さくらインターネット 専用サーバ付加サービス（マネージアップ） パッケージ お申込書

[お申込みの際の注意事項]
・本お申込書は原本のみ有効で、FAX・コピー等では受付いたしておりません。
・お申込み前にサービス約款(http://www.sakura.ad.jp/join/agreement/agreement.html)をお読みください。
・本契約は、消費者契約法に基づくクーリングオフを行うことは出来ません。
・本契約を未成年者の方が行う場合、親権者の方が了承した上で行わなければなりません。
・本申請書は、申請年月日より3ヵ月間有効です。
・お申込受理後、請求書のお支払期限までに入金がない場合は、自動的にキャンセルとして扱わせていただきます。

ご契約者情報

①～⑤の項目についてご記入下さい

申請年月日	年 月 日

①会員ID	□ 会員IDなし (新規お申込み)	□ 会員IDあり	[ ]	例：abc12345
②ご契約者	種別	□ 営利法人	□ 社団法人	□ 自営業	□ 医療法人
		□ 個人	□ 任意団体	□ その他法人 ( )	
	フリガナ				
	組織名／お名前	印			
	性別	□ 男性	□ 女性	生年月日	年 月 日
④ご住所	〒				
	建物・ビル名 ( )				
⑤ご連絡先	電話番号	( ) －		FAX番号	( ) －
	ﾒｰﾙｱﾄﾞﾚｽ	@		ﾒｰﾙｱﾄﾞﾚｽ (予備)	@

専用サーバサービス基本情報

①～②の項目についてご記入下さい。

①サービスコード													
②基本IPアドレス	.	.	.										

※新規に専用サーバサービスと同時にお申込みのお客様は記入不要です。

パッケージお申込み情報（新規）

新規お申込みのお客様は以下いずれかのパッケージをご選択ください。

パッケージの選択	□ step1パッケージを申し込む
	このパッケージには以下のサービスが含まれます。 サービス監視、ネットワーク監視、アクセス解析
	□ step2パッケージを申し込む
	このパッケージには以下のサービスが含まれます。対象のサービスについてお申込み情報のご記入が必要です。 サービス監視、ネットワーク監視、障害復旧、セキュリティアップデート、バックアップ（5GB)、アクセス解析
	□ step3パッケージを申し込む
	このパッケージには以下のサービスが含まれます。対象のサービスについてお申込み情報のご記入が必要です。 サービス監視、ネットワーク監視、障害復旧、セキュリティアップデート、バックアップ（30GB)、ファイアウォール、アクセス解析

プラン変更情報（※）

（※）現在マネージアップをご利用中のお客様でパッケージを変更される場合のみご選択ください。

ご利用中のパッケージ	□ step1パッケージ	□ step2パッケージ	□ step3パッケージ

変更後のプラン	□ step1パッケージへ変更する	□ step2パッケージへ変更する	□ step3パッケージへ変更する

お支払い方法	□ 銀行振込	□ 金融機関自動口座振替	自動口座振替依頼書を送付しますので必ずご返送ください。
	□ 郵便振替・コンビニ決済	□ クレジットカード	必ず「クレジットカード登録申込書」を同封の上ご返送ください。

※本申請書面の内容は改善等の理由のため予告なく変更することがございます。

<郵送先> 〒541-0054 大阪府大阪市中央区南本町1-8-14 堺筋本町ビル9階 さくらインターネット株式会社「マネージアップ」申込宛
<お問合せ先> さくらインターネットサポートセンター 0070-800-816398 月～金 10:00～18:00

