IDC フロンティア ネットワークサービス
DDoS 対策

Version: 1.9
Date Released: 2022/4/19

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し、お客様通信機器への負荷軽減が可能です
- 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

1.1. サービスメニュー

本サービスでは、以下 2 種類、4 品目をご用意しております。

タイプ		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 • 本タイプには DDoS 検知・防御は含まれません	1 回線番号単位 IDCF クラウドの場合 20IP アドレスが 1 単位
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、当社指定となります	
	[カスタム]	• 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 • 追加機能設定及び静的フィルター機能を提供します • サマリーレポートを提供します	

*:本サービスは、当社クラウド、データセンター、ネットワークサービス用に、当社が割り当てた静的 IP アドレス単位の防御が可能です。

1.2. 提供範囲

本サービスをご利用可能なデータセンター及びクラウドサービスは下表の通りです。

サービス区分			提供場所	アクセスレポート	ガード [スタンダード]		ガード [カスタム]	
					非常時タイプ	常時タイプ	非常時タイプ	常時タイプ
クラウド	IDCF クラウド	インフィニットLB	東日本リージョン 1	○*	○*	○*	○*	○*
			東日本リージョン 2	○*	○*	○*	○*	○*
			東日本リージョン 3	○*	○*	○*	○*	○*
			西日本リージョン	○*	—	○*	—	○*
データセンター			白河データセンター	○	○	○	○	○
			有明データセンター	○	○	○	○	○
			日本橋データセンター	○	○	○	○	○
			府中データセンター	○	○	○	○	○
			吹田データセンター	○	—	○	—	○
			北九州データセンター	○	—	○	—	○

*:インフィニット LB 固定パブリック IP アドレスオプションを申し込む必要があります

2. サービス仕様

2.1. アクセスレポート

ネットワークトラフィックのフロー情報を、グラフ化したレポートとして、カスタマーポータルにてお客様にご提供いたします。

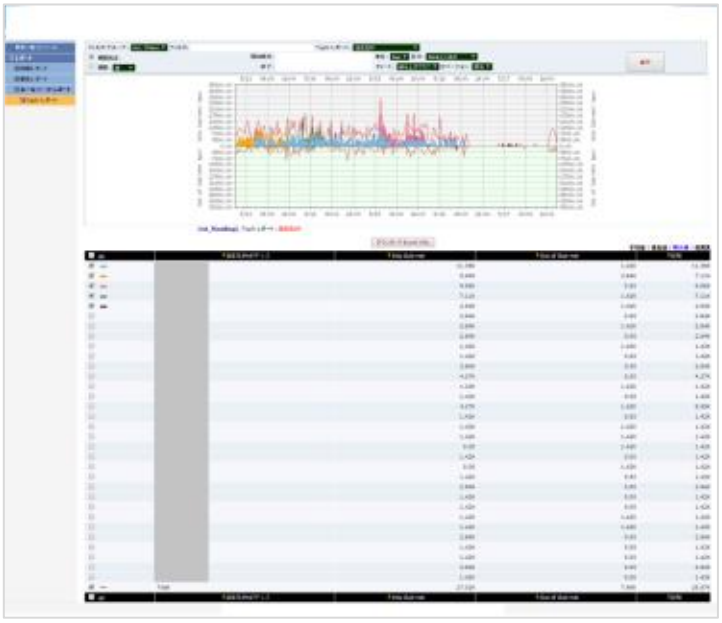
アクセスレポート 項目説明

項目	レポート名	内容
異常一覧コンソール	—	当社指定の値を超えた通信の一覧を表示します
詳細レポート	トップトーカー	お客様 IP アドレス毎の通信量のトップ 10 を表示します
属性レポート	アプリケーション	アプリケーション単位の通信量を表示します
	プロトコル	プロトコル単位の通信量を表示します
	プロトコル＋ポート	プロトコル/ポート単位の通信量を表示します
	パケットサイズ	パケットサイズ(bytes/packet)単位の通信量を表示します
ルールベース・レポート	TopN レポート	送信元毎の、トラフィック量（bps）、パケット数（pps）の値を、順位付けして表示します

