CYBER SECURITY CLOUD

クラウド型 Web Application Firewall
「攻撃遮断くん」ご提案
補足資料

2018年7月
株式会社サイバーセキュリティクラウド

1:サーバセキュリティタイプ（IPS＋WAF）

サーバセキュリティタイプの特長

1. **様々な環境での導入が対応が可能**

   サーバのRoot権限があれば、エージェントプログラムを埋め込むだけで導入が可能です。
   クラウド型(SaaS)のため、各社様のクラウド環境(IaaS)にも対応しております。

2. **サーバへの負荷は1%以下**

   攻撃の判定をクラウド上の監視センターで行うことにより攻撃の検知・遮断の最中でもサーバへの負荷は1%を超えません。また導入によりサーバやサービス性能への影響はほとんどありません。

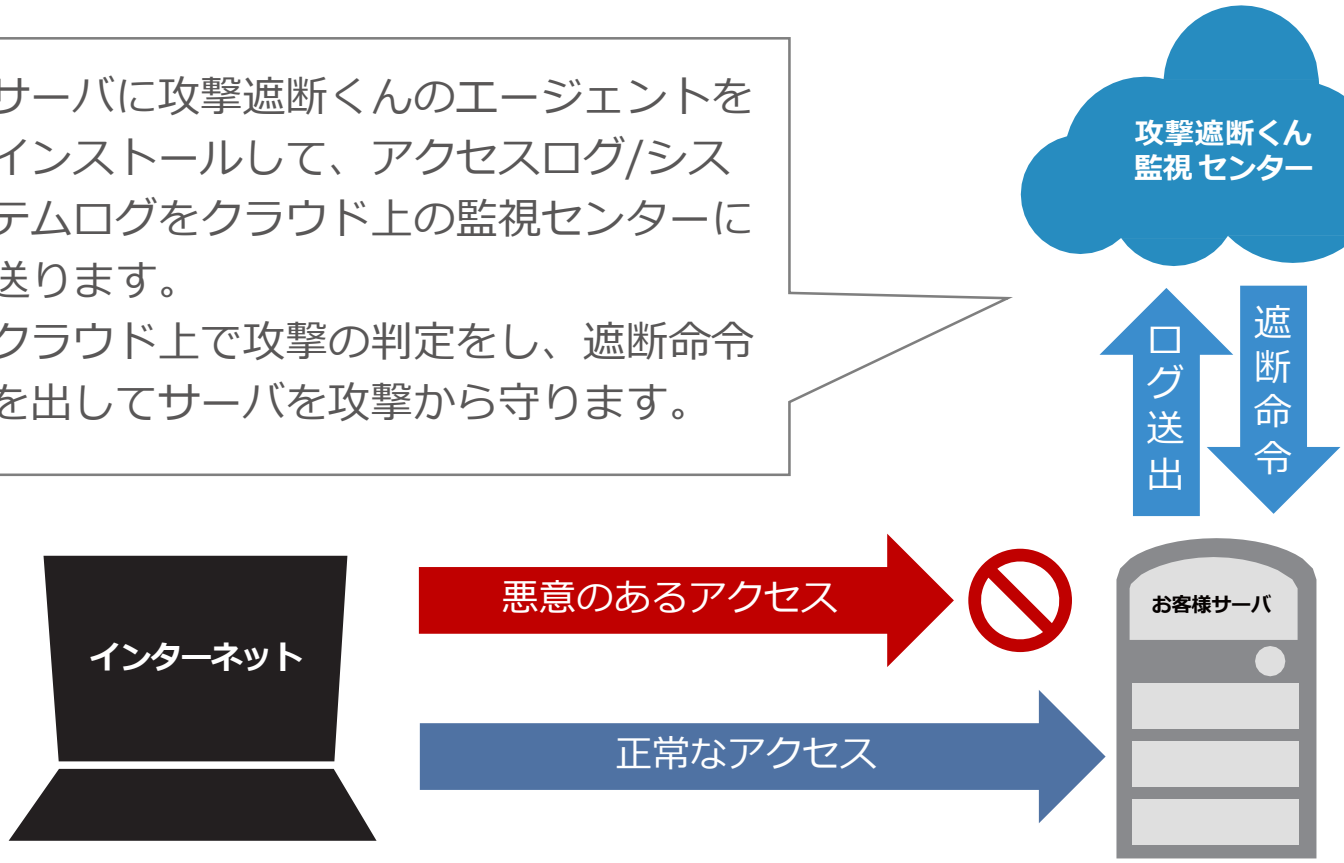
3. **サービスへの影響なし**

   通信はクラウド上の攻撃遮断くん監視センターとの（アクセスログ/システムログ）のみとなる為、
   障害発生時にもお客様側のサービスに影響しません。

サーバセキュリティタイプ仕様

IPS＋WAFの革新的な仕組みにより、ネットワーク、OS、WEBアプリケーションへのサイバー攻撃を防ぎます。サイトを訪れるユーザーへのレスポンスにも影響しません。

サーバに攻撃遮断くんのエージェントをインストールして、アクセスログ/システムログをクラウド上の監視センターに送ります。
クラウド上で攻撃の判定をし、遮断命令を出してサーバを攻撃から守ります。



サーバセキュリティタイプ導入要件①

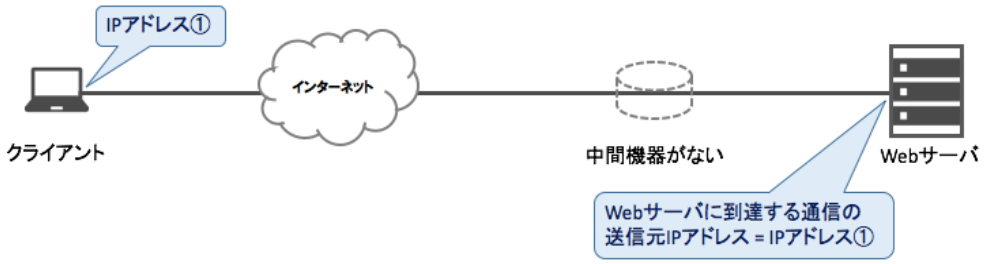
No	導入前確認	詳細・備考
0	検知・遮断動作確認のため、CSC(IP:153.156.84.123、52.68.229.190)より数リクエストの擬似攻撃を不定期に実施することがございます。	
1-1	Webサーバに到達するIPアドレスの確認し、詳細・備考欄に記載の遮断方法が利用できること ※別紙の参考図Aをご参照ください	Webサーバにクライアントの IPアドレスが直接到達する、かつ iptables(firewalld)/Windowsファイヤウォールが利用できる。 ※No.1-1に合致しない場合には、No.1-2へお進みください。合致する場合は、No.1-2の確認は不要です ※検知モードのみでご利用される場合はiptables(firewalld)/Windowsファイヤウォールは不要です
