J商ひかりVPN
サービス仕様書

ジェイアール西日本商事株式会社

まえがき

本資料はジェイアール西日本商事株式会社が提供する J商ひかりVPN サービスのサービス仕様に関する情報を提供するものです。
今後、本資料は予告なく変更される可能性があります。

1 J商ひかりVPNサービスについて

本サービスは、ジェイアール西日本商事株式会社（以下、「当社」）が提供するVPN サービスです。
NTTPC社 が構築した共用ネットワーク上にお客さま毎のプライベートネットワークを構築します。

2 J商ひかりVPN Cloud WAN サービス

提供事業者がWEB 掲載しているサポートサイト（https://support.onewan.cloud/）」内の技術マニュアル（技術仕様書）のうち、以下をご確認ください。

サービス構成（セキュアパッケージタイプ）

エッジ装置およびクラウドコネクタのサポートバージョンについて

提供機能（セキュアパッケージタイプ） 提供機能一覧

（適用範囲はセキュアパッケージタイプに限定し、オーバーレイタイプは適用いたしません。）

3 J商ひかりVPN 付加機能

3－1 ビジネスインターネット接続

① FW タイプ
別冊の仕様書をご確認ください。

② UTM タイプ
別冊の仕様書をご確認ください。

3－2 モバイルスタンダード

別冊のSD-WANモバイル_スタンダードタイプ_仕様書をご確認ください。

ビジネスインターネット接続サービス

FW タイプ

サービス仕様書

まえがき

本資料は、当社が提供する J商ひかりVPNビジネスインターネット接続サービスに関するサービス仕様を記載したものです。今後、本資料は予告なく変更される可能性があります。

1. サービス内容

J商ひかりVPNサービスにおいてインターネット接続機能を提供するサービスです。本サービスを利用するにあたり、J商ひかりVPNサービスを別途ご契約いただく必要がございます。

2. サービス品目

以下サービス品目の提供を行います。

品目	接続帯域
FW タイプ	ベストエフォート型：1G 帯域確保型：1M～10M(1M 刻み)

※ベストエフォート型：100M については新規申し込み終了

2.1. FW タイプ 提供機能について

機能名	内容
ファイアウォール機能	共通設定
標準アプリケーション制御	共通設定
DDoS 対策機能	共通設定

3. 機能説明

3.1. ファイアウォール機能

本機能では、FW 機器に流れるトラフィックをルールに従って制御を行います。

■基本ルール

ルール設定（通過/遮断）

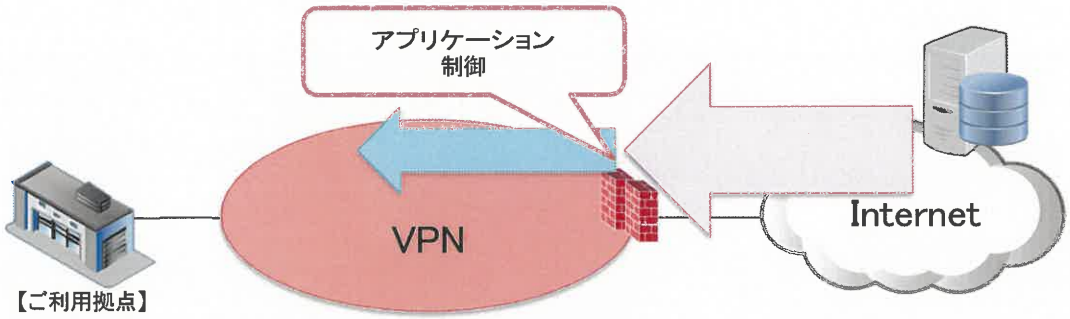
共通ルールとして、VPN 内部ネットワークから外部ネットワークに対しては全通過、外部ネットワークから VPN 内部ネットワークに対して全遮断の設定が含まれます。個別設定はできません。

提供仕様	値
同時セッション数	複数ユーザーにて共用
TCP セッションタイムアウト	600 秒
UTP セッションタイムアウト	600 秒

※本機能は共通設定となります。個別のFW設定を実施したい場合は、UTMタイプでのご利用をお願い致します。
※FTP の転送モードはPASV モードとなります。Active モードではご利用頂けません。

3.2. 標準アプリケーション制御機能

ベストエフォート型では、以下アプリケーションについて輻輳が発生しないように、トラフィックの制御を行う場合がございます。

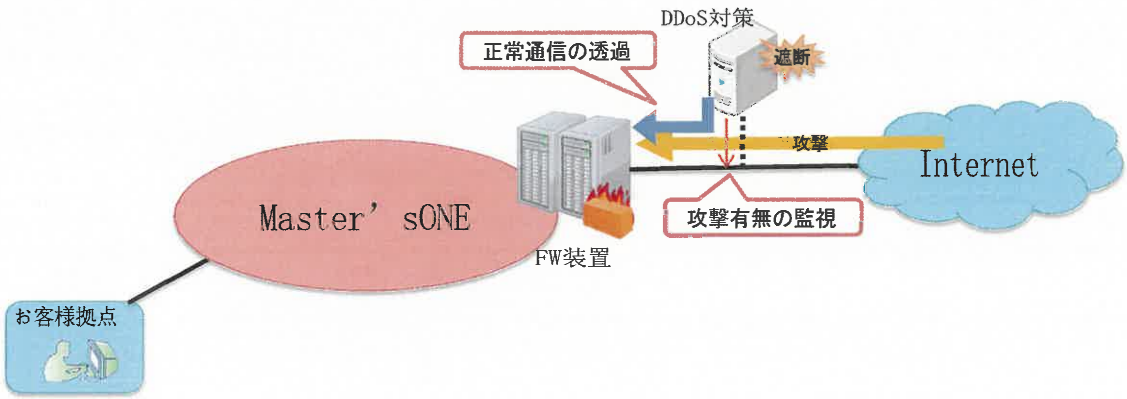


＜対象＞

- MS.Windows.Update
- Apple.Software.Update
- Chrome.Update
- Firefox.Update

3.3. DDoS 対策機能

払い出したグローバル IP に対して、DDoS 攻撃が発生した場合、自動で検知し攻撃パケットのみをドロップすることで、正常な通信トラフィックを透過致します。



※DDoS 装置が故障した場合、復旧に 6 時間程度かかることがございます。
※攻撃内容の分析・報告等の通知は致しません。

4. IPアドレス

4.1. お客様ネットワークアドレス

インターネットに接続することが可能なお客様ネットワークアドレスは RFC1918 に示されたプライベートアドレスもしくは、お客様に正式に割り当てられているグローバルアドレスとなります。

