Confidential

文書番号 SST-SCTM-20121024-01

Scutum サービス仕様書

Version1.2

Secure Sky Technology Inc.

株式会社 セキュアスカイ・テクノロジー

更新履歴

日付	Version	摘要
2009/06/01	1.0	初版発行
2011/04/19	1.1	広帯域メニュー追加に伴う修正
2012/10/24	1.2	オプションメニュー（CDN）追加に伴う修正

目次

1 はじめに

1.1. 本資料について

本資料は SaaS 型 Web アプリケーションファイアーウォールサービス「Scutum」(以下本サービス)のサービス仕様を説明するものです。

1.2. 用語の説明

- 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。通信を実施している方の web ブラウザー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、モニタリングすることを決める基準となるルール。お客様毎に必要に応じてカスタマイズします。また新しい攻撃が発見された場合等に随時更新されます。
- CDN データ量
  ScutumCDN オプションを利用した場合の、CDN を利用したデータ量です。
- オリジンサーバ
  Scutum を導入する Web サイトを指します。
- CDN サーバ
  ScutumCDN オプションで利用する CDN 機能を提供するサーバです。このサーバーに配信する画像やファイルを保存します。

2 サービス概要

2.1. Scutum について

本サービスは、お客様サイトへのエンドユーザからの通信を弊社が提供するWebアプリケーションファイアウォール（以下 WAF）を経由させることにより、不正な通信を防御するサービスです。

SST が管理する Scutum センターを経由する形で Web アプリケーションファイアウォールの機能を提供いたします。

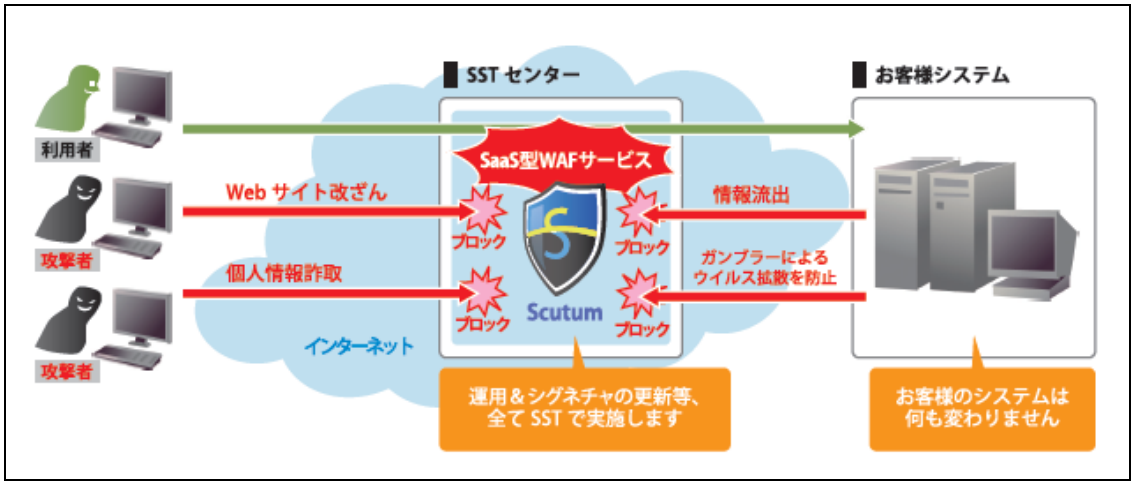


図 1 Scutum サービスイメージ

本サービス形態では、お客様の Web サーバが本来持つ IP アドレスを Scutum の IP アドレスとなるように DNS の設定を変更するだけで設定が完了します。余分な自前の設備を持つことなく、より安全な Web サービス環境を構築することができます。

3 Web アプリケーションファイアウォール機能

3.1. ブロック、モニタリング機能

本サービスを利用するWebサイトに対して攻撃と思われる通信をブロックもしくはモニタリングする機能です。ブロック(モニタリング)する基準は本サービスで提供する防御シグネチャとなります。この防御シグネチャは定期的に更新されます。