1-2	Webサーバに到達するIPアドレスの確認し、詳細・備考欄に記載の遮断方法が利用できること ※別紙の参考図Aをご参照ください	Webサーバに中間機器のIPアドレスが到達する、かつModSecurityがインストールできる。 ※検知モードのみでご利用される場合はModSecurityのインストールは不要です ※IISには対応しておりません ※No.1-1、No.1-2に合致しない場合や、不明な場合には、お問い合わせください
2	エージェント発行する際に IPアドレスでの発行かANYキーでの発行か確認した ※別紙の参考図Bをご参照ください	参考図をご参照して、どちらのキーを発行するか確認してください ※お客様でのエージェント発行時に、必要な情報となります
3	管理者権限（root）アカウントを使用可能（※） 共用のレンタルサーバではない	エージェントをインストールする際に、root権限が必要となります 管理者権限(root)がない場合、導入することができません。WEBタイプでの導入が可能ですのでお問い合わせ下さい。
4	下記の環境が整っていること（※） ・コンパイラ "gcc" または "cc" ・コマンド "make"	エージェントをインストールする際に必要となります。 Windows/RedHat 6.X/RedHat 7.X/Ubuntu 14.04/Ubuntu 16.04の場合には本項目は確認不要ですのでチェックしてください。
5	UDPのハイポート（10000以上）を制限していない	監視センターと通信するために使用します <制限している場合> FWの設定を変更し、弊社指定のポートを開放する必要がございます
6	監視対象IPアドレスが固定されている （変化しない）	変化する場合には、エージェント発行時に"any"キーでの登録が必要となります
7	Dockerなどコンテナ環境を利用していない	利用している場合には、お申し込み前に必ずご相談ください
8	オートスケール環境ではない	利用している場合には、お申し込み前に必ずご相談ください
9	CDN(Contents Delivery Network)を利用していない	利用している場合には、お申し込み前に必ずご相談ください

