文書番号 SST-SCTM-2022-03-31

Scutum サービス仕様書

Version3.1

Secure Sky Technology

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
2014/07/02	1.3	オプションメニュー（キャプチャ認証、SMS 認証）追加に伴う変更
2014/08/22	1.4	オプションメニュー（CDN）廃止に伴う修正
2014/09/10	1.5	証明書更新機能の変更による修正
2018/11/20	2.0	オプションメニュー（SMS 認証）の廃止、障害対応についての修正等
2020/11/02	3.0	API 機能追加に伴う修正
2022/03/31	3.1	弊社ロゴ変更に伴う差し替え、お問い合わせ先の修正等

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したものです。

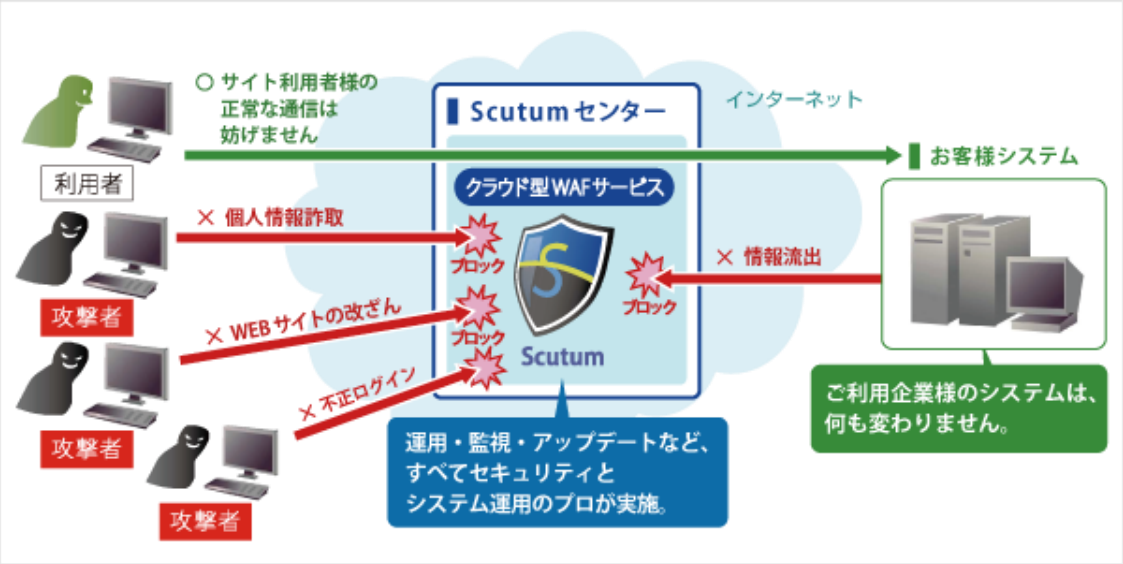
1.2. 用語の説明

- FQDN
  ホスト名とドメイン名を省略せずにつなげて指定した記述形式のことです。
- ブロック機能
  不正と思われる通信を Scutum にて防御する機能。防御された場合にはアクセス元の 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
  通信を防御せずに検知対象となる通信のログを取得する機能。
- 防御ロジック
  Scutum を通過する通信をブロックまたはモニタリングすることを決める基準となるルール。誤検知等が発生した場合、（お客様の申請により）FQDN 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。
  シグネチャだけではなく、複数のロジックを組み合わせ、ブロック、モニタリングを行います。
- API 機能
  API（Application Programming Interface）のうち、これを経由することにより、本サービスの特定の機能、情報にアクセスすることができます
- API キー
  ユーザIDおよびパスワードによりログインした者に対して発行するアクセスキー、トークン等の認証情報であって、これを利用することにより、本サービスのAPI機能を利用することができます。

2 サービス概要

2.1. Scutum について

本サービスは、DNS の設定を変更することにより、外部からの通信を Scutum センターへ経由させ、不正な通信を検知・防御する Web Application Firewall（以下 WAF）サービスです。



Scutum サービスイメージ

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ロジックです。この防御ロジックは随時更新されます。防御する攻撃の一例を以下に記載します。