サービス監視お申込み情報

①～③の項目についてご記入下さい。 ※ご記入が必要なお客様：全てのお客様（Step1、Step2、Step3共通）

①監視対象サービス	□ ICMP（icmp）	□ HTTP（80：tcp）	□ HTTPS（443：tcp）	□ FTP（21：tcp）	□ SSH（22：tcp）
	□ TELNET（23：tcp）	□ SMTP（25：tcp）	□ POP3（110：tcp）	□ IMAP（143：tcp）	□ DNS（53：tcp）
②オプション	□ Ping が通らない場合弊社判断でリブートを行うことを了承する（※1）				
	□ web の ステータスコード 400番台をエラーとして扱うことを認める				
③通知先メールアドレス（3箇所設定可能）	登録先1	@			
	登録先2	@			
	登録先3	@			

（※1）サーバリブート対応時、OSやアプリケーション、ハードウェアの障害が判明する場合がございます。
本サービスではこの場合の復旧作業は対象外となります。別途担当へご相談ください。

リソース監視お申込み情報

①～②の項目についてご記入下さい。 ※ご記入が必要なお客様：全てのお客様（Step1、Step2、Step3共通）

①サーバプラットフォーム	□ FreeBSD4以上	□ RedHatLinux 9以上
	□ Fedra Core1以上	□ Debian 3.0以上
②ご利用条件	このサービスはお客様のサーバへ監視エージェント（SNMP)を投入し設定を行います。	
	このため弊社監視用ネットワークからの制限解除が必要ですのでご了承のほどよろしくお願いいたします。	
	○弊社設定時に必要な制限解除ポート(SSH 22:tcp)	
	○サービス提供のため必要な制限解除(SNMP 161:tcp)	

[！重要！ 本サービスに関する注意事項]
・サーバの再インストール等をお客様側の理由で行われた場合、本サービス提供のために再度弊社側での設定が別途必要となります。
・上記に関連し弊社側で再度サーバへの設定作業を行った場合は、別途有料となりますのでご了承ください（\5,250税込）
・Windows Serverが搭載されたサーバはサービス対象外となります。
※本申請書面の内容は改善等の理由のため予告なく変更することがございます。

バックアップお申込み情報

※ご記入が必要なお客様：Step2、Step3をお申込みのお客様

バックアップ対象パス（絶対パスを記入）	登録例	/home/abc/123
	登録先1	
	登録先2	
	登録先3	
	登録先4	
	登録先5	

[！重要！ 本サービスに関する注意事項]
・バックアップの容量は、Step2をお申込みの場合は最大5GB、Step3をお申込みの場合は最大30GBとなります。
・本サービスは、弊社管理用ネットワークである 210.224.172.0/24 および 210.188.224.0/24 よりお客様サーバへ対する接続を行います。
サーバへアクセス制限を行われている場合は、(SSH 22:tcp) に対する解除の設定が必要となります。
・本サービスは、SSHでルートログインのうえrsyncを利用しデータのバックアップを行います。
このためSSHでルートログインするための設定およびrsyncのインストールを行いますのであらかじめご了承ください。
・WindowsServerが搭載されている専用サーバは本サービス対象外となります。
・サーバ障害の発生などによりOS再インストールとなった場合は、新規OS上の指 定パス以下にバックアップデータの書き戻し行います
（/home/backup以下へ書き戻し）
・バックアップデータ取得のタイミングは、毎朝5時／1日・1回となります。
・データの世代管理は行いません。
・Windows Serverが搭載されたサーバはサービス対象外となります。

障害復旧お申込み情報　「障害復旧 各サービスの接続確認および対応方法について」をご確認のうえ①～②の項目をご記入下さい

※ご記入が必要なお客様：Step2、Step3をお申込みのお客様

①サーバプラットフォームのご確認		□ FreeBSD4以上	□ RH Linux9以上	□ Fedora Core1以上	□ Debian 3.0以上	
		※上記各OSバージョン以下のOSが搭載されたサーバへの本サービス適用は不可となりますのでご了承ください。				
②対応サービスの選択	PING (icmp)	□ 要	□ 不要			
	HTTP (80/tcp)	□ 要	□ 不要			
	HTTPS(443/tcp)	□ 要	□ 不要			
	FTP (21/tcp)	□ 要	□ 不要			
	POP3 (110/tcp)	□ 要	□ 不要			
	IMAP(143/tcp)	□ 要	□ 不要			
	SMTP (25/tcp)	□ 要	□ 不要			
	TELNET (23/tcp)	□ 要	□ 不要			
	SSH (22/tcp)	□ 要	□ 不要			