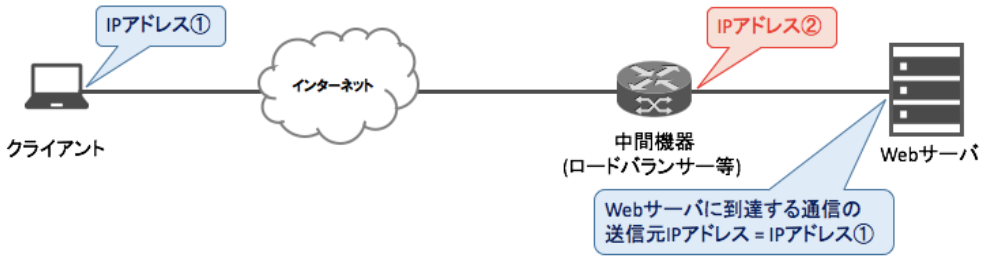
サーバセキュリティタイプ導入要件②

No	監視ログについて	詳細・備考
1	ログ形式にカスタマイズを加えていない	デフォルト以外の場合は弊社側でカスタマイズが必要となりますので、ログサンプルをご送付ください 例）　LTSV、その他の形式、ログフォーマットの変更 攻撃遮断くんの初期設定では下記のログが対象となります ログインログ(secure), メールログ(maillog), メッセージログ(messages), アクセスログ(httpd/access_log), エラーログ(httpd/error_log)
2	ログにクライアントのIPアドレスが記述されている	＜記述されていない場合＞ x-forwarded-forを使ってユーザのIPアドレスを取得する必要がございます。 その際には、サーバやLBなどの設定変更が必要になる場合がございます
3-1	ログファイル名に日付が含まれていない	含まれている場合にはNo.3-2に進んでください ※No.3-1に合致する場合には、No.3-2の確認は不要です
3-2	ログファイル名に日次が含まれる（※） かつ 毎日ローテンションされている	No.3-1、No.3-2のいずれにも合致しない場合には、下記に変更する必要がございます ・ログファイル名に日付が含まれなていない形式にする もしくは ・ログファイル名に日次が含まれる、且つ毎日ローテーションする形式にする
4	※Windows IISの場合（※） ログファイルのローテーション時間がサーバの時間になっている	Noの場合には、日本時間に設定変更する必要がございます ※Windowsサーバの場合には、デフォルトでUTCになっているのでご注意ください
5	WEBサーバでPOSTを使用していない	POSTメソッドのパラメータを使用した攻撃を検知するためにはログへの出力が必要となります。 ※POSTログを出力させるためにはお客様で設定作業をしていただく必要がございます ※Windows IISに関しては、POST出力ができませんのでご了承ください