攻撃区分	攻撃名称
認証	総当り攻撃、パスワードリスト攻撃　等
クライアント側での攻撃	クロスサイトスクリプティング　等
コマンドでの実行	SQL インジェクション、OS コマンドインジェクション、リモートファイルインクルージョン　等
情報公開	情報漏えい、パストラバーサル、リソースの位置を推測　等
特定ミドルウェア/フレームワーク等を狙った攻撃	ShellShock 攻撃、Apache Struts2 の脆弱性を狙った攻撃、POODLE 攻撃　等
マルウェア拡散	ドライブバイダウンロード攻撃
サービス運用妨害	プラットフォームの脆弱性をついた DoS 攻撃（ApacheKiller、hashDoS など）　等

防御できる攻撃の詳細につきましては、以下 URL をご参照ください。

https:// www.scutum.jp/details/system_and_services.html

※上記攻撃に対し、100%の防御を保証するものではございません。

3.2. 防御ログ閲覧機能

防御ロジックによりブロック（モニタリング）した通信のログは、Scutum 管理画面にて閲覧することができます。

機密情報保護の観点からレスポンスをブロック（モニタリング）した通信の詳細ログについては、一定期間後消去されます。

3.3. レポート機能

以下の内容を Scutum 管理画面上で提供する機能です。

- 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

3.4. 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です。

3.5. 防御ロジック更新機能

ブロック・モニタリング機能の向上させる為、防御ロジックを更新する機能です。

3.6. 特定 URL 除外機能

本サービスを利用する Web サイト内で WAF の防御対象外にするディレクトリを指定することができます。本機能は Scutum 管理画面にて提供されます。

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または許可することができます。本機能は Scutum 管理画面にて提供されます。

3.8. 脆弱性検査用 IP アドレスの管理機能

本サービスを利用する Web サイトへの脆弱性診断等を行う際、特定の IP アドレスからの通信については、ブロック、モニタリングを行わない設定が可能です。

本機能は Scutum 管理画面にて提供されます。尚、本機能を設定していない IP アドレスからの診断は許可しておりません。

3.9. SSL/TLS 通信機能

本サービスでは SSL/TLS 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お客様でご用意頂いた電子証明書と秘密鍵を Scutum に設定する必要があります。

電子証明書と秘密鍵は Scutum 管理画面から設定することができます。

3.10. API 機能

Scutum 管理画面で利用できる機能の一部を API にて利用することができます。利用にあたっては Scutum 管理画面より、API キーを発行する必要があります。

4 オプション機能

Scutum のオプション機能について説明します。本機能は別途オプションをお申し込んで頂いた場合のみ利用することができます。

4.1. キャプチャ認証追加機能

4.1.1. サービス概要

キャプチャ認証追加機能では、ユーザ認証などの重要な処理をより安全に実施することが可能です。

「キャプチャ認証」とは、ユーザ認証や購入決定など重要な処理を行う際、コンピューターが認識しづらい文字列の入力を利用者に促すことで、自動化されたユーザ認証等への攻撃を防止するための機能です。

Scutum を導入している Web サイトでは、本機能を利用することにより、Web アプリケーションに変更を加えることなく任意の箇所にキャプチャ認証機能を導入することができます。

4.1.2. 提供機能

- キャプチャ認証はお客さまWebサイトの任意の場所に設置可能です（標準では3箇所、設置箇所の追加も可能）。
- キャプチャ認証に表示される文字列はひらがなで3文字です。
- キャプチャ認証で表示される文字列は更新することが可能です。
- キャプチャ認証で表示される文字列には一定の制限をかけています（放送禁止用語等 NG ワードを制限）。
- キャプチャ認証を設置する箇所や設置ページのサイトデザインはお客様が自由に設定可能です。

4.1.3. 利用方法

オプションのキャプチャ認証機能を追加でお申込みいただいた場合のみ利用することができます。

管理画面中のキャプチャ認証追加機能メニューを選択し、「キャプチャ認証を有効にする」のチェックボックスにチェックを入れ反映ボタンを押下するとキャプチャ認証が有効になります。

キャプチャ認証を無効にする場合は、チェックボックスのチェックを外し、反映ボタンを押下します。

キャプチャ認証を複数箇所設定している場合でも、この有効／無効は一括で設定されます。複数あるキャプチャ認証のなかで特定箇所のみ有効（無効）にすることはできません。

4.1.4. 注意事項

- キャプチャ認証で表示される文字数やフォントは変更できません。
- 設定後、キャプチャ認証箇所を変更する場合は別途変更費用が必要です。
- キャプチャ認証オプションは利用する FQDN 毎に利用契約が必要です。

