スマートコネクト マネージドサーバ

WAF オプション 仕様書

(第 1.0 版 2015 年 6 月 22 日版)

We are the future.

Smart Connect

＜ 目次 ＞

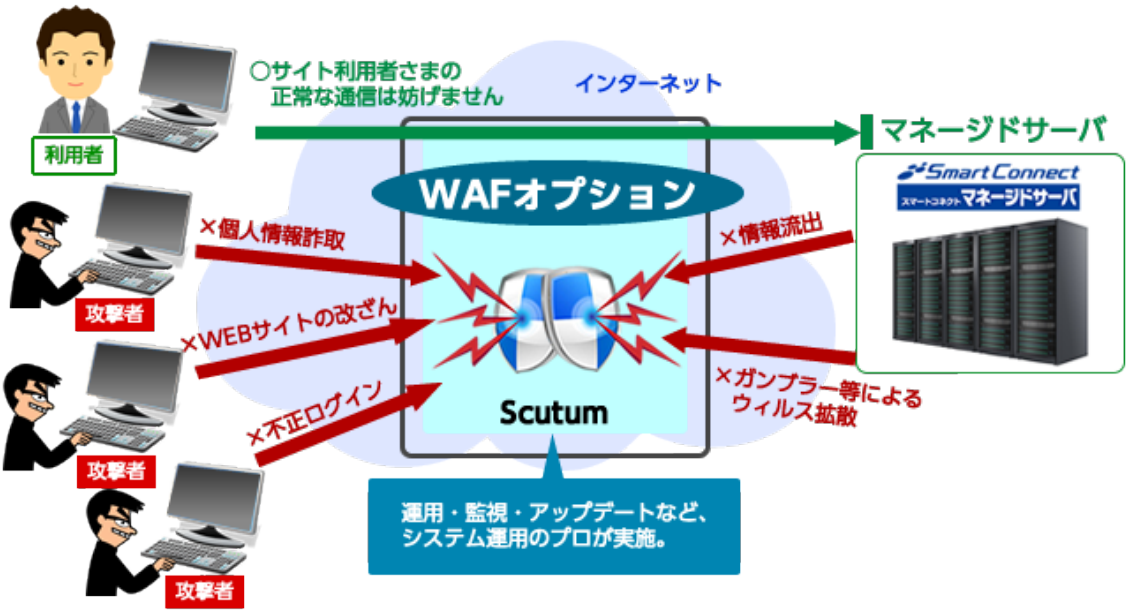
◆ スマートコネクト マネージドサーバ WAF オプション

1. WAF オプション概要

1.1. オプション概要

WAF オプション（以下、本オプション）は、スマートコネクト マネージドサーバ（以下、マネージドサーバ）を利用して提供する Web サイトについて、Web アプリケーションの脆弱性を突いた攻撃から防御するためのオプションサービスです。

WAF オプションはリバースプロキシとして提供します。DNS サーバに登録する Web サーバ（マネージドサーバ）の IP アドレスを、本来の Web サーバの IP アドレスから WAF 設備の IP アドレスに切り替えることでご利用いただけます。



1.2. オプション特徴

（1）実績のある WAF サービスを採用

SaaS 型 WAF サービスとして多くの実績を持つ、株式会社セキュアスカイ・テクノロジーの「Scutum（スキュータム）」を採用しています。

（2）導入・運用が容易

Web 管理画面による簡易な設定と、DNS サーバの設定変更を行うだけで容易に導入が可能です。専門知識を要するパラメータチューニングは必要ありません。 アップデートも自動的に行うので、運用の負担もありません。

（3）多くの攻撃を防御可能

下表に示す、多くの攻撃から防御可能です。

攻撃区分	攻撃名称
認証	総当たり
クライアント側の攻撃	クロスサイトスクリプティング（XSS）、クロスサイトリクエストフォージェリ（CSRF）
コマンド実行	バッファオーバフロー、書式文字列攻撃、OS コマンドインジェクション、LDAP インジェクション、SQL インジェクション、Xpath インジェクション、SSI インジェクション
情報公開	ディレクトリインデクシング、パストラバーサル
マルウェア対策	ドライブバイダウンロード攻撃