サーバセキュリティタイプ　参考図A

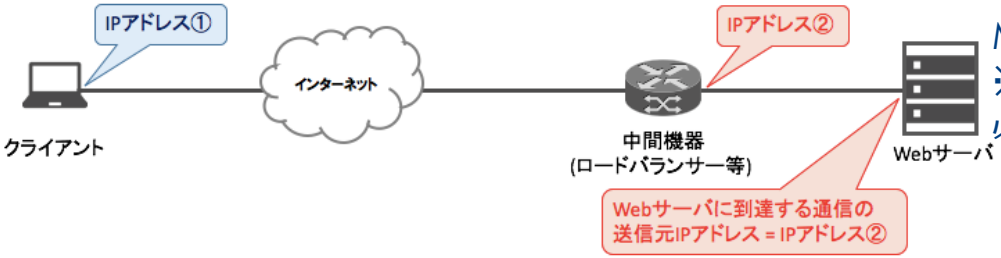
Webサーバにクライアントの IPアドレスが到達する





iptables等による遮断方法となります

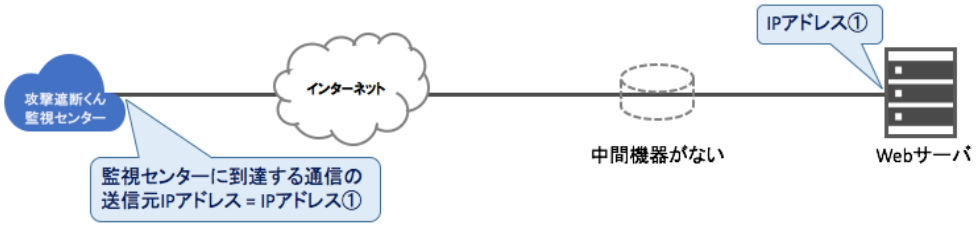
Webサーバに中間機器の IPアドレスが到達する



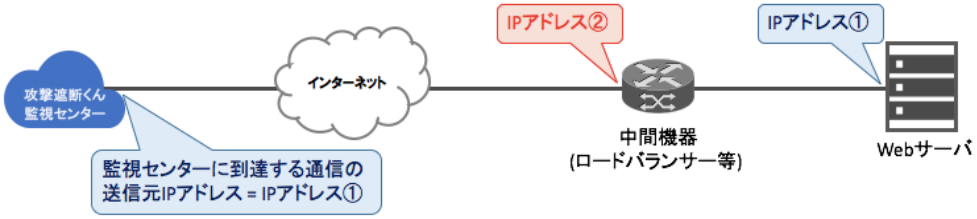
ModSecurityによる遮断方法となります
※お客様でWebサーバに組み込んでただく必要がございます

