項目	連携メニューに関する質問	質問の回答
1	お客様サーバへの外部からの攻撃を、サイバーセキュリティクラウド社のIPSにてブロックする前に、サイバーセキュリティクラウド社からお客様に事前連絡をして頂くことは可能でしょうか？	IPSモードで動作している場合、攻撃を検出した際、自動的にブロックが行われる仕様となり、これを変更することはできません。代替案としては、「IDSモードで動作し、攻撃検出メールを確認次第、手動でブロックを行う」という使用方法も考えられます。 しかし、攻撃検出時、お客様にブロック可否判断を仰いでいる間、または手動で対応を行っている間に、侵入を許してしまう危険性もありますので、この仕様が最も安全かと思われます。
2	IPSのソフトウェアを仮想サーバに登録するときに必要な情報項目があれば教えてください。	登録するときに必要な情報項目は下記になります ・企業名 ・契約期間 ・導入作業（お客様側で行うか、サイバーセキュリティクラウド側で行うか） ・URL ・IPアドレス ・rootID（サイバーセキュリティクラウド側で導入作業を行う場合） ・ご報告用メールアドレス ・機器利用内容（例：WEBサーバ） ・OS ・下記ディレクトリの場所 /var/log/messages /var/log/secure /var/log/maillog /var/log/httpd/error_log /var/log/httpd/access_log
3	お客様サーバからサイバーセキュリティクラウド社の仮想アプライアンスにログを送信する経路と、セキュリティーをどのように確保しているのでしょうか。	AES128による暗号化処理がされています。また、仮想アプライアンスにおいて不具合が生じた際にはその旨を伝えるアラートが上がる仕様になっております。
4	万が一、誤検知して通信を遮断した場合の、サイバーセキュリティクラウド社とお客様の責任範囲を事前に把握したいので条件を教えて頂くことは可能でしょうか。	本サービスはシグネチャを用いた検出を行っておりますので、正常な通信であれば誤検知は考えられません。また、条件につきましては、サービス約款にて記載されておりますので、お問い合わせください。
5	IPSでお客様サーバ側の通信を遮断した場合のメール報告は、自動設定で送られてくるイメージ でしょうか？	仰るとおり、仮想アプライアンスに設置してあるシグネチャで攻撃を検知した際、システムから自動でメールが送られる仕組みになっております。
6	IPS側で誤検知してお客様側の通信を遮断した場合、どうしたら解除できるのでしょうか？（明示的に解除したい場合の方法を教えて欲しい）。	前述の通り、誤検知は通常考えられません。しかし、もし万が一誤検知にてブロックしてしまった場合の対処方法としては、 ・ブロック処理解除までお待ちいただく ・手動でiptablesの通信拒否行を削除 その後、 ・該当通信元からのIPアドレスをホワイトリストへ登録するようご依頼いただく といった対応が考えられます。
7	IPS-LB-Webサーバ-DB サーバ　というロードバランサを挟んだシステム構成の場合、サーバテクトのIPSは利用できるのでしょうか？	左記のような構成でも導入は可能です。 ・LBにサーバテクトは導入できない（OSがないため） ・LBで負荷分散がされている場合、分散先のサーバ全てに導入の必要性がある 上記2点は注意点としてご参考下さい。