*: フロー情報レポートの保存期間は 1 年間です

アクセスレポート表示例

TopN レポート



異常一覧コンソール

詳細レポート

※本サービスは以下の「2.2 ガード」とは別にご契約が必要なサービスとなります。

2.2. ガード [スタンダード/カスタム]

DoS/DDoS 攻撃の緩和、防御機能を提供します(10Gbps まで対応可能)。本サービスには 2 つのタイプがあります。非常時タイプはトラフィックベースで検知するため、大規模なトラフィックを伴う攻撃の防御に向いています。常時タイプは大規模なトラフィックに加え、大規模なトラフィックが発生しないようなアプリケーションへの攻撃も検知可能です。

[非常時タイプ]：攻撃検知時に通信経路を切替え、不正トラフィックのフィルタリングを実施します。

[常時タイプ]：全通信を常時学習し、不正トラフィックのフィルタリングを実施します。

<table>
<tr><th></th><th colspan="2">ガード[スタンダード]</th><th colspan="2">ガード[カスタム]</th></tr>
<tr><th></th><th>非常時タイプ *1</th><th>常時タイプ</th><th>非常時タイプ *1</th><th>常時タイプ</th></tr>
<tr><td>攻撃検知時の通信経路切替</td><td>あり</td><td>なし</td><td>あり</td><td>なし</td></tr>
<tr><td>防御可能攻撃種別</td><td colspan="4">• Syn Flood
• UDP Flood
• ICMP Flood
• IGMP Flood
• DNS Flood
• TCP RST Flood
• TCP ACK+FIN Flood
• TCP SYN+ACK Flood
• TCP Fragmentation Flood</td></tr>
<tr><td>追加機能設定</td><td colspan="2">不可</td><td>• 静的フィルター適用
• 検知閾値チューニング*2
• WhiteList/ BlackList
• 攻撃種別のカスタム</td><td>• 静的フィルター適用
• WhiteList/ BlackList
• 攻撃種別のカスタム</td></tr>
<tr><td>防御フィルター終了時</td><td>手動復旧</td><td>自動復旧</td><td>手動復旧</td><td>自動復旧</td></tr>
<tr><td rowspan="2">通知方法</td><td rowspan="2">閾値の超過時及び
防御終了時、
障害時通知(メール)</td><td rowspan="2">防御終了時及び
障害時通知(メール)</td><td>閾値の超過時及び
防御終了時、
障害時通知(メール)</td><td>防御終了時及び
障害時通知(メール)</td></tr>
<tr><td colspan="2">防御システムの定期通知サマリーレポート*3
（日毎、週毎、月毎から選択）</td></tr>
<tr><td>推奨帯域</td><td colspan="4">全帯域</td></tr>
</table>

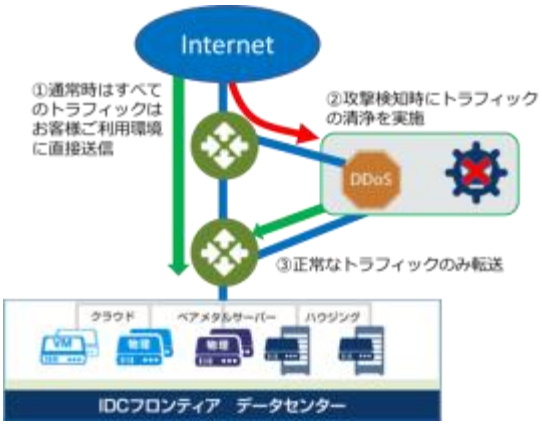
*: 全通信の攻撃検知、緩和、防御を実施しておりますが、攻撃元と攻撃先が当社サービス同士となる、当社ネットワーク内での折り返し通信については検知防御出来ません。また、トラフィック量や通信の内容から判断するサービスの特性上、誤検知による防御が発生した場合、正常通信を遮断してしまう可能性があります。