4.2. インターネット接続アドレス

インターネット接続用に /32 のグローバルアドレスを払い出し、使用いたします。このグローバルアドレスはTGにて申請代行いたします。またお客様ですでに所有されているアドレスを利用することはできません。また、IPv6 インターネットの利用をすることはできません。

4.3. DNS アドレス

お客様がインターネットに接続する際に参照可能な DNS アドレスは以下となります。
・プライマリ:203. 138. 71. 154
・セカンダリ:210. 150. 255. 66

※帯域、品目変更を実施する場合は、グローバル IP が変更となります。

5. 保守運用

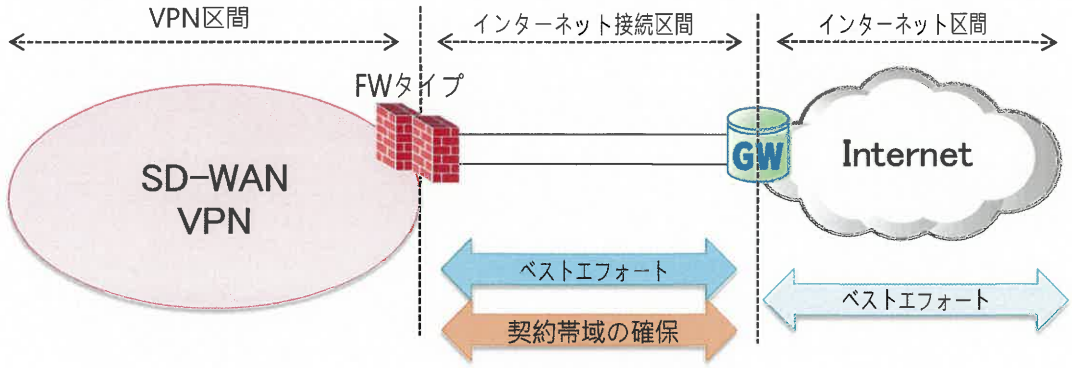
5.1. 故障発生連絡

当社で故障検出した場合、通信ができないお客様に対して申し込み時に申請された連絡先へ弊社指定の方法で連絡をします。

5.2. 当社からの借用通知について

あらかじめ計画された通信断を伴う工事については、1ヶ月前にお客様連絡します。ただし、緊急を要する場合を除きます。

6. 品質



6.1. ベストエフォート型

他のお客様と設備を共有する最大 1Gbps（または最大 100Mbps）のベストエフォートサービスです。他のお客様のトラフィック利用状況によりお客様の通信速度に影響を受ける可能性がございます。NTT 通信設備での輻輳･故障等が発生する可能性がある場合、対象のお客様トラフィックを制御させて頂く場合がございます。また、標準アプリケーション制御機能により Windows アップデート等のトラフィックは制御されます。

6.2. 帯域確保型

インターネット接続区間をお客様契約帯域分だけ確保するサービスです。インターネット接続区間については他のお客様のトラフィック利用状況によるお客様の通信速度に影響は受けません。ただし、VPN 内、インターネットについてはベストエフォートサービスとなり、他のお客様のトラフィック利用状況により、お客様の通信速度に影響を受ける可能性がございます。また標準アプリケーション制御機能は実施されません。

6.3. 設備構成

NTTPC 通信設備とインターネットとの接続点は二重化しており、接続点で故障が発生した場合でも、自動的に通信の復旧が行われます。ただし、故障個所により最大 30 分程度要する場合がございます。また、お客様利用状況によっては、品質維持のためメンテナンスウィンドを設ける場合がございます。

ビジネスインターネット接続サービス

UTM タイプ

サービス仕様書

まえがき

本資料は、当社が提供する J商ひかりVPNビジネスインターネット接続サービス UTM タイプ(以下、本サービス)のサービス仕様書です。今後、本資料は予告なく変更される可能性があります。

1. サービス内容

本サービスは J商ひかりVPNサービスにおいてインターネット接続機能を提供するサービスです。
本サービスを利用するにあたり、J商ひかりVPNサービスを別途ご契約いただく必要がございます。

2. サービス品目と提供機能

2.1. サービス品目

以下サービス品目を提供します。

品目	プラン
UTM タイプ	ベストエフォート型：1G

オプションメニューについては7. オプションメニュー参照

2.2. 提供機能一覧

機能名	内容
ファイアウォール機能	IP フィルタ／ポートフィルタ
Web セキュリティ機能	アンチウイルス／ホワイトリスト／ブラックリスト ／カテゴリフィルタ／スタティック URL フィルタ
メールセキュリティ機能	アンチウイルス/アンチスパム（SMTP／POP3／IMAP）
その他機能	IPS 機能 DDoS 対策機能
カスタマコントロール機能	ログ保管／設定変更(Web セキュリティ機能)
月次レポート	統計情報レポート

2.3. サービススペック

プラン	ベストエフォート型：1G
グローバル IP 追加	IP1 プラン
ファイアウォール	最大 200 項目
ホワイトリスト	最大 300 項目(※1)
ブラックリスト	最大 300 項目(※1)
アドレス	最大 1300 項目
アドレスグループ	最大 500 項目
URL カテゴリフィルタ	○
スタティック URL フィルタ	最大 5000 項目
同時接続セッション数	最大 100,000 セッション ベストエフォート(※2)
アンチウイルス	○
ソース NAT	○
ディスティネーション NAT	○
IPS	○
DDoS 対策	○
リアルタイムレポート	○
カスタマコントロール	○
ログ保管	100GB

※1 宛先リスト／送信元リストごとの最大値となります。

※2 同時接続セッション数はあくまでも最大値となり、設定内容やパケットサイズまたは他のお客様のご利用状況によっては、利用可能なセッション数が低下する場合がございます。

※インターネット接続用のグローバル IP アドレスは初期構築時に 1IP 払い出されます。

＜セッション保持時間について＞

提供仕様	値
TCP セッションタイムアウト	3600 秒
UDP セッションタイムアウト	180 秒

2.4. サービス性能の利用目安

UTM 設備の CPU、メモリ等のリソースは共用となります。リソースは確保しておりませんので他のお客様の利用状況により影響を受ける可能性があります。

お客様の利用状況に応じて、サービス設備全体の増強も並行して実施しますが、共用リソースである CPU 使用率を対象に、ご利用のメニュー毎の目安値を設定させていただきます。この目安値を超えた利用をされているお客様には、サービス品目の変更をお願いする場合があります。