[本サービスに関する注意事項]

・「対応サービスの選択」欄では、それぞれのサービス項目に対するサービスの監視及び障害検知から障害復旧作業の要/不要を必ずご選択ください。

・miniadmin/minirootのパスワードを削除された場合は、管理ユーザのパスワードを弊社宛にご連絡頂く必要があります。

・「要」とされたサービス項目に関しては、「障害復旧 各サービスの接続確認および対応方法について」に基づき障害復旧を行います。

・「不要」とされたサービス項目に関しては、弊社での監視・障害検知および障害の復旧は行われません。

・各サービスの接続確認および対応方法については「障害復旧 各サービスの接続確認および対応方法について」をご参照ください。

・本サービスでは弊社管理用ネットワークである 210.224.172..0/24 および 210.188.224.0/24 からお客様サーバへ対する接続・監視を行わせて頂きます

・前項に関連し Tcp wrapper、ファイアウォールによるフィルタリング設定等を行れる場合は、210.224.172..0/24 および 210.188.224.0/24のネットワークからの接続を許可する設定を行って頂く必要があります。

・Windows Serverが搭載されたサーバはサービス対象外となります。

障害復旧 各サービスの接続確認および対応方法について

PING (1/icmp)

確認方法	(1)リモートよりPINGによるサーバへの接続確認を行います。 (2)PINGによる応答がない場合は、現地でのコンソールによる状況確認を行います。
対応方法	サーバが停止している場合は、電源再起動などによる復帰作業を行います。

HTTP (80/tcp)／HTTPS(443/tcp)

確認方法	(1)ブラウザでの該当IPアドレスでのウェブの表示を確認します。 (2)表示できない場合、サーバにログインを行い、サーバ内でhttpdが動作しているか確認します。
対応方法	(1) サービスが停止または動作異常と確認された場合は、再起動コマンドを実行します。 ・FreeBSDの場合 /usr/local/etc/rc.d/apache.sh restart ・Redhat/Fedoraの場合 /etc/init.d/httpd restart ・Debianの場合 /etc/init.d/apache restart その後、ps コマンドでhttpdプロセスの稼動を確認します。また、ブラウザでウェブの表示状態を確認します。 (2)その他トラブルが発生している場合は、お客様に

FTP (21/tcp)

確認方法	(1)FTPコマンドによる該当IPアドレスへの接続確認を行います。 (2)接続できない場合は、サーバにログインを行い、サーバ内から接続できるか確認を行います。
対応方法	1) サービスが停止または動作異常と確認された場合は、サービスまたはinetd、xinetdの再起動コマンドを実行します。 ・FreeBSDの場合 killall HUP inetd ・Redhatの場合 /etc/init.d/xinetd restart ・Fedoraの場合 /etc/init.d/vsftpd restart その後、プロセスの稼動または、接続を確認します。 (2)その他トラブルが発生している場合は、お客様に状況のご報告を行います。

POP3 (110/tcp)／IMAP(143/tcp)

確認方法	(1)TELNETコマンドにより外部より110番及び、143番ポートへの接続を確認します。 (2)接続できない場合、サーバにログインを行い、サービスが動作しているかを確認します。
対応方法	(1) サービスが停止または動作異常と確認された場合は、サービスまたはinetd、xinetdの再起動コマンドを実行します。 ・FreeBSDの場合inetdの状態確認を行い killall HUP inetd ・Redhatの場合 /etc/init.d/xinetd restart ・Fedoraの場合 /etc/init.d/dovecot restart ・Debianの場合 /etc/init.d/qpopper restart その後、ps コマンドでサービスプロセスの稼動と接続を確認します。