*1: 通信経路切替までの間、攻撃による通信影響が続く場合があります。

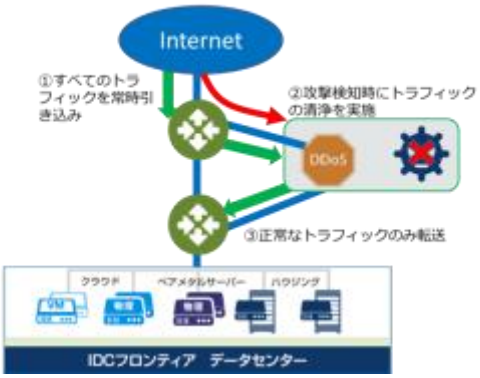
*2: 初期導入時は当社指定の閾値を設定させて頂きます。お客様ご希望により bps、pps の閾値を変更することが可能です。

*3: 攻撃検知時の情報が記載されたレポートが定期的に送付されます。また攻撃が検知されない場合でも本レポートは選択したタイミングで送付されます。

2.3. 概念図

ガード [スタンダード、カスタム] [非常時タイプ] 概念図	説明
	● 本サービスご利用のお客様は、検知閾値の超過時（非常時タイプ）にトラフィックを DDoS 防御 システムを通過する通信経路に変更させて頂きます。 ● 通信経路変更後から検知された不正トラフィックのフィルタリングを実施致します。

*: 不正トラフィックの終了時には、手動で正常な経路に戻します。

ガード [スタンダード、カスタム] [常時タイプ] 概念図	説明
	● 本サービスご利用のお客様は、常時 DDoS 防御システムを通過する通信経路に変更させて頂きます。 ● 不正通信を検知した場合、自動的に不正トラフィックのフィルタリングを実施致します。

3. 納期

本サービスの標準納期は以下のとおりです。

新規導入	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。

*: 設定内容合意の翌営業日を 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。

4. サービス運用保守

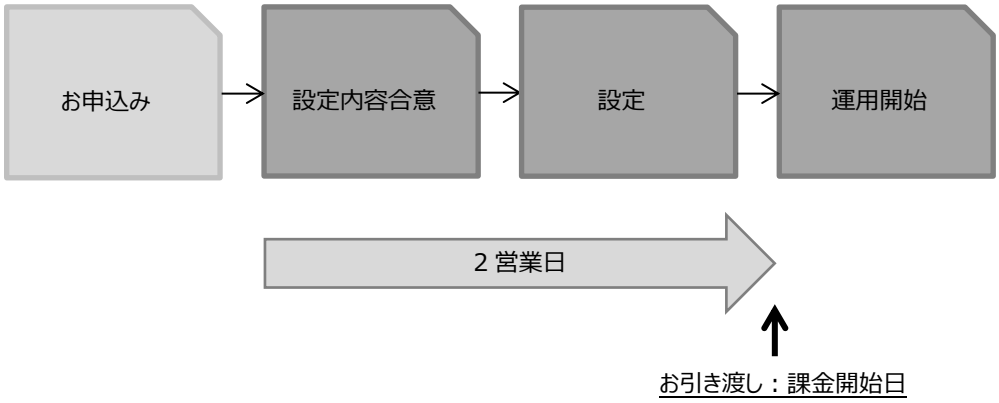
4.1. 導入/運用保守

項目	内容	説明	ガード [スタンダード]		ガード [カスタム]	
			非常時タイプ	常時タイプ	非常時タイプ	常時タイプ
導入設定	ポリシー設定	各種ポリシーやフィルター・通知方法を設定します。	○	○	○	○
	通信経路変更	DDoS 検知/防御システムを常時通過する通信経路に変更させて頂きます。	—	○	—	○
	モニタリング（学習期間）	お客様ネットワーク環境をモニタリングし学習期間といたします。（通常 5 営業日）	—	○	—	○
	追加機能設定カスタマイズ	各種ポリシー設定やフィルタリング・通知方法の最適値を当社からの案内若しくはお客様からご提示頂き、カスタマイズさせて頂きます。	—	—	○	○
	防御機能有効化	DDoS 防御機能を有効化します。	○	○	○	○
運用	①トラフィック切替	閾値超過時、自動的に通信をクリーニングする経路に切り替えます	○	—	○	—
	②トラフィックフィルタリング（クリーニング）	DDoS 検知時、自動的にフィルタリング(クリーニング)を実施します。	○	○	○	○
	③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。	○	○	○	○
	④トラフィック切り戻し	検知の閾値を下回った場合、手動で通信経路を元に戻します。	○	—	○	—
設定変更	閾値等の変更	検知の閾値を変更します。	○	—	○	—
	通知の設定/IP アドレス追加変更*	DDoS 検知防御対象 IP アドレスの追加、変更をいたします。	○	○	○	○