※CPU 使用率とは、共有リソースのうち、お客様が利用しているリソース分の使用状況になります。

※CPU 使用率はカスタマコントロールにてご確認いただけます。

※確認方法はカスタマコントロールマニュアルをご参照ください。

＜CPU 利用目安値＞

プラン	帯域	CPU 利用目安
ベストエフォート	100Mbps	1%
	1Gbps	1%
帯域確保	10～50Mbps	1%
	60～100Mbps	2%
	150～300Mbps	5%
	350～600Mbps	10%
	700～900Mbps	15%
	1Gbps	20%
	1.5Gbps	25%
	2Gbps	30%
	3Gbps	40%

3. 提供機能

3.1. ファイアウォール機能

本機能では、UTM 装置に流れるトラフィックを IP アドレス／ポート番号を元に制御を行います。

3.1.1. 初期設定

以下のファイアウォールポリシーを設定して提供します。

通信の方向	ポリシー名	用途
LAN（お客様ネットワーク）→WAN（インターネット）	NTTPC モニタルール	NTTPC 保守監視用

LAN(お客様ネットワーク)→WAN(インターネット)	送信元ブラックルール	送信元ブラックリスト
LAN(お客様ネットワーク)→WAN(インターネット)	宛先ブラックルール	宛先ブラックリスト
LAN(お客様ネットワーク)→WAN(インターネット)	送信元ホワイトルール	送信元ホワイトリスト
LAN(お客様ネットワーク)→WAN(インターネット)	宛先ホワイトルール	宛先ホワイトリスト
LAN(お客様ネットワーク)→WAN(インターネット)	ALL_ICMP	Ping/Traceroute を許可
LAN(お客様ネットワーク)→WAN(インターネット)	LAN→WAN	全ての通信を許可
LAN(お客様ネットワーク)→WAN(インターネット) WAN(インターネット)→LAN(お客様ネットワーク)	暗黙の拒否ルール	全ての通信を遮断

3.1.2. 個別設定

カスタマコントロールにてファイアウォールルールを追加・編集することで個別設定が可能です。個別設定は最大 200 ポリシーまで設定可能です。

3.1.3. ホワイトリスト

指定した対象ネットワークのスキャンを行なわず、セキュリティを無効化することができます。

指定可能な項目は、IP アドレス、サブネット、FQDN、アドレスグループです。

HTTPS 通信が必要な Web サイトでも識別できます。

3.1.4. ホワイトリスト初期設定以

下の設定で提供します。

種類	初期設定
送信元ホワイトリスト	なし
宛先ホワイトリスト	なし

3.1.5. ブラックリスト

指定した対象ネットワークにフィルタをかけ、通信を遮断することができます。

指定可能な項目は、IP アドレス、サブネット、FQDN、アドレスグループです。

HTTPS 通信が必要な Web サイトでも識別できます。

3.1.6. ブラックリスト初期設定

以下の設定で提供します。

種類	初期設定
送信元ブラックリスト	なし
宛先ブラックリスト	なし

※IP アドレスもしくは FQDN を登録できます。URL は登録できません。
※保守用の設定として、Ping/Trace route の許可が初期設定に含まれます。削除はできません。
※ホワイトリストは送信元リスト／宛先リストでそれぞれ最大　300　行までご利用頂けます。
※ブラックリストは送信元リスト／宛先リストでそれぞれ最大　300　行までご利用頂けます。
※ポリシー設定変更は通常カスタマコントロール機能をご利用頂き、お客様自身で行って頂きます。
　設定方法については「カスタマコントロール利用マニュアル」をご確認ください。
※送信元ブラックリスト→宛先ブラックリスト→送信元ホワイトリスト→宛先ホワイトリストの順に適用されます。
※ブラックリスト・ホワイトリストでは 2 バイト文字は利用することができません。
　全て　1　バイト文字=半角文字のみとなります。

3.2. NAT 機能

本機能では、UTM を経由して通信する際に IP アドレスとポート番号のいずれか、もしくは両方を変換します。

※通常のインターネット接続用のソースNAT 機能については初期設定として登録されます。

3.3. アンチウイルス機能

本機能では、HTTP、メール（SMTP、POP3、IMAP）、FTP においてウイルスチェックを行い、検知・駆除します。

3.3.1. サポート対象となるプロトコル

プロトコル	サポート対象	初期設定
HTTP	対象	有効
SMTP	対象	無効
POP3	対象	無効
IMAP	対象	無効
MAPI	対象外	
FTP	対象	無効
CIFS	対象外	
SSH	対象外	

※スキャン対象は 80 番ポート(HTTP)、25 番、587 番ポート(SMTP)、110 番ポート(POP3)、143 番ポート(IMAP)、20 番、21 番ポート(FTP)のみとなります。HTTPS 通信は対象外となります。
※スキャンを行うコンテンツサイズは 30M までとなります。それを超えるコンテンツについては、スキャンを行いません。
※スキャンを行うコンテンツサイズは固定値であり、変更することはできません
※ウイルスを検知したメールはメールごと破棄します。

3.4. アプリケーションコントロール機能

本機能では、UTM 装置を流れるトラフィックをアプリケーション指定のルールに従って制御を行います。

3.4.1. 初期設定

アプリケーションコントロール機能:有効
ブロック対象アプリケーションカテゴリ:なし

3.4.2. 個別ルール

カスタマコントロールにてアプリケーションコントロールルールを編集することで個別設定が可能です。

クラウドアプリケーション(雲マークのクラウドシグネチャアプリケーション)はアプリケーションコントロールの対象外となります。

3.5. Web フィルタ機能

本機能では、UTM 装置で分類されている 91 カテゴリで制御を行います。

3.5.1. カテゴリベースのフィルタ

Web サイトは 93 カテゴリに分類されており、UTM 装置にてカテゴリを識別し通信の制御を行います。
本機能は HTTPS 通信が必要な Web サイトでも識別できます。