サーバセキュリティタイプ　参考図B

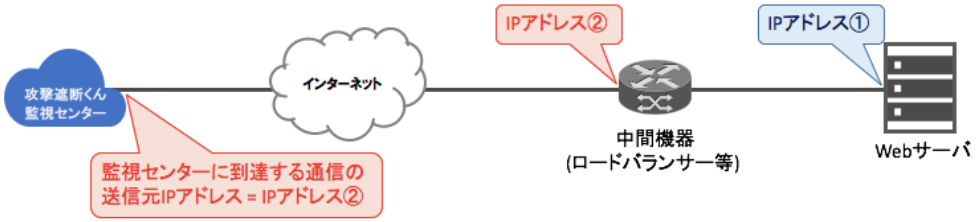
監視センターにWebサーバのIPアドレスが到達する



WebサーバのIPアドレスで
エージェントキーを発行



監視センターに中間機器のIPアドレスが到達する



ANYキーで
エージェントキーを発行

2:WEBセキュリティタイプ（WAF）&DDoSセキュリティタイプ（WAF＋DDoS対策）

WEB/DDoSセキュリティタイプの特長

1. ネットワーク構成の変更やサーバ停止の必要なし

担当者様の作業はDNSの切り替えだけ。簡単に導入が可能です。

2. DDoS対策機能

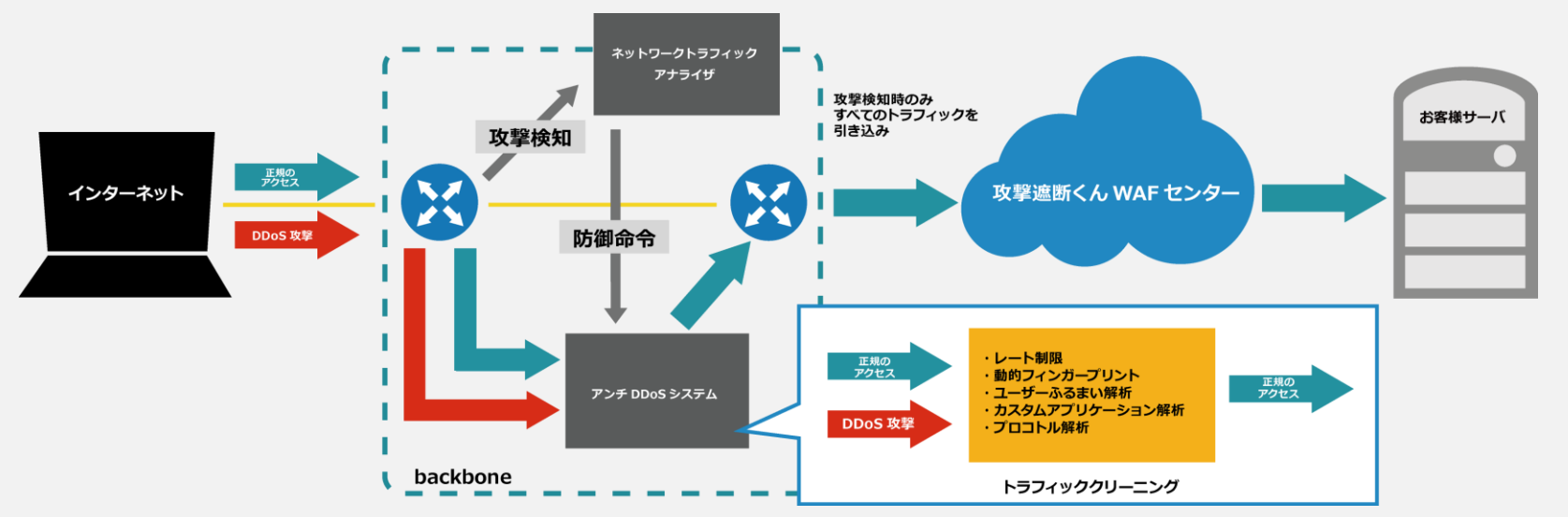
WAFでは防御できないDoS/DDoS攻撃を、お客様ネットワークより上位のネットワーク側で検知/軽減するサービスです。

WEB/DDoSセキュリティタイプの基本動作

お客様のシステムに変更を加えることなく、DNSの切替えだけで短期間での
WAF導入が可能です。シグネチャ更新や運用は、全て「攻撃遮断くん」が対応します。

SaaS/クラウドの形で提供するタイプ。
DNSを切り替えるだけで簡単に導入可能です。
WAFセンターを経由して、正規のアクセスはそのまま通し、不正なアクセスはWAFセンターで遮断します。

DDoSセキュリティタイプ基本動作/特長



DDoS対策

WAFでは防御できないDoS/DDoS攻撃を、
お客様ネットワークより上位のネットワーク側で検知/軽減することにより、サーバやネットワーク機器、インターネット回線までを含めた防御が可能です。

対象のDoS/DDoS攻撃

- TCP（Syn flood, Ack flood, Fins flood, Fragments）
- HTTP GET/POST Flood
- HTTP Slow Attack Protection
- UDP（Random port Floods、Fragments）
- ICMP（Unreachable, Echo, Fragments）
- Connection Exhaustion
- Stream Flood
- DNS Flood attacks