※すべての攻撃に対する防御を保証するものではありません。

2. WAF オプション仕様

2.1. オプション提供プラン

本オプションで提供するプランは以下のとおりです。

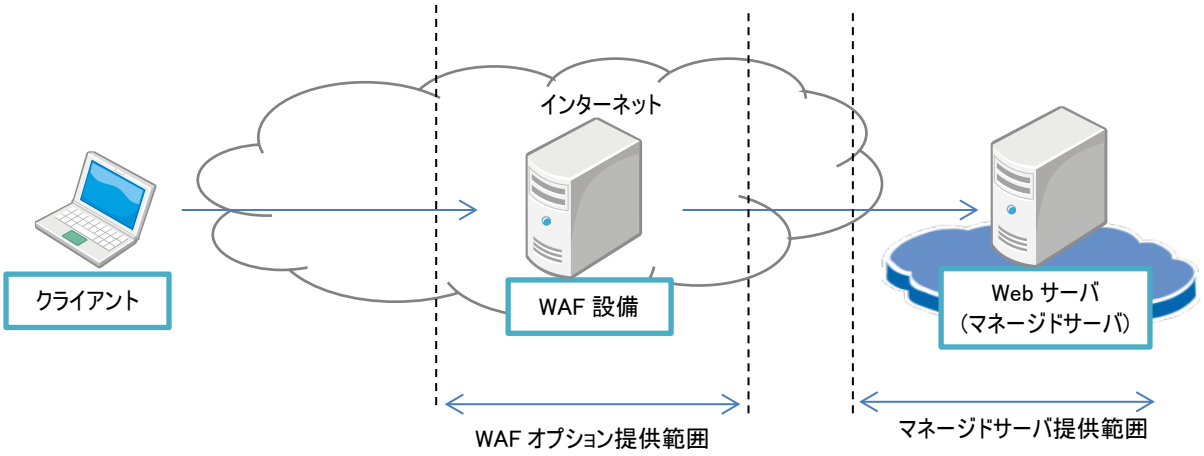
品目	単位	備考
WAF（～500kbps）	1ドメイン（1FQDN）	ピーク時トラフィックが、500kbps未満の場合
WAF（500kbps～5Mbps）	1ドメイン（1FQDN）	ピーク時トラフィックが、500kbps以上5Mbps未満の場合
WAF（5Mbps～10Mbps）	1ドメイン（1FQDN）	ピーク時トラフィックが、5Mbps以上10Mbps未満の場合
WAF（10Mbps～50Mbps）	1ドメイン（1FQDN）	ピーク時トラフィックが、10Mbps以上50Mbps未満の場合
WAF（50Mbps～100Mbps）	1ドメイン（1FQDN）	ピーク時トラフィックが、50Mbps以上100Mbps未満の場合

ピーク時トラフィックが不明の場合には、当社インフォーメーションセンタまでお問い合わせください。ヒアリングに基づき、予想帯域を提示させていただきます。

ピーク時トラフィックがご契約の品目で定めた帯域を越える場合には、上位の品目に契約変更をお願いいたします。お客さまのご利用状況によっては、ご契約品目の範囲でトラフィックの制限をさせていただく場合があります。