3.5.2. 初期設定

カテゴリごとに以下の設定で提供します。

項目	カテゴリ	設定アクション
違法性の高いサイト	薬物乱用	ブロック
	ハッキング	ブロック
	違法または非倫理的	ブロック
	差別	ブロック
	明示的な暴力	ブロック
	過激派グループ	モニタ
	プロキシ回避	モニタ
	盗作	ブロック
	児童虐待	ブロック
	テロリズム	モニタ
	クリプトマイニング	モニタ
	望ましくない可能性のあるプログラム	モニタ
アダルト/成人コンテンツ	民間信仰	モニタ
	人工中絶	モニタ
	その他のアダルトマテリアル	ブロック
	政策支援団体	モニタ
	ギャンブル	ブロック
	ヌードとワイセツ	ブロック
	ポルノ	ブロック
	出会い系	ブロック
	兵器(販売)	モニタ
	マリファナ	ブロック
	性教育	モニタ
	アルコール	モニタ
	タバコ	モニタ
	下着と水着	モニタ
	スポーツハンティングと戦争ゲーム	モニタ
帯域を消費しやすいサイト	フリーウェアとソフトウェアのダウンロード	モニタ
	ファイル共有とストレージ	モニタ
	ストリーミングメディアとダウンロード	モニタ
	ピアツーピアファイル共有	モニタ
	インターネットラジオとテレビ	モニタ

	インターネット電話	モニタ
セキュリティリスクの高いサイト	悪意のある web サイト	ブロック
	フィッシング詐欺	ブロック
	スパムURL	ブロック
	ダイナミック DNS	モニタ
	新たに観察されたドメイン	モニタ
	新たに登録されたドメイン	モニタ
一般的な関心事–個人	広告	モニタ
	証券会社と仲買業	モニタ
	ゲーム	モニタ
	Web ベースの E メール	モニタ
	エンターテインメント	モニタ
	芸術と文化	モニタ
	教育	モニタ
	健康とウェルネス	モニタ
	求人情報	モニタ
	医学	モニタ
	ニュースとメディア	モニタ
	ソーシャルネットワーキング	モニタ
	政治団体	モニタ
	リファレンス	モニタ
	グローバルな宗教	モニタ
	ショッピング	モニタ
	社会とライフスタイル	モニタ
	スポーツ	モニタ
	旅行	モニタ
	パーソナルビークル	モニタ
	ダイナミックコンテンツ	モニタ
	無意味なコンテンツ	モニタ
	民間伝承	モニタ
	ウェブチャット	モニタ
	インスタントメッセージ	モニタ
	ニュースグループと掲示板	モニタ
	デジタルポストカード	モニタ
	児童教育	モニタ

	不動産	モニタ
	レストランとダイニング	モニタ
	個人のWeb サイトとブログ	モニタ
	コンテンツサーバ	モニタ
	ドメインパーキング	モニタ
	個人のプライバシー	モニタ
	オークション	モニタ
一般的な関心事-ビジネス	金融と銀行	モニタ
	検索エンジンとポータル	モニタ
	一般組織	モニタ
	ビジネス	モニタ
	情報とコンピュータセキュリティ	モニタ
	政府機関および法的機関	モニタ
	情報技術(IT)	モニタ
	軍事(軍隊)	モニタ
	Web ホスティング	モニタ
	安全な Web サイト	モニタ
	Web ベースのアプリケーション	モニタ
	慈善団体	モニタ
	リモートアクセス	モニタ
	ウェブ分析	モニタ
	オンライン会議	モニタ
	短縮 URL	モニタ
	人工知能技術	モニタ
	暗号通貨	モニタ
Unrated	Unrated	モニタ

3.5.3. URL フィルタ

指定した対象 URL の通信を許可/拒否することができます。

指定可能な項目は、ブロック、許可、除外です。

3.6. アンチスパム機能

本機能は、メール送受信時にメールチェックを行い、スパムメールの制御を行う機能です。

3.6.1. 対象プロトコル

SMTP、POP3、IMAP

3.6.2. スパム判定時のアクション

破棄（SMTP のみ）、タグ、転送

3.6.3. タグ付与のアクション

スパムメールのサブジェクトにタグをつけてメール転送を行います。

3.6.4. 初期設定

プロトコルごとに以下の設定で提供します。

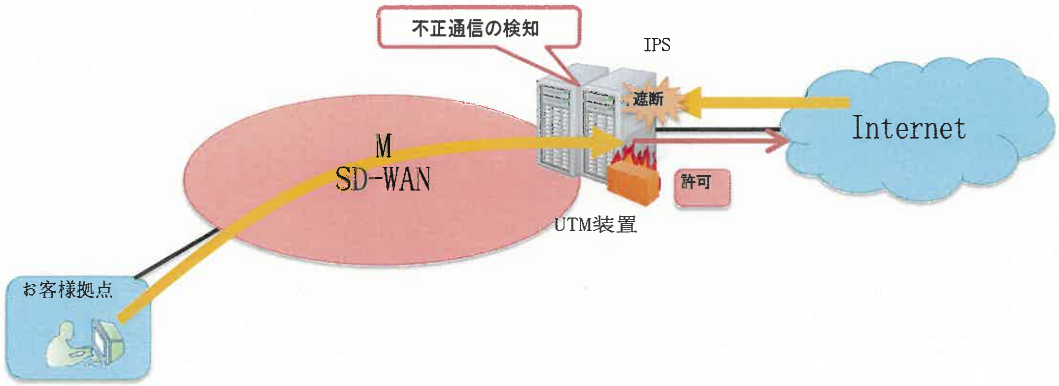
プロトコル	スパムアクション	タグ形式
SMTP	タグ	サブジェクトに[Spam]を付与
POP3	タグ	サブジェクトに[Spam]を付与
IMAP	タグ	サブジェクトに[Spam]を付与

3.7. IPS（侵入防止）機能

本機能は、お客様 VPN からの通信またはインターネット上からの通信に対して、指定のポリシーに則り、パケット監視を行うことで宛先ネットワークに到達する前に不正な通信を自動的に検知・遮断します。