特長

お客様ネットワークに最適化したポリシー

サービス開始にあたって、事前に防御対象ネットワークのトラフィックを学習/分析します。その学習結果に基づいて、お客様ネットワークに最適化した防御ポリシーを設定することにより、精度の高いクリーニングを実現します。

不正なトラフィックを選択的に遮断

平常時は、ネットワークトラフィックアナライザによってトラフィックのモニタリングのみを実施し、異常を検知した場合のみ、お客様サーバ/ネットワーク宛のすべての通信をアンチDDoSシステムへ引き込みます。アンチDDoSシステムは引き込んだ通信を精査し、不正なトラフィックをクリーニングの上、正常な通信をお客様サーバ/ネットワークへ転送します。

WEBセキュリティタイプ/ DDoSセキュリティタイプ導入時の注意点

No.	導入前確認点	詳細・備考
0	検知・遮断動作確認のため、CSC(IP:153.156.84.123、52.68.229.190)より数リクエストの擬似攻撃を不定期に実施することがございます。	
1	DNSの切り替えが可能である	
2	使用するプロトコルはHTTP/HTTPSのみである	その他のプロトコルはWAFセンターを経由することができませんので、 IPアドレス直　もしくは、別FQDNを割り当ててください。 HTTP/80, HTTPS/443以外を利用の場合には、ご連絡ください。
3	証明書をWAFセンター用に用意できる	HTTPSを利用する場合、お客様にてSSL証明書一式（SSLサーバ証明書、中間CA証明書、秘密鍵など）のご用意とWAFセンターへの設定依頼が必要となります。 ※現在ご利用中の証明書のコピーでも問題ございません。
4	クライアント証明書は使用していない	クライアント証明書は対応はしておりません。
5	CDN(Contents Delivery Network)を利用していない	CDNをご利用されている場合には、１サイトプランはご利用いただけません。WEBサイト入れ放題プランのご案内となりますので、ご相談ください。
6	ドメインエイリアスを行っていない	同じドメインで「www.」あり、なしのいずれのものでアクセスされても、同じサイトを表示される設定を行っている場合、「www.」あり・なし2つのFQDNをお申込みいただく必要がございます。
7	ソースIPがWAFセンターのIPアドレスになるが、問題ない	ソースＩＰアドレスは、ＨＴＴＰヘッダ内に以下のフォーマットをお送りしますので、必要に応じて設定の変更をお願いいたします。 X-Forwarded-For：XXX.XXX.XXX.XXX (ソースIPアドレス) 【ソースIPアドレス使用例】 ・アクセス解析　※GoogleAnalyticsなどのビーコン型には影響ありません。 ・ソースIPアドレスを利用したWEBアプリケーションによる表示変更 ・ソースIPアドレスを利用したロードバランシング

WEBセキュリティタイプ/ DDoSセキュリティタイプ導入時の注意点

No.	導入前確認点	詳細・備考
8	ファイアーウォールでＩＰアドレスの制限をしていない	<特定のIPアドレスのみ許可をしている場合> 1サイトプランでは対応できないため、WEBサイト入れ放題プランをご検討ください。 <同じＩＰアドレスからの同時接続数を制限している場合> ソースIPがすべてWAFセンターのIPアドレスになるため、制限の解除をお願いいたします。
9	httpsのWebサイトに、 ガラケーや古いブラウザからのアクセスは受け付けなくても良い	受け付ける必要がある場合には、SNI非対応対応として別途費用が発生いたしますので、お問い合わせください ※httpのみのWebサイトの場合は、問題ございません。
10	1リクエストで20MBを超えるファイル転送は行われていない	ファイル転送容量が20MBを超える場合は、WEBサイト入れ放題プランをご検討ください。
11	タイムアウト値が60秒となるが、問題ない	1サイトプランでは、タイムアウト値を60秒とさせていただいております。 タイムアウト値を60秒以上またはそれ以下を希望される場合は、WEBサイト入れ放題プランをご検討ください。