2.2. 提供範囲

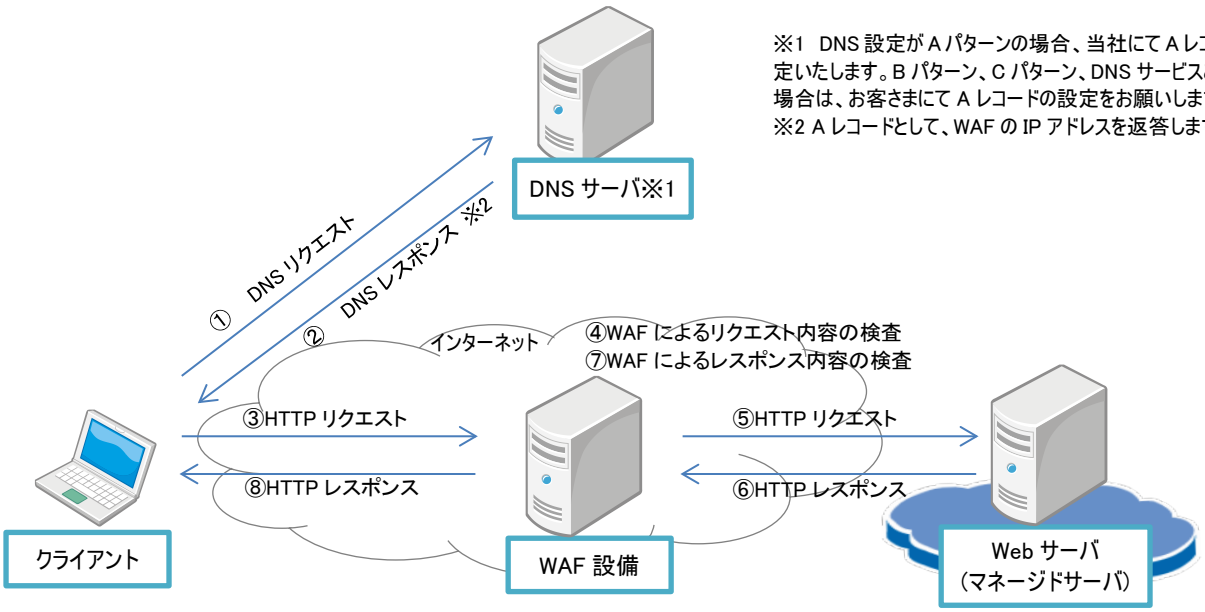
本オプションの提供範囲は以下の通りです。



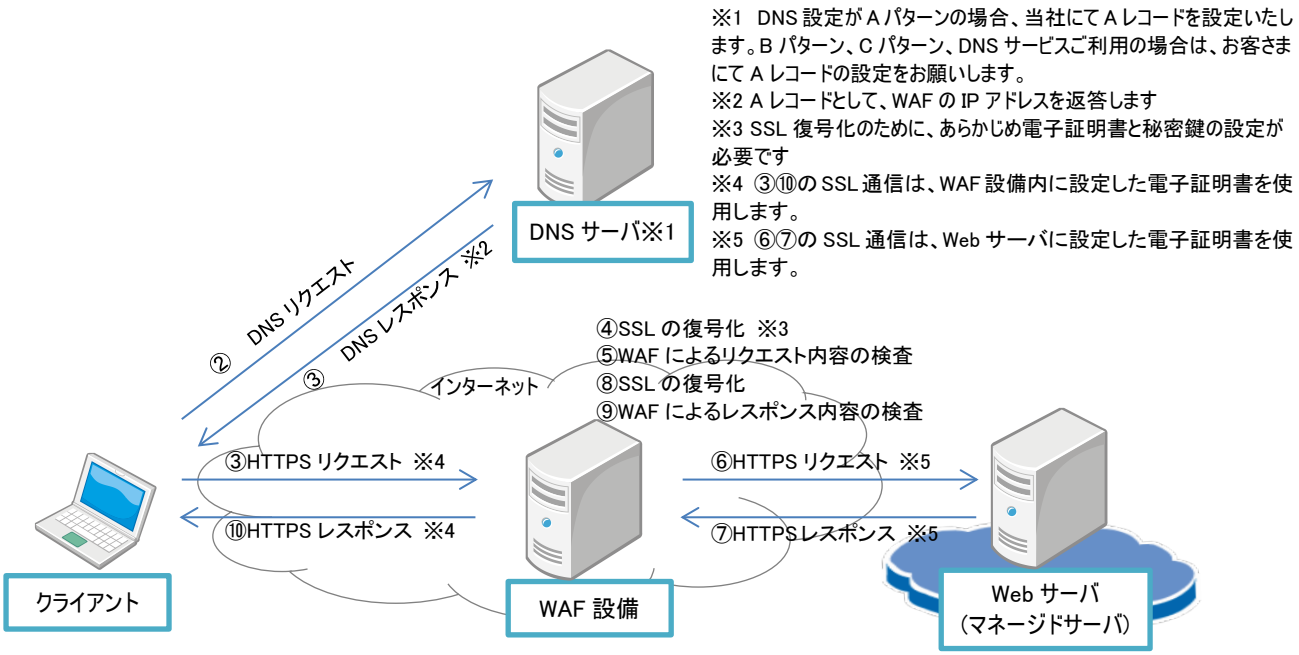
2.2. 通信方式

本オプションの通信方式は以下の通りです。

2.2.1. HTTP（TCP ポート 80）



2.2.2. HTTPS（TCP ポート 443）



2.2.3. HTTP（TCP ポート 80）・HTTPS(TCP ポート 443）以外の通信

HTTP（TCP ポート 80）と HTTPS（TCP ポート 443）以外は、WAF 設備を経由した通信はできません（例：ステージング用ポート、メール、SSH など）。これらのポートを利用する通信は、マネージドサーバのホスト名（sXXXXX.mngsv.jp）をご利用いただき、マネージドサーバと直接通信するようにしてください。

2.3. オプション機能一覧

本オプションにて提供する機能は以下のとおりです。

項目	内容	scutum 設定画面名	備考
防御機能	あらかじめ登録されている不正な通信パターンを検出した場合、該当通信を遮断します。	WAF 機能制御	
モニタリング機能	あらかじめ登録されている不正な通信パターンを検出した場合、該当通信を記録します。（通信自体は遮断されません）		
ログ機能	Scutum にて検出された不正と思われる通信を記録し、閲覧できます。ログについては一定期間後消去されます。	ログ閲覧	正常な通信のアクセスログは、マネージドサーバのアクセスログに記録されます。
ソフトウェア更新機能	Scutum の防御機能等を向上させるため、ソフトウェアを更新します。	なし	サービス提供者側で実施しますので、お客さまによる作業は不要です。
シグネチャ更新機能	防御効果の向上を図る為、不正な通信パターンを随時最新の状態に更新します。	なし	サービス提供者側で実施しますので、お客さまによる作業は不要です。
特定 URL 除外機能	防御機能が不必要な Web ページを防御対象から除外できます。	除外 URL の設定	