防御する主な脆弱性は下記となります※。

区分	認証	クライアント側での攻撃	コマンド実行	情報公開	マルウェア対策
名称	総当り	クロスサイトスクリプティング クロスサイトリクエストフォージェリ	バッファオーバーフロー OS コマンドインジェクション SQL インジェクション XPath インジェクション 書式文字列攻撃 LDAP インジェクション SSI インジェクション	ディレクトリインデクシング 情報漏えい パストラバーサル リソース位置を推測	ガンブラーによるウィルス拡散

※ 一部攻撃についてはシグネチャ以外で対応するものもございます。

※ 上記攻撃を100%防御するものではありません。

3.2. 防御ログ閲覧機能

防御シグネチャにより、ブロック(モニタリング)した通信をログとして保存する機能です。ログの内容はScutum管理画面にて提供されます。ログは一覧と詳細で提供されます。機密情報保護の観点から詳細ログについては一定期間後消去されます。

3.3. ソフトウェア更新機能

ブロック・モニタリング機能等を向上させる為、ソフトウェアを更新する機能となります。

3.4. シグネチャ更新機能

ブロック・モニタリング機能の向上を図る為、不正な通信パターンを随時最新の状態に更新する機能となります。

3.5. 特定 URL 除外機能

本サービスを利用する Web サイト中の WAF 機能を利用したくない箇所を URL 単位で除外する事ができます。本機能は Scutum 管理画面にて提供されます。

3.6. レポート機能

以下の内容を Scutum 管理画面上で報告する機能となります。

- 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

3.7. IP アドレスの拒否／許可の設定機能

本サービスを利用する Web サイトへの特定 IP アドレスからの通信を拒否することができます。ホワイトリスト、ブラックリストによる設定が可能です。本機能は Scutum 管理画面にて提供されます。

3.8. SSL 通信機能

本サービスでは SSL にて暗号化されている通信についても防御することが可能です。本機能を利用する場合は電子証明書と秘密鍵が必要になります。

電子証明書と秘密鍵は Scutum 管理画面からアップロードできます。

4 オプション機能

4.1. ScutumCDN オプション

4.1.1. サービス概要

ScutumCDN オプションは、Scutum を導入している Web サイトに手軽に CDN 機能をご利用いただけるサービスになります。

画像ファイルや大きな PDF ファイルなどを CDN サーバ上から配信することにより、Web 閲覧を高速かつ安定して行えるようになります。また、海外等の遠隔地からの接続については、その接続元に近い CDN サーバから配信することにより素早いレスポンスで表示させることが可能になります。

4.1.2. 提供機能

特定のファイル（画像や PDF ファイル等）を CDN サーバに保存し配信できます。遠隔地から閲覧する場合は接続元に近い CDN サーバから該当するファイルを配信します。お客様の Web サーバへのアクセスが混み合った時のみ CDN サービスを利用することも可能です。

4.1.3. キャッシュ可能なファイル

- 画像ファイル(jpeg,jpg,gif,png)
- PDF ファイル(pdf)
- JavaScript（js）

※ファイルサイズの上限は、1 ファイル 200MB までとなります。

4.1.4. 提供価格

初期料金：無料
月額料金：無料（100GB/月）

4.1.5. 利用方法

本オプションサービスは Scutum 管理画面よりお申し込みいただけます。メニュー上で CDN オプション機能を選択し、初回利用時に利用規約をご確認いただき、問題がなければ OK ボタンを押下していただければ利用開始となります。