3:ご利用料金

サーバセキュリティタイプ　ご利用料金

プラン名	単位	初期費用	費用／月
ベーシックプラン（サーバ１台毎）	1～3IP(1IPあたり)	10,000円	40,000円
	追加1IP(4IP以降)		10,000円

※１ヶ月単位の契約が可能です。
※20IP以上、または中間機器に導入する場合は別途お問い合わせください。
※秒間4,000リクエストを超過する場合、別途お問い合わせください。

プラン名	初期費用	費用／月
使い放題プラン（サーバ台数無制限）	500,000円	800,000円

※初回６ヶ月利用後、単月での更新となります。
※親会社・子会社・関連会社までご導入可能です。詳細は別途お問い合わせください。
※秒間4,000リクエストを超過する場合、別途お問い合わせください。

Web/DDoSセキュリティタイプ「１サイトプラン」ご利用料金

		Webセキュリティタイプ		DDoSセキュリティタイプ	
プラン名	ピーク時 トラフィックの目安	初期費用	費用／月	初期費用	費用／月
1サイト プラン	～500kbps	30,000円	10,000円	30,000円	15,000円
	500kbps～ 2Mbps		30,000円		40,000円
	2Mbps～5Mbps		50,000円		60,000円
	5Mbps～ 10Mbps		100,000円		120,000円

オプション	費用/月
月次レポート	20,000円
スポット作業	**費用/月**
登録済みFQDNの変更や転送先IP変更について	10,000円
SSL証明書更新時の差し替え作業	

※課金体系は1FQDNごとになります。１ヶ月単位の契約が可能です。
※SNI非対応端末には 別途ご相談ください
※大幅な超過、長時間にわたる超過があった場合には弊社によりご連絡をさせていただき、月次以降のプランの変更をお願いする場合がございます。自動的にプランが更新される、もしくは従量課金のように請求額が変動するといった事もございません。

Web/DDoSセキュリティタイプ「入れ放題プラン」ご利用料金

	Webセキュリティタイプ		DDoSセキュリティタイプ	
トラフィックの上限	初期設定費用	月額利用費用	初期設定費用	月額利用費用
～100Mbps	150,000円	180,000円	200,000円	220,000円
～200Mbps	220,000円	340,000円	270,000円	380,000円
～300Mbps		450,000円		480,000円
～400Mbps		550,000円		580,000円
～500Mbps		600,000円		620,000円
～1Gbps		700,000円		720,000円

スポット作業メニュー	費用	サービス概要
帯域の変更	70,000円	※契約後に帯域を変更する場合、1回につき変更作業を¥70,000-にて承ります。 ※平日営業時間受付、２～３営業日で反映いたします。
FQDN登録・ SSL登録	無料	・登録済みFQDNの変更や転送先IP変更（最大10件／月） ・SSL証明書更新時の差し替え（最大10件／月） ・新規FQDN登録（最大10件／月） ※上記件数を超えた場合、1回につき10件までの作業を¥30,000-にて承ります。 ※1度に50件を超える作業の場合、価格ならびに納期のご相談をさせていただきます。 ※平日営業時間受付、２～３営業日で反映いたします。
遮断・検知モード切替		お客様から弊社サポート窓口までご連絡いただければ、随時切替させていただきます。 ※平日営業時間受付、０～２営業日で反映いたします。

お問い合わせ

電話でお問い合せ：03-6416-1579（平日10:00～18:00）

メールでお問い合わせ：sales@cscloud.co.jp

Webからお問い合せ：https://shadan-kun.com/

会社名	株式会社サイバーセキュリティクラウド
本社所在地	〒150-0011 東京都渋谷区東3-9-19　VORT恵比寿maxim3階
電話番号	03-6416-9996
FAX番号	03-6416-9997
Webサイト	http://www.cscloud.co.jp
代表取締役	大野 暉
事業内容	Webセキュリティ事業 ・Webセキュリティサービスの開発・運用・保守・販売 ・サイバー攻撃対策コンサルティング