障を来すと判断される場合、上位プランへの移行をお願いする場合がございます。

3.3 最低利用期間

- 本サービスの最低利用期間は1ヶ月となります。
- 解約のお申し出がない場合、1ヶ月毎の自動更新となります。

3.4 免責等

- 当社は、本サービスについて、お客様が意図する特定利用目的への適合性、有用性等に関し、いかなる保証責任も負いません。
- 当社は、契約約款記載の免責事項に加え、本サービスの利用によって生じた契約者または第三者の損害に対して、いかなる責任も負わないものとします。

4. 標準納期

本サービスの標準納期は以下のとおりです。

標準納期	2 営業日
------	-------

*: お申込の内容によっては、別途、日数が必要となる場合があります。

*: お申込書受領の翌営業日を1営業日目として起算いたします。

*: サービス提供に必要な情報が全て揃っていることが前提となります。

株式会社 IDC フロンティア

〒160-0004 東京都新宿区四谷 4-29

www.idcf.jp

Copyright ©2013 IDC FRONTIER INC. All rights reserved.

記載されている会社名、商品名は、各社の登録商標または商標です。

Doc : SS-PUB-R0091-DDoS_20141001_ver11.docx