*: 防御対象インフラ側で IP アドレス追加変更がある場合、本サービス側での設定変更（有償）が必要となります。お申し込みが無い場合、本サービスの検知・防御対象 IP アドレス外となります。

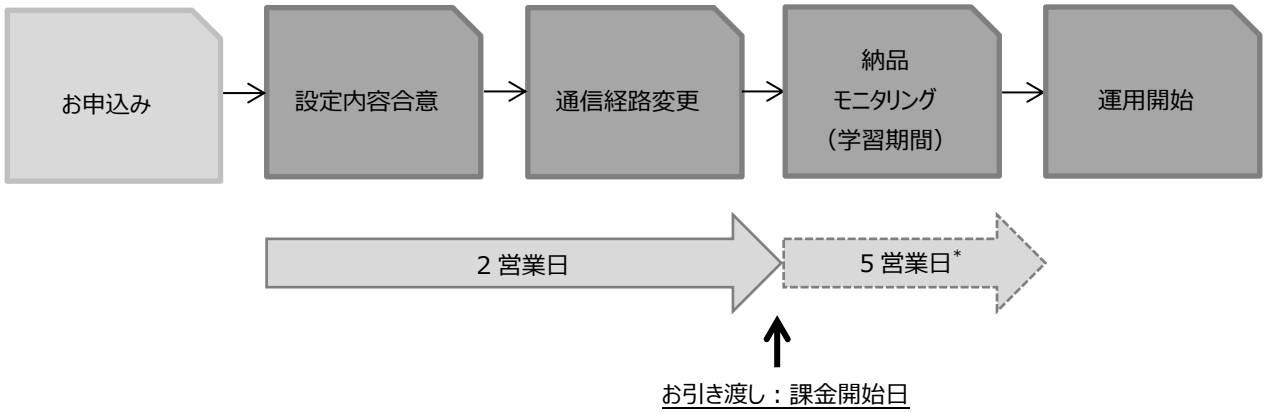
4.2. 導入フロー

ガード
[スタンダード・カスタム]
非常時タイプ



お引き渡し：課金開始日

ガード
[スタンダード・カスタム]
常時タイプ



お引き渡し：課金開始日

*：ガード[カスタム]の場合、モニタリング期間の変更及び追加機能設定の変更が可能となります。納期については事前に相談させて頂きます。

4.3. カスタマーサポート

サポートの受付・対応時間は以下のとおりです。

項目	媒体	受付時間	対応時間
サービスお問い合わせ	ポータルサイト	24 時間 365 日	平日 9:00～17:00
障害連絡受付 および その対応	電話	24 時間 365 日	24 時間 365 日
	メール	24 時間 365 日	24 時間 365 日
設定変更	ポータルサイト	24 時間 365 日	平日 9:00～17:00

*: お問い合わせや障害連絡受付の応答時間および解決時間は、当該事象の Severity（深刻度）等に応じて異なります。
また、当社は当該事象の解決のために商業的に妥当と思われる努力を行いますが、あらかじめ特定の時間内に完了することは保証しません。

5. 契約条件

5.1. サービスご利用条件

本サービスは、以下の契約書類に定めるご利用条件に従いお客様に提供されます。

契約名	契約書類
本サービス 利用契約	「クラウドサービスに関する契約約款」及び当社が定める各種規程にご同意いただくこと。 当社 IDC フロンティアのデータセンターサービス又はクラウドサービスをご契約であること。

5.2. 契約期間・最低利用期間

本サービスの契約期間および最低利用期間は以下のとおりです。

項目	詳細
契約期間 および 最低利用期間	• 本サービス利用契約の契約期間は、課金開始日から 1 か月間とします。ただし、本サービス利用契約は、当社又はお客様が期間満了日の 10 営業日前までに、相手方に対し、当社所定の書面による更新しない旨の意思表示をしない限り、さらに 1 か月間自動的に更新されるものとし、以後も同様とします。 • 本サービスの最低利用期間は 1 か月となり、以降 1 か月毎の自動更新となります。ただし、本サービス利用契約等において両者の合意による取り決めがある場合はこの限りではありません。