3.7.1. 初期設定

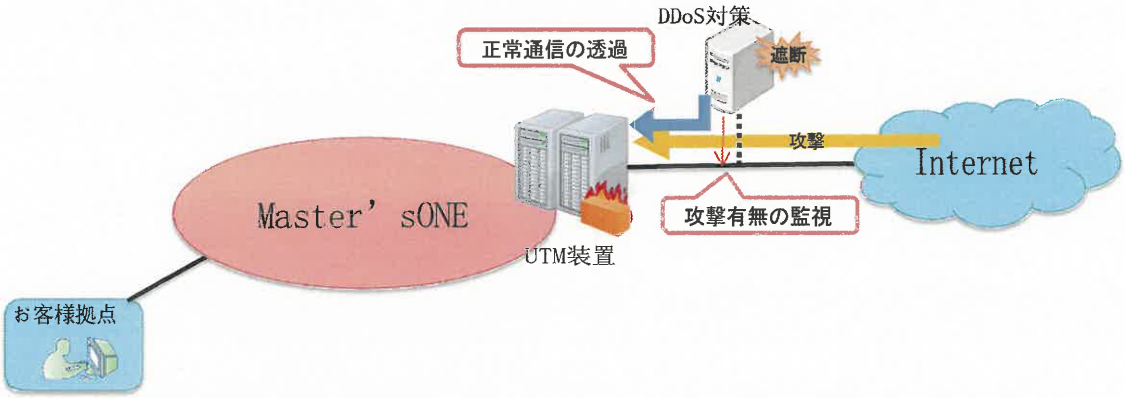
IPS：無効化



※有効化／無効化以外の設定変更はできません。
※防御シグネチャについて、更新がある都度アップデートされます。原則通信断は発生致しません。

3.8. DDoS 対策機能

NTTPC 払い出し、または代行取得したグローバル IP に対して、DDoS 攻撃が発生した場合、自動で検知し攻撃パケットのみをドロップすることで、正常な通信トラフィックを透過致します。



※DDoS 装置が故障した場合、復旧に 6 時間程度かかることがございます。
※攻撃内容の分析・報告等の通知は致しません。

4. カスタマコントロール機能

本機能では、お客様自身で UTM 装置の設定を変更可能なカスタマコントロールサイトを提供します。

4.1. カスタマコントロール画面

機能一覧	
ネットワーク セキュリティ	ファイアウォール設定(各種セキュリティ設定の有効/無効)
	SNAT/DNAT 設定
Web セキュリティ	許可ネットワーク (Web セキュリティを適用するホスト/ネットワーク)の追加/削除
	アンチウイルスの詳細設定
	アンチスパムの詳細設定
	アプリケーションコントロールの詳細設定
	Web フィルタの詳細設定
	ホワイトリストの詳細設定(追加/変更/削除)
	ブラックリストの詳細設定(追加/変更/削除)
ログ	ログのダウンロード

※接続は当社の提供する　VPN　上からのみとなり、インターネットからの接続はできません。
※カスタマコントロールログイン ID は VPN ごとに 1ID 登録が可能です。
※カスタマコントロール機能はログイン状態かつ未操作で放置する場合は 60 分でログアウト致します。再度ご利用する際は、改めてログインして頂く必要がございます。
※設定方法等については、別紙「カスタマコントロール利用マニュアル」をご確認ください。
※「カスタマコントロール利用マニュアル」でご案内の無い機能はサポート対象外機能となり、利用することができません。サポート対象外機能を設定した場合、通信不通や通信不安定などの原因になる可能性があり、サポート対象外機能を利用したことによる動作保証は致しません。また、サポート対象外機能に関する問合せには回答できません。
＜推奨ブラウザ＞
Mozilla Firefox/Google Chrome/Microsoft Edge
上記ブラウザでリリースされている最新バージョンの使用を推奨
但し、ブラウザ側の仕様変更に伴い正常に画面の表示ができない場合がございます。

4.2. ログ保管

ログ保管容量はサービス品目およびプランごとに異なります。

保管容量または期間のいずれかを超えた情報については自動的に削除します。

4.2.1. ログ保管容量

サービス品目およびプランに応じたログ保管容量を提供します。

サービス品目	帯域	ログ保管容量
ベストエフォート	100Mbps	100GB
	1Gbps	
帯域確保	10Mbps	100GB
	20Mbps	
	30Mbps	
	40Mbps	
	50Mbps	
	60Mbps	
	70Mbps	
	80Mbps	
	90Mbps	
	100Mbps	150GB
	150Mbps	200GB
	200Mbps	300GB
	300Mbps	450GB
	400Mbps	600GB
	500Mbps	750GB
	600Mbps	900GB

	700Mbps	1.05TB
	800Mbps	1.2TB
	900Mbps	1.35TB
	1Gbps	1.5TB
	1.5Gbps	2TB
	2Gbps	3TB
	3Gbps	4.5TB

4.2.2. ログ保管期間

保管期間は 1 年間となります。

4.2.3. 保管するログレベル

information 以上

5. IPアドレス

5.1. お客様ネットワークアドレス

インターネットに接続することが可能なお客様ネットワークアドレスは RFC1918 に示されたプライベートアドレスもしくは、お客様に正式に割り当てられているグローバルアドレスとなります。また RFC6598 に示された 100.64.0.0/10 は NTTPC ネットワーク内で利用するため、お客様の VPN 内のアドレスとしてご利用頂くことができません。

5.2. インターネット接続アドレス

インターネット接続用に NTTPC にて/32 のグローバルアドレスを払い出し、使用します。このグローバルアドレスはNTTPC にて申請代行します。また、お客様ですでに所有されているアドレスを利用することはできません。また、IPv6 インターネットの利用をすることはできません。
※ご利用の帯域や品目変更を実施する場合は、グローバル IP が変更となる場合がございます。
※NAT 機能利用において複数グローバル IP が必要な場合は別途有料オプションが必要です。
NAT 機能の設定内容により、お客様よりご指定頂く「NTTPC 利用アドレス」を広く頂く場合がございます。

5.3. DNS アドレス

お客様がインターネットに接続する際に参照可能な DNS アドレスは以下となります。
・プライマリ：203. 138. 71. 154
・セカンダリ：210. 150. 255. 66

6. 保守運用

6.1. 故障発生連絡

当社で故障検出した場合、通信ができないお客様に対して申し込み時に申請された連絡先へ当社指定の方法で連絡をします。冗長化により 1 分以内に通信が迂回し、復旧する故障の場合は連絡しません。
ただし、”9.3. 設備構成”のとおり、”片系設備の故障が発生した場合は 2 分以内に通信が迂回し、復旧する設計”であるため、迂回による通信の復旧が 1 分以上かかる場合については連絡します。

6.2. 故障受付

お客様からの故障申告は以下で受け付けます。

【故障受付用連絡先】
・別途当社より連絡させて頂く連絡先

申告の際は以下の情報が必要となります。
・システム番号
・故障状況
※システム番号は開通案内記載の VPN 番号/ASG 番号/GSS 番号/nuas 番号/ngas 番号/nhas 番号/biu 番号となります。