4.1.6. 利用上の注意点

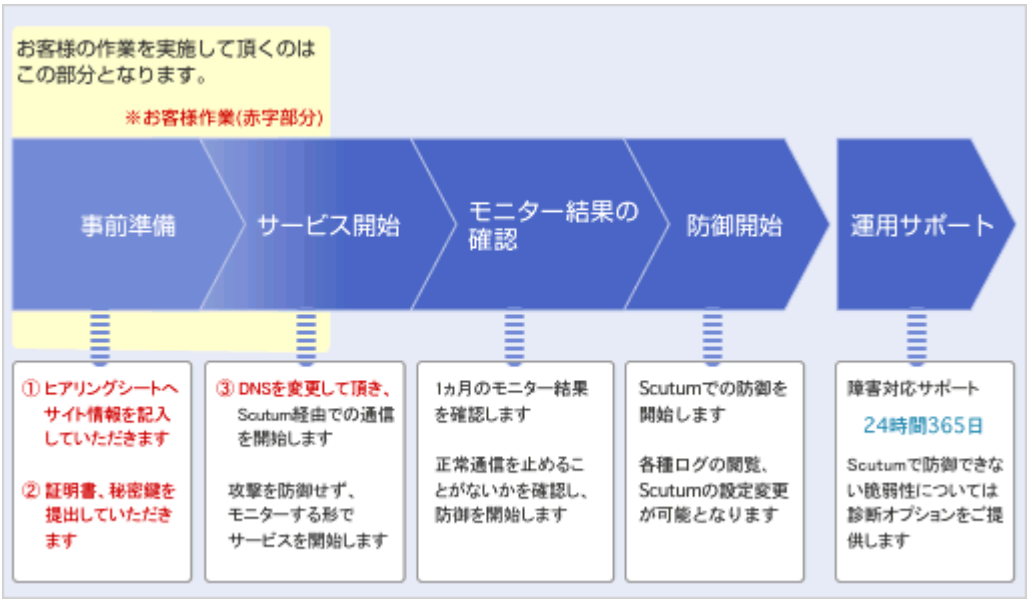
ScutumCDN オプションを利用する場合は以下の注意点をご確認ください。

- CDN を利用する際には、保存するファイルの URL がオリジナルのものから変更されて配信されます。
- CDN を利用するファイルを即時クリアすることは原則としてできません。基本は 24 時間で新しいものに変更されます。
- CDN を利用してすぐのファイルへのアクセスは若干遅くなる場合があります（CDN サーバへのコピーを行っているため）。
- CDN を利用するファイルは海外に設置されている CDN サーバに保存されます。
- 携帯電話での HTTPS の利用は推奨いたしません（エラーが表示される場合があります）。
- フラッシュサイトでの利用は推奨いたしません（画像表示でエラーが発生する場合があります）。
- CDN オプションによって CDN サーバ上にキャッシュされた画像等を直接削除することはできません。オリジンサーバで削除後、最大 24 時間以内に CDN サーバから自動削除されます。
- 同一ファイル名（同一パス）の画像/PDF ファイルで、その内容が動的に変化する場合であっても、CDN オプションによりキャッシュされた CDN サーバ上の画像/PDF は最大 24 時間の間、更新前の内容が表示され続けることになります。
- 実質的に画像/PDF であっても、ファイル名（URI）の拡張子が「jpg/jpeg/gif/png/pdf」のいずれかに該当しないものは、CDN オプションのキャッシュ対象となりません。

5 運用管理機能

5.1. 初期設定及び導入作業

本サービスの初期設定及び導入は以下の流れとなります。



5.2. Scutum 管理画面の提供

5.2.1. Scutum 管理画面とは

サービス利用者にお客様専用の Web サイトを提供します。利用されるサイト毎に一つの Scutum 管理画面を提供します。

5.2.2. Scutum 管理画面にて提供する機能

1	防御ログの閲覧
2	ログ統計機能（攻撃元 IP アドレス Top5、攻撃種別 Top5）
3	WAF 防御 on/off 機能
4	除外 URL の設定
5	IP アドレスの拒否/許可の設定
6	管理 Web サイト用アカウント管理　　※パスワード、メールアドレスの変更
7	証明書の更新
8	Web サーバの設定
9	Scutum パネルの管理
10	CDN 機能の管理