SMTP (25/tcp)

確認方法	(1)TELNETコマンドにより外部より25番ポートへの接続を確認します。 (2)接続できない場合、サーバにログインを行い、サーバ内でサービスが動作しているかを確認します。
対応方法	(1) サービスが停止または動作異常と確認された場合は、再起動コマンドを実行します。 ・FreeBSDの場合 cd /etc/mail →make restart ・Redhat/Fedoraの場合 /etc/init.d/sendmail restart ・Debianの場合 /etc/init.d/exim restart その後、ps コマンドでサービスプロセスの稼動と接続を確認します。 (2)その他トラブルが発生している場合は、お客様に状況のご報告を行います。

TELNET (23/tcp)

確認方法	(1)TELNETコマンドにより弊社より接続を確認します。 (2)接続できない場合、サーバにsshにてログインを行いサービスが動作しているか確認します。 (3)sshでのログインもできない場合、現地よりコンソールにログインを行い、サーバ内でサービスが動作しているか確認しま
対応方法	(1) サービスが停止または動作異常と確認された場合は、サービスまたはinetd、xinetdの再起動コマンドを実行します。 ・FreeBSDの場合inetdの状態確認を行い killall HUP inetd ・Redhatの場合 /etc/init.d/xinetd restart ・Fedoraの場合 /etc/init.d/dovecot restart ・Debianの場合 /etc/init.d/qpopper restart その後、ps コマンドでサービスプロセスの稼動と接続を確認します。

SSH (22/tcp)

確認方法	(1)SSHコマンドにより弊社より接続を確認します。 (2)接続できない場合、現地よりコンソールにログインを行い、サーバ内でサービスが動作しているか確認します。
対応方法	(1)サービスが停止または動作異常と確認された場合は、再起動コマンドを実行します。 ・FreeBSDの場合 kill HUP `cat /var/run/sshd.pid` または /usr/sbin/sshd ・Redhat/Fedoraの場合 /etc/init.d/sshd restart ・Debianの場合 /etc/init.d/sshd restart その後、ps コマンドでサービスプロセスの稼動と接続を確認します。 (2)その他トラブルが発生している場合は、お客様に状況のご報告いたします

ファイアウォールお申込み情報 ①～③の項目についてご記入下さい。※ご記入が必要なお客様：Step2、Step3をお申込みのお客様

①アクセス制限の可否		☐ アクセス制限を行う ※アクセス制限を行う場合は、下記②で選択したサービスのみ外部からのアクセスが許可されます。 なお、制限を行う場合でも、内部から外部向けの通信は全て許可されます。		
		☐ アクセス制限を行わない ※全てのアクセスが許可されます。		
②各アクセス制限		「アクセス制限を行う」にチェックいただいた方のみ以下事項のチェック及びご記入をお願いいたします。		
基本サービス	例) PING (icmp)	☐ 全体から許可する	■ 接続元を制限する	接続元：[210.188.224.0/255.255.255.0(IPアドレス/ネットマスク指定]
	※PING (icmp)	☐ 全体から許可する	☐ 接続元を制限する	接続元：[ ]
	※SSH (22/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	※FTP (21/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	※HTTP (80/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	※POP3 (110/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	※SMTP (25/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	TELNET (23/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	HTTPS (443/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	NNTP (119/tcp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	DNS (53/udp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	NTP (123/udp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
	SNMP (161/udp)	☐ 許可する	☐ 接続元を制限する	接続元：[ ]
ご確認事項		※印のついた項目はサーバ上で稼動する基本的なサービスとなります。通信を許可されない場合、運用に際し充分ご留意ください。		

		ポート番号	プロトコル(TCP/UDP)	接続元
その他サービス（記入式）	設定内容	例　8765	TCP	210.188.224.0/24

③攻撃対策設定	☐ 攻撃対策を有効にする	☐ 攻撃対策を無効にする