6.3. 当社からの借用通知

あらかじめ計画された通信断を伴う工事については、1週間前までにお客様へ当社指定の方法で通知します。ただし、緊急を要する場合を除きます。また冗長化により 1 分以内に通信が迂回し、復旧する工事の場合はご連絡しません。

6.4. 変更工事に伴う借用

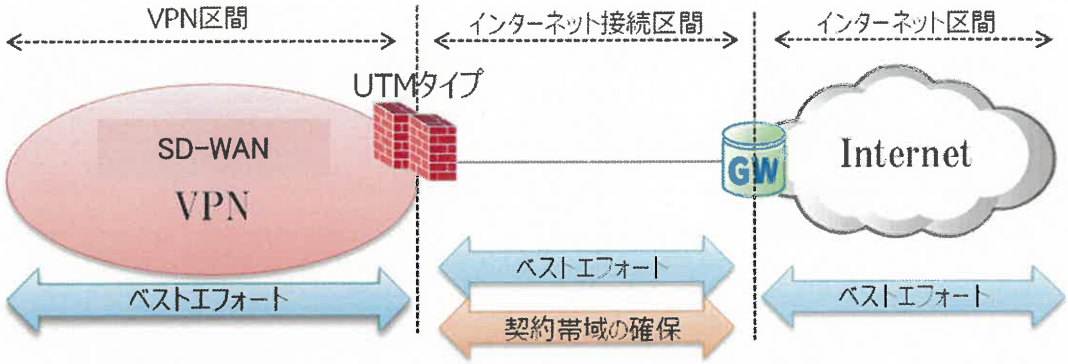
下記追加・変更を行う場合は、借用が発生します。
・インターネット接続サービスタイプ変更
FW タイプからUTM タイプ(逆を含む)の変更は、本サービスの廃止および新設での対応が必要となります。
※インターネット接続用グローバル IP アドレスの引き継ぎはできません。

・ネットワーク構成変更工事(NTTPC 利用アドレス変更/収容設備変更)

※設備変更を行う場合、ログ情報を引き継ぐことはできません。

・UTM OS の Ver.UP

7. 品質



7.1. ベストエフォート型

他のお客様と設備を共有する最大 1Gbpsのベストエフォートサービスです。他のお客様のトラフィック利用状況によりお客様の通信速度やセッション数に影響を受ける可能性がございます。当社通信設備での輻輳・故障等が発生する可能性がある場合、対象のお客様トラフィックを制御させて頂く場合がございます。

また、設備保護の観点から輻輳が発生しないように特定のアプリケーションのお客様トラフィックを制御させていただく場合がございます。

例)

・MS.Windows.Update

・Apple.Software.Update

7.2. 設備構成

UTM 設備、当社通信設備とVPN との接続点、当社通信設備とインターネットとの接続点はいずれも冗長化しており、片系設備の故障が発生した場合は2 分以内に通信が迂回し、復旧する設計になっております。ただし、ネットワークセキュリティ機能や Web セキュリティ機能の不具合などにより通信ができない場合には通信の迂回は行いません。

また、お客様利用状況によっては、品質維持のためメンテナンスウィンドウを設ける場合がございます。

8. 注意事項

・各セキュリティ機能を有効にした場合、通信速度が遅くなる可能性がございます。

・全てのウイルスや攻撃等を検知・防御するものではございません。

・攻撃の検知やトラフィックの急激な増加などによりログが非常に多くなった場合、ログが欠損する可能性がございます。

・UTM設備に割り当てたグローバル IP アドレスはインターネット上からの ICMP エコー要求に応答します。応答を拒否することはできません。

J商ひかりVPN
モバイルスタンダードタイプ
サービス仕様書

ジェイアール西日本商事株式会社

目次

13. エリアメール
14. 強制黒化

まえがき

本資料は、ジェイアール西日本商事株式会社（以下、当社）が提供する J商ひかりVPNモバイル スタンダードタイプ（以下、本サービス）に関するサービス仕様を記載したものです。

今後、本資料は予告なく変更される可能性があります。

1. サービス内容

IoT／M2M 通信のモノ向け利用から、リモートワークなどの人向け利用まで、お客さまの用途にあわせて適切なモバイルサービスをご利用いただけます。モバイル回線はLTE／5G(NSA)より選択できます。

●LTE

LTE 端末を使用する際にご選択ください。

ドコモ社 Xi® 圏内ではLTE 規格に準じ、また Xi® 圏外かつ FOMA® 圏内では 3G 規格に準じたデータ通信をご利用になれます。

●5G(NSA)

5G 端末を使用する際にご選択ください。

NSA とは「Non-Stand Alone」の略で、ドコモ社 5G 圏内では 5G 規格に準じ、また 5G 圏外かつXi® 圏内では 4G 規格に準じたデータ通信をご利用になれます。通信品質としては LTE と同等となります。

2. サービス詳細

「①サービスタイプ」+「②プラン」+「③オプション」

2.1. ①サービスタイプ

(1) VPN モバイル

接続先ネットワークをＪ商ひかりＶＰＮとする閉域型モバイルアクセスです。

2.2. ②プラン

(1) 3GB プラン

月間 3GB までご利用できるプランです。

上下常時制限なし。

月間 3GB 超えでその日から月末まで通信速度が制限されます。

(2) 5GB プラン

月間 5GB までご利用できるプランです。

上下常時制限なし。

月間 5GB 超えでその日から月末まで通信速度が制限されます。

LTE／5G(NSA)のみの提供です。

(3) 10GB プラン

月間 10GB までご利用できるプランです。

上下常時制限なし。

月間 10GB 超えでその日から月末まで通信速度が制限されます。

LTE／5G(NSA)のみの提供です。

(4) 20GB プラン

月間 20GB までご利用できるプランです。

上下常時制限なし。

月間 20GB 超えでその日から月末まで通信速度が制限されます。

LTE／5G(NSA)のみの提供です。

(5) 30GB プラン

月間 30GB までご利用できるプランです。

上下常時制限なし。

月間 30GB 超えでその日から月末まで通信速度が制限されます。

LTE／5G(NSA)のみの提供です。

⑹ 50GB プラン

月間 50GB までご利用できるプランです。

上下常時制限なし。

月間 50GB 超えでその日から月末まで通信速度が制限されます。

LTE／5G(NSA)のみの提供です。

2.3. ③ 端末

		LTE	5G(NSA)
SIMタイプ	SMS 非対応	標準／Micro／nano／チップ SIM（ノーマル）／チップ SIM（インダストリアル）	標準／Micro／nano