※操作方法は、別途提供するマニュアルをご参照ください。

5.2.3. ユーザ ID・パスワード、メールアドレスの設定変更

Scutum 管理画面のユーザ ID・パスワードは、弊社より発行致します。パスワード、連絡先メールアドレスはお客様自身で変更することが可能です。

変更申請は、Scutum 管理画面よりいつでも実施可能です。

5.3. 契約者設定情報の変更

契約者設定情報（以下「設定」）の変更が必要になった場合、お客様の申請に従い、設定変更を行います。

- 変更申請はメールにて 24 時間 365 日受付けます。
- 設定変更申請は予め登録頂いた方からのみの受付となります。
- 設定変更実施希望日時をご指定される場合は、変更実施希望日の 5 営業日前までにご申請ください。
- 申請受領後、受付連絡を実施し、内容を確認した後に申請受領連絡を行います。
- 受領連絡は、本サイトから申請された場合はメールにて行います。
- 受領連絡にてお伝えした実施日時で設定変更を行います。
- 設定変更後メールにて完了を連絡します。

5.4. 防御シグネチャの更新

Scutum は不正な通信をシグネチャにて防御いたします。Web アプリケーションの脆弱性に対する主要な攻撃の多くをカバーしています。新たな脆弱性についても、随時シグネチャを更新して対応いたしますが、お客様の通信に影響が出ないことを確認した上で反映いたします。また、更新作業によりシステムが停止する等の影響はございません。

5.5. 不正と思われる通信の判定

不正な通信のうち、誤検知の可能性あるものや、危険性が高くないと判定された場合は、通信をブロックせずにログにのみ記録します。この状態を判定待ちといいます。判定待ち状態では、ログをアプリケーションセキュリティ専門エンジニアによる解析後、攻撃とされたもののみ WAF コントロールパネルに表示されます。表示には、アプリケーションセキュリティ専門エンジニアの解析の時間を要するため、通信が発生したタイミングから最大 2 日程度のずれが発生します。

5.6. システム監視

弊社にてシステムの稼働状況を 24 時間 365 日監視いたします。万一障害が発生した場合は、次項の「障害時の対応について」にて明記されている対応を実施いたします。

5.7. 月次レポートの提供

Scutum の月次稼働レポートを有償にて提供いたします。詳細はご確認ください。

6 障害時の対応について

6.1. Scutum システム障害の基本方針

Scutum は構成される機器や回線などをすべて冗長化しているため、長時間システムが停止するような障害は想定しておりません。 ただ、万が一想定外の障害が発生し、システムが長時間停止するような事態が発生した場合は、以下に説明する内容にて障害対応を実施いたします。

6.2. 障害の定義

Scutum を利用している Web サイトが、通常よりも明らかに Web 画面の表示に時間がかかる、もしくはいつまでも画面が表示されないかエラー画面が表示される、正常な画面が表示されない（画面が何度更新しても崩れている）場合を障害と定義いたします。

6.3. 障害時の対応

Scutum システムに障害が発生し、一定時間以上回復が見込めない場合は、お客様のビジネス継続を最優先させていただくため、ご契約 Web サイトを Scutum から切り離し、通信を復旧させます。その際、お客様への確認は実施しない場合がございますので、ご了承ください。

切り離しを実施するタイミングは障害検知より 60 分後以内といたします。

6.4. 障害発生後の報告

障害発生後のご報告につきましては、個別でメール、お電話にて実施させていただきます。

6.5. 注意事項

導入方法により、上記対応が行えない場合がございますが、その際は別途協議の上、対応方法を決めさせて頂きます。

7 お問合せ

7.1. お問合せ先

緊急お問い合わせ　24 時間 365 日

ご利用上のお問い合わせ　平日　10:00～18:00

TEL：050-5539-6657

E-mail：support@scutum.jp