5.3. 解約

サービス利用契約を解約する場合は、解約希望日の 10 日前までに当社宛てに当社所定の書面で通知することにより、解約することができます。

5.4. 支払方法

本サービスのサービス料金は当社所定の方法にてお支払いください。本サービスの開始月及び終了月の月額利用料金はご利用日数に応じた日割り料金となります。料金の計算方法は以下の通りとなります。

区分	料金計算方法
利用を開始した月の料金	当社が本サービスを利用できる状態にした日から起算し、その月の末日までの利用日数に、月額の 30 分の 1 を乗じて得た額
利用を終了した日の料金	サービスの利用を終了する月の初日から現実にサービスを終了した日までの利用日数に、月額の 30 分の 1 を乗じて得た額

5.5. SLA（Service Level Agreement: 品質保証制度）

下記に定める品質を保証し、これに満たない場合にはサービス料金の減額を行います。減額する額は、別途協議の上決定されます。

5.5.1. ネットワーク接続の可用性に関する品質保証

お客様システムを収容する装置から、当社 DDoS 対策システム装置を経由して、当社データセンターバックボーンに接続可能な時間を、当サービスにおける網稼働時間とし、月間における稼働時間の割合（網稼働率）が 99.95%以上であることを保証します。

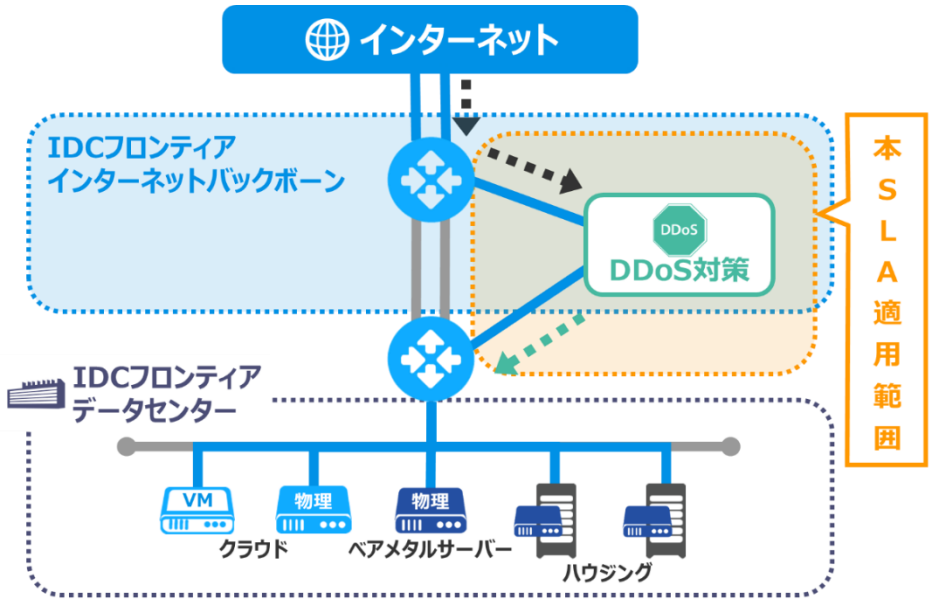
当社が規定する測定の結果、その保証値に満たない場合には、下記の定めに従い本サービス利用契約のサービス料金の月額費用を減額します。

基準値	減額の上限
99.95%未満	該当する本サービス利用契約総額の月額費用（税抜）の 10%

5.5.2. SLA 適用範囲

本サービスの SLA 適用範囲は以下となります。

サービス区分	SLA 適用範囲
クラウドサービス	当社 DDoS システムに接続する上位装置から下位装置まで
データセンターサービス	当社 DDoS システムに接続する上位装置から下位装置まで



5.5.3. 品質保証の範囲

本項で定める SLA が本サービスの品質保証の全てであり、その他の事項について、当社は、品質保証いたしません。また、本サービスは、お客様の特定の目的を達成することを保証するものではありません。