SIMはレンタルとなります。ご契約終了後はご返却ください。（配送料お客様負担）

※納品後のチップSIM 取扱い注意について

	チップSIM（ノーマル）	チップSIM（インダストリアル）
開封後のフロアライフ	1 週間（168 時間）	期限なし
フロアライフを維持するための条件	温度 30 度以下かつ湿度 60%以下	温度 30 度以下かつ湿度 85%以下

2.4. ④ オプション機能

カテゴリ	品目	選択肢	適用単位	内容
回線	クーポン	有/無	SIM	モバイル回線の通信量を追加することが出来ま す。
端末 IP	端末IP	標準提供	契約企業様 （システム番号）	VPN モバイルが提供対象となります。 端末 IP アドレスはお客様によるクラス指定の上で当社より払い出します。
通信制限	折り返し通信禁止	有／無	契約回線全体 （Suffix）	VPN モバイルのみ選択できます。 本オプションを利用のときは、SIM 同士の通信が出来なくなります。

3. サービス仕様

基本仕様は次のとおりです。

項目			SD-WAN モバイル
接続先ネットワーク			Master's ONE IP-VPN
アクセス回線種			LTE／5G(NSA) ＊5G（NSA）はモバイルスタンダードタイプかつ、カード型 SIM のみ
PDP タイプ			
	LTE／5G(NSA)		IP（PAP またはCHAP）
ユーザ認証	ユーザID		共通 ID 方式／ユニークID 方式 ＊SIM タイプがチップSIM の場合は共通 ID 方式のみ
	パスワード		固定パスワード
端末 IP アドレス	使用アドレス		当社指定プライベートIP
	付与方式		1 回線毎に/32 を固定的に付与
DNS アドレス			お客様指定のプライベートDNS をPDP 接続認証時に自動付与
通信制限	長時間通信断		－
		3GB プラン	制限なし
		5GB プラン	制限なし
		10GB プラン	制限なし
		20GB プラン	制限なし
		30GB プラン	制限なし
		50GB プラン	制限なし

通信制限	月間通信量上限	3GB プラン	3GB　超で月末まで速度制限
		5GB プラン	5GB　超で月末まで速度制限
		10GB プラン	10GB　超で月末まで速度制限
		20GB プラン	20GB　超で月末まで速度制限
		30GB プラン	30GB　超で月末まで速度制限
		50GB プラン	50GB　超で月末まで速度制限
	公平制御		網全体の混雑状態で通信帯域を回線毎に公平割り当て
	アプリ規制		Windows Update　は全体で一定値に制限
その他制限	同時PDP 認証数		最大 50 端末/秒
オプション	クーポン		○

4. 端末 IP アドレス

お客様モバイル端末用 IP アドレスには、当社より払い出したIP アドレスを使用します。

●標準サービス

サービスタイプが VPN モバイルの場合、お客様は、初期のお申し込み時点でクラスA 又はクラスB のどちらか一方の範囲をご指定ください。(お客様ネットワークにおいて未使用の IP アドレス・クラスをご指定ください。)

当社はご指定頂いたクラス内より任意のIP アドレス帯を払い出します。

どちらの範囲もご利用中の場合には、当社のシェアードアドレス帯から任意の IP アドレスを払い出しますの

<クラスAをご指定の場合>

リモート接続端末には 10.0.0.0～10.255.255.255 の範囲より割り当てられます。

<クラスBをご指定の場合>

リモート接続端末には 172.16.0.0～172.31.255.255 の範囲より割り当てられます。

<その他をご指定の場合>

リモート接続端末には 100.64.0.0~100.127.255.255 の範囲より割り当てられます。

5. 折り返し通信禁止

VPN モバイルのみ選択できます。本オプションを選択したときは、SIM 同士の通信が出来なくなります。

お客さまで複数のアドレス・クラスを Master'sONE モバイルスタンダードタイプ(旧称:モバイル M2M VPN タイプ) として利用している場合、異なるクラス間での折り返し通信は出来ますが、将来的に通信不可となる可能性がありますので折り返し通信禁止のオプションをご利用の上異なるアドレス・クラス間での通信を想定したネットワーク設計は控えていただけますようお願いいたします。

なお、お客さまが契約するMaster'sONE の他モバイルサービス (Master'sONE モバイルスタンダードタイプ認証オプション (旧称:セキュアモバイル定額通信) 等) との通信は仕様上可能です。

本オプションを利用した場合のMaster'sONE モバイルスタンダードタイプ (旧称:モバイル M2M VPN タイプ) サービス通信例

例:10.0.0.3 (クラスA アドレス帯) と 10.10.3.3. (クラスA アドレス帯) は、折り返し不可

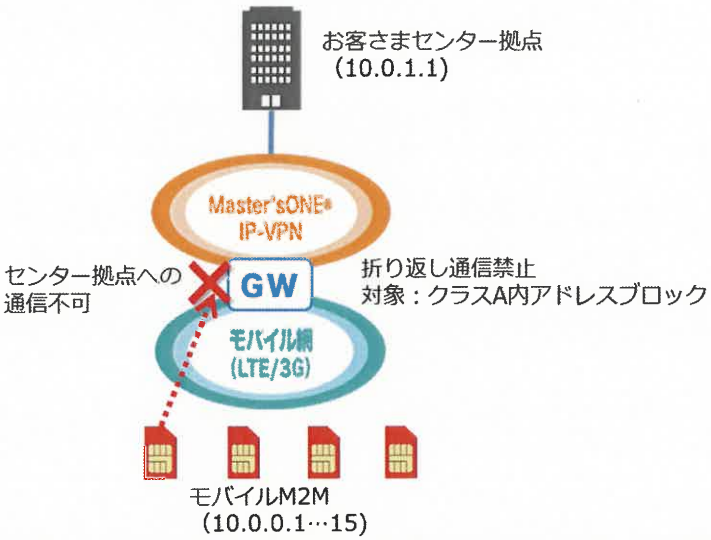
10.0.0.3 (クラスA アドレス帯) と 172.16.1.10 (クラスB アドレス帯) は、折り返し可