レポート機能	下記の内容を管理画面（Web ブラウザ利用）上で確認できます ・攻撃元（IP アドレス）top5 ・攻撃種別 top5 ・防御ログの月別ダウンロード	ログ閲覧	
IP アドレス拒否/許可機能	特定の IP アドレスからの通信を拒否、もしくは特定の IP アドレスからの通信のみ許可することができます。	IP アドレスの拒否/許可の設定	
SSL 通信機能	SSL 通信を解読し、防御することができます。	SSL 証明書の更新	・お客さまが scutum 管理画面から、SSL 証明書、中間証明書、秘密鍵を設定する必要があります。

			・SSL 証明書を当社からご購入いただいた場合には、SSL 証明書・中間証明書・秘密鍵については当社から所定の方法でお客さまに提供させていただきます。 ・SSL 証明書持ち込みの場合には、お客さまにて SSL 証明書・中間証明書・秘密鍵をご準備ください。 ・SSL 通信を利用するには、マネージドサーバ側にも SSL 設定が必要です。 ・証明書の更新時には、マネージドサーバ側での更新および scutum 管理画面での更新が必要です。

2.3. HTTP ヘッダ

WAF を経由した時には、マネージドサーバ（Web サーバ）に対して以下の HTTP ヘッダが付与されます。

HTTP ヘッダ名	内容
X-Forwarded-For:	アクセス元クライアントの IP アドレス
X-Forwarded-For2:	アクセス元クライアントの IP アドレス
X-Client-Port:	アクセス元クライアントのポート番号

2.3. 制約事項

・ネットワーク的なアクセス経路が増えるため、WAF オプションを利用しない場合と比較してレスポンスが低下する可能性があります。

・レディドメインでは、WAF オプションをご利用いただけません。

・対応プロトコルは HTTP（ポート 80）と HTTPS（ポート 443）のみです。ステージングのポート（11180 および 11443）には対応しておりません。ステージングへは、テストドメイン機能を利用してアクセスしてください。