5.5.4. 減額の制限

- 品質保証の基準値は暦月の初日から末日までの期間において測定します。
- 減額申請は品質保証に違反する事項ごとに毎月 1 回限りの申請が可能です。
- 減額となる月額費用は、減額対象となる月のお客様が支払うべき月額費用額となります。
- 品質保証に基づくサービス料金の減額は、次項に定める Severity 1 のサービス提供状態のみとなります。

Severity の設定

当社は本サービスの提供の状態について、次に定める基準に従い、Severity を設定します。

Severity	定義
Severity1	全面的にインターネット接続が提供不可となった場合
Severity2	部分的にインターネット接続が提供不可となった場合
Severity3	上記以外

5.5.5. 免責事項

約款に定める事項のほか、品質保証の基準に該当する事実が以下事由により生じた場合には、品質保証の対象とはなりません。

（1） サービスの導入に関連して発生した場合
（2） 稼働時間の算定がお客様の計測のみにより認められる場合
（3） メンテナンス（緊急メンテナンスを含む）の場合
（4） 本サービス用設備及び当社のデータセンターバックボーン以外の故障による場合
（5） 大量通信等、外部からの攻撃、妨害等による場合
（6） お客様の行為、帰責性に起因・関連する場合
（7） 当社に帰責性のない事項に起因・関連する場合
（8） その他、不可抗力による場合

5.5.6. 除外事項

以下の各号のいずれの事由の場合も、本規定の品質保証及び減額の対象となりません。

（1） 減額の対象となる本サービス利用契約が無償利用期間又はトライアルサービス利用時の場合
（2） 稼働時間に影響を及ぼさないシステム（管理系・監視系サーバー等）の故障又は障害
（3） 通信への影響を及ぼさない本サービスの故障又は障害（冗長構成の複数の物理インターフェースのうち片系のインターフェースのみの障害等）

5.5.7. 故障又は障害の覚知

当社は、お客様のご連絡又は当社独自の調査により故障又は障害を覚知した場合は、トラブルチケットを発行し、お客様に対して当該チケット番号を連絡します。お客様の当社へのご連絡方法は、当社所定の手続きによります。

5.5.8. 減額申請

- お客様は減額申請を希望される場合には、該当するトラブルチケット番号に基づいて当社所定の申請書を当社に提出いただく必要があります。当社は申請内容を確認し、これを受理した場合には原則として減額対象となった月の翌月分のお客様に対して請求する月額費用から減額を実施いたします。ただし、障害発生の時期や契約状況によっては翌月以降に実施される場合があります。
- 減額申請の提出期限はその事由が生した日から 14 日以内に行っていただく必要があります。お客様から当社所定の申請書の提出がない限り、減額を行うことはありません。

5.6. ご利用上の制限および注意事項

- 同一アカウントであっても、東日本と西日本で本サービスを利用する場合は別契約になります。
- 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無い点予めご承知おきください。
- DDoS 攻撃等外部からの攻撃が当社の定める閾値（非公開）を著しく超過し、当社の本サービス用設備等若しくは DDoS 検知防御システムに障害・支障が生じた場合、又はお客様若しくは他のお客様の IDCF クラウドその他当社が提供するサービスの利用に支障がでた場合、DDoS 防御機能を停止するか、お客様への事前通知の上、通信の制限又は遮断を行う場合があります。ただし、現実的な被害又は急迫の危難がお客様又は他のお客様に発生し、緊急を要する場合、事前通知無しに通信の制限又は遮断を行う場合があります。
- 使用インフラ側で IP アドレスの新規追加又は変更がある場合、本サービス側での設定変更（有償）が必要となります。お申し込みが無い場合、本サービスの検知・防御対象 IP アドレス外となります。

5.7. 免責事項

「クラウドサービスに関する契約約款」およびサービス申込み時に提示されるもののほか、本サービスに関して、以下の免責事項があります。

- 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、確実性、完全性等に関し、いかなる保証責任も負いません。
- 当社は、本サービスの利用によって生じたお客様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。

5.8. その他

- 本サービス仕様書の記載事項および本サービス仕様書に記載がない事項については、サービス約款およびサービス申込み時に提示される各条項および各規定が優先的に適用されます。