※但し、通信機器の仕様変更等により将来的に通信不可となる可能性があるためクラス間の折り返しを前提としたネットワーク設計は推奨しません。

本オプションは契約回線全体(企業識別子単位)に適用されます。

（注意）

Master'sONE モバイルスタンダードタイプ（旧称:モバイル M2M VPN タイプ）では、お客さまネットワークにおいて未使用のIP アドレス・クラスをご指定いただく仕様となっているため、本仕様に違反した場合は下記のケースのように正常に通信が出来なくなる恐れがあります。また、ご利用当初通信が出来ていた場合でもMaster'sONE モバイルスタンダードタイプ（旧称:モバイルM2M VPN タイプ）のIP アドレスは予告なく拡張・縮小されるため、将来的に通信が出来なくなる可能性があります。必ず、仕様を厳守の上ご利用ください。本仕様に違反して通信に影響が出た場合は、ご利用のIP アドレス・クラスを変更していただくこととなりますのでご注意ください。



6. 認証情報

6.1. ユーザID

PDP 接続認証に用いるユーザID は以下の構成をとります。

お客様には[ユーザ識別子]と[企業識別子]を指定して頂きます。

１つのユーザID を複数のお客様で共用することはできません。

【ユーザID の構成】

[ユーザ識別子]@ [企業識別子].[サービス識別子].[ドメイン]

- ユーザ識別子

3 文字以上 14 文字以内でお客様にご指定いただきます。

利用可能な文字は半角の英字（大文字・小文字の区別あり）、数字、「-(ハイフン),_(アンダースコア)」です。但し「ユーザ識別子」と「企業識別子」の合計文字数が 16 文字以内でなければなりません。

- 企業識別子

2 文字以上 13 文字以内でお客様にご指定いただきます。

但しご指定の企業識別子が他のお客様で既に利用中の場合は他の識別子に変更をお願いいたします。利用可能な文字は半角の英字（大文字・小文字の区別あり）、数字、「-(ハイフン)」です。なお、数字だけの企業識別子は指定できません。但し「ユーザ識別子」と「企業識別子」の合計文字数が 16 文字以内でなければなりません。

● サービス識別子

NTTPC が指定する識別子です。網内で接続制御のために使用します。

本サービスで使用するサービス識別子は以下のとおりです。

ネットワーク種別	ユーザID 方式	アクセス回線種別	サービス識別子
VPN モバイル	共通 ID 方式	3G	vc3（標準／Micro／nano）
		LTE／5G(NSA)	vct（標準／Micro／nano）
		LTE	cva（チップSIM（ノーマル／インダストリアル））
	ユニーク ID 方式	3G	vu3（標準／Micro／nano）
		LTE／5G(NSA)	vut（標準／Micro／nano）

● ドメイン

アクセス回線種	ご契約サービス	ドメイン
LTE／5G(NSA)	Master's ONE モバイルスタンダードタイプ	msone.jp

6.2. パスワード

お申し込み時に、お客様にてパスワードを指定の上で申請して頂きます。

パスワードの長さは半角 3 文字以上 15 文字以内です。

英字（大文字・小文字の区別あり）、数字、「-(ハイフン),_(アンダースコア)」のご利用が可能です。

6.3. 認証方式

アクセス回線種	APN 名	PDP タイプ	認証方式
LTE／5G(NSA)	lte-mobile.jp	IP	PAP またはCHAP

7. その他制限事項

7.1. レンタル品の故障交換

SIMが故障した際の交換は当社へお問い合わせください。

故障を判定、交換を承りましてから最大 2 営業日以内に交換品を発送します。

SIM のPIN ロック解除 当社の窓口へご連絡ください。※チップSIM は完全ロック解除不可（PIN ロック解除コードを 10 回間違えた場合の完全ロックは解除できない）となります。

7.2. 故障申告の受付

チップSIM の初期不良対応

以下の条件を全て満たす場合のみ、対象チップSIM の事務手数料・発行手数料、基本サービス月額料金を請求額から相殺（請求額が相殺額に満たない場合は返金）します。

【相殺（または返金）の条件】

・対象のチップSIM 納品日の 12 か月以内にお客さまから当社保守窓口へ初期不良の申告をしたもの

・対象のチップSIM で通信ログが存在しないこと

・対象のチップSIM で利用開始登録を実行後、1 か月以内に申告したもの

※上記の条件をすべて満たさない場合は相殺（または返金）の対象となりませんのでご注意ください。

7.3. メンテナンス通知（借用通知）について

通信に関する建設工事、保全工事等あらかじめ計画された工事については、1 ヶ月前にお客様連絡します。ただし、緊急を要する場合を除きます。

お客様連絡は、連絡時点で利用中の SIM をお持ちのお客様が対象となります。連絡以降に初めて SIM を利用中にされたお客様は災害・工事・故障情報に掲載されている情報をご確認ください。

また MNO にて計画された工事についてはこの限りではありません。

カスタマーコンソールに関する保全工事等あらかじめ計画された工事については 2 週間前に災害・工事・故障情報に掲載致します。ただし、緊急を要する場合を除きます。

8. その他制限事項

8.1. SIM と端末の組み合わせによる通信のご利用可否

SIM	モバイル端末	エリア	接続国	3G-APN	LTE-APN
5G プランSIM	3G 端末 (Single)	3G 在圏時	国内	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×
		3G 在圏時	海外	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×
	LTE 端末 (3G/LTE dual)	3G 在圏時	国内	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×
		3G 在圏時	海外	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×
	5G 端末 (LTE/5G dual)	3G 在圏時	国内	×	×
		LTE 在圏時		×	○
		5G 在圏時		×	○
		3G 在圏時	海外	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×
LTE プランSIM	3G 端末 (Single)	3G 在圏時	国内	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×
		3G 在圏時	海外	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×
		LTE 在圏時		×	○
		5G 在圏時		×	×

		3G 在圏時	海外	×	×
		LTE 在圏時		×	×
		5G 在圏時		×	×

※5G プランSIM は 3G 接続できません。

LTE 端末は 5G プランSIM の保証対象外です。

8.2. その他

- MNP には対応しておりません。
- 音声サービスには対応しておりません。
- 国際ローミングには対応しておりません。

9. 強制黒化

SIM タイプが「チップSIM（ノーマル）」または「チップ SIM（インダストリアル）」の場合、納品日から 334 日を経過して利用開始登録がされていないSIM を強制的に黒化し、チップSIM 維持料金が請求されます。（※強制黒化の状態になっても利用開始登録がされるまで通信はできません）