・テストドメイン機能によってアクセスする場合は、WAF を経由しません。

・クライアント証明書には対応しておりません。

・クライアントの IP アドレス制限を行う場合に、.htaccess やサーバファイアウォールによる制限ができなくなります。クライアントの IP アドレスを制限したい場合、下記のいずれかの方法で制限してください。

① X-forwarded-for ヘッダを元に制限を行う

② scutum 管理画面の「IP アドレス拒否/許可機能」でクライアント IP アドレスの制限を行う

3. WAF オプションお申込み（新規･変更･解約）

3.1. オプション開始までの所要期間

オプション開通までの所要期間は以下のとおりです。

営業日の起算は、必要事項が全て記載された申込を当社で受け付けた営業日からの日数です。

オプション	ご提供までの所要期間
WAF（全品目）	8 営業日以降の翌月末までの指定日

※開通後、お客さまによる scutum の設定変更が必要になる場合があります。

※DNS 設定が B パターン、C パターンの場合、または DNS サービスご利用の場合には、お客さまによる A レコードの変更が必要です。

3.2. オプション変更までの所要期間

オプション変更までの所要期間は以下のとおりです。

営業日の起算は、必要事項が全て記載された申込を当社で受け付けた営業日からの日数です。

オプション	ご解約までの所要期間
WAF（全品目）	8 営業日以降の翌月末までの指定日

3.3. オプション解約までの所要期間

オプション解約までの所要期間は以下のとおりです。

営業日の起算は、必要事項が全て記載された申込を当社で受け付けた営業日からの日数です。

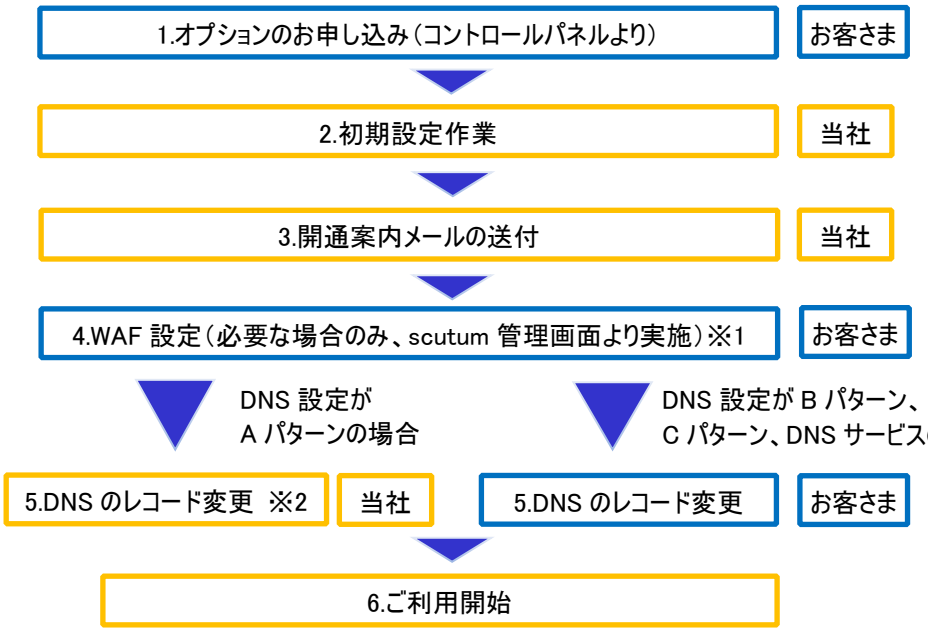
オプション	ご解約までの所要期間
WAF（全品目）	10 営業日以降の翌月末までの指定日

※月途中の解約でも、当月の月額料金は全額発生します。

3.4. オプション開始までの流れ

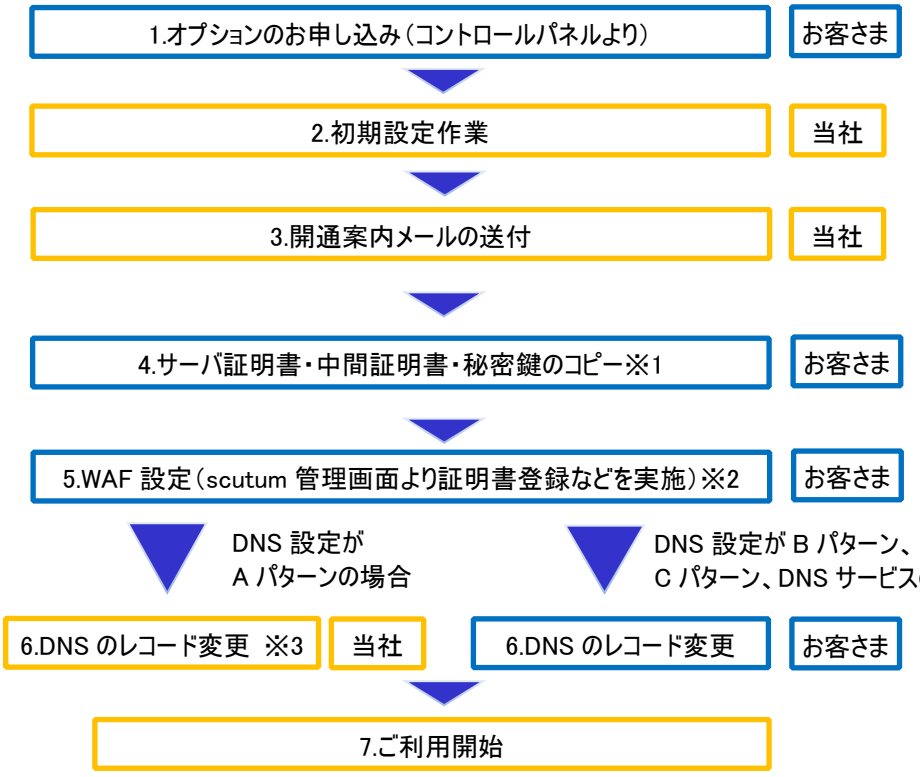
オプション開始までの流れは以下のとおりです。

3.4.1 SSL 未利用の場合



※1 モニタリング機能状態で初期導入し、誤検知がないことを確認したのちに防御機能を ON にすることを推奨します。
※2 DNS レコードの変更希望日は、お申し込み時にコントロールパネルでご指定ください。

3.4.2 SSL ご利用の場合



※1 マネージドサーバ内の所定パスにファイルを保管させていただきます。ファイルマネージャや ftp などをご利用いただき、ファイルを取得ください。
※2 モニタリング機能状態で初期導入し、誤検知がないことを確認したのちに防御機能を ON にすることを推奨します。
※3 DNS レコードの変更希望日は、お申し込み時にコントロールパネルでご指定ください。

4. 用語集

用語	説明
WAF 設備	WebApplicationFirewall 機能を提供する設備（scutum）です。リバースプロキシとして動作します。
ブロック機能	不正と思われる通信を Scutum にてブロックする機能です。ブロックされた場合、web ブラウザにブロック画面が表示されます
モニタリング機能	不正と思われる通信ではあるが、誤検知の可能性がある、もしくは攻撃だとしても危険性がそれほど高くないと思われる場合は通信をブロックせずに攻撃ログに結果を残します。 モニタリング機能のログについては、アプリケーションセキュリティ専門エンジニアが確認後ログを表示させる場合があるため、通信が発生したタイミングとログに表示されるタイミングにずれが生じる場合があります。
防御シグネチャ	Scutum を通過する通信をブロックしたりモニタリングすることを決める基準となるルールです。攻撃が発見された場合等に随時更新されます。
scutum 管理画面	scutum の設定を行うための管理画面です。マネージドサーバのコントロールパネルとは異なります。
DNS 設定	A パターン：お客様ドメインについて、プライマリ DNS サーバ・セカンダリ DNS サーバともに当社が提供します。 B パターン：お客様ドメインについて、プライマリ DNS サーバはお客さまにご準備いただきます。セカンダリ DNS サーバは当社が提供します。 C パターン：お客様ドメインについて、プライマリ・セカンダリともにお客さまにご準備いただきます。

5. 変更履歴

版数・日付	変更内容
初版（2015.6.22）	