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の流れは次の通りです。

No	作業概要	作業期間	作業担当
1	ヒアリングシートの記入	―	契約者様
2	テスト環境構築	5 営業日	SST
3	テスト実施	最大 1 か月間	契約者様
4	お申し込み	―	契約者様
5	本番環境構築	5 営業日	SST
6	証明書の設定	―	契約者様
7	DNS の変更	―	契約者様

5.2. Scutum 管理画面の提供

5.2.1. Scutum 管理画面とは

契約者様に FQDN 毎に専用の管理用 Web サイトを提供します。

5.2.2. Scutum 管理画面にて提供する機能

以下に提供する機能を記載します。詳細の内容、操作方法は「Scutum お客様サポートサイト」をご参照ください。

1	WAF 機能制御
2	ウェブサーバの設定
3	IP アドレスの拒否/許可の設定
4	SSL の設定
5	ログ閲覧
6	SSL 証明書の更新
7	除外 URL の設定
8	パスワード変更
9	メールアドレスの変更
10	API の設定
11	キャプチャ機能の管理

※No11 については、オプションの「キャプチャ認証追加機能」をお申込みいただいた場合のみ利用することができます。

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します。
パスワード、連絡先メールアドレスは Scutum 管理画面より変更することが可能です。

5.3. 契約者情報の変更

契約者様情報の変更が必要になった場合、契約者様の申請に従い変更を行います。

- 契約者様情報の変更申請はメールにて受付けます。
- 契約者様情報の変更申請は予め登録頂いた方からのみ受付けます。
- 変更実施希望日時をご指定される場合は、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。
- 変更後メールにて完了を連絡します。

5.4. 防御ロジックの更新

Scutum は不正な通信を防御ロジックにて防御します。

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、Scutum にて対応可能な脆弱性は随時防御ロジックを更新して対応します。誤検知等の確認は十分に行いますが、誤検知が発生しないことを保証するものではございません。

5.5. システム監視

弊社にてシステムの稼働状況を常時監視しております。障害時の対応につきましては、「6. 障害時の対応について」をご参照ください。

5.6. 月次レポートの提供

Scutum の月次レポートを有償にて提供します。

6 障害時の対応について

6.1. 障害対応の基本方針

Scutum を構成する機器や回線などは冗長化しているため、サービスが長時間利用できない状況は想定しておりません。 ただし、想定外の事態が起こり、サービスが長時間利用できない状況が発生した場合は以下に説明する内容にて対応を実施します。

6.2. 障害の定義

Scutum の不具合に起因して Web サイトが複数回更新しても画面の表示に時間がかかる、もしくは正常な画面が表示されない場合を障害と定義します。

6.3. 障害時の対応

Scutum に障害が発生し一定時間以上回復が見込めない場合は、お客様にて DNS を変更することにより Scutum を切り離し、Web サイトの通信を継続させることが可能です。

前項 6.2 の状態が継続する時間に合わせて以下の報告を行いますので、DNS 変更の実施についてはお客様にてご判断ください。

約 10 分　　:Scutum お客様サポートサイトへ障害速報を掲載します。

約 30 分　　:該当サイトの緊急連絡先に、障害が発生している旨をメールにて通知します。

※復旧の連絡については、安定稼働確認後、Scutum お客様サポートサイトへ障害情報を掲載します。

6.4. 注意事項

Scutum は、DNS を CNAME で設定していただくことを前提に障害対応を設計しています。

Scutum では、冗長化している 2 系統のサーバに対して DNS ラウンドロビンにより通信しますが、片側でサーバダウン等の不具合が発生した場合、弊社にて不具合を検知してから約 5 分で正常稼働しているもう一方に通信を寄せる対応を行います。

また、DNS が A レコードで設定されている場合には、上記の対応を行うことができないため DNS ラウンドロビン(※)による動作となり、表示に遅延等が発生する場合があります。

このようなケースでは、片側の不具合発生検知から約 30 分で通知を行いますので、DNS 変更の実施についてはお客様にてご判断ください。

※ DNS ラウンドロビン

1つのドメイン名に複数の IP アドレスを割り当てる負荷分散技術です。ご利用のブラウザにより挙動は異なりますが、1つの IP アドレスで接続に失敗した場合、もう一方の IP アドレスに接続し直します。この際、ご利用ブラウザやサーバダウンの状態により挙動は異なり、接続できない、もしくは著しく遅延が発生する場合がございます。

7 お問合せ

7.1. お問合せ先

緊急時のお問い合わせ　24 時間 365 日

ご利用上のお問い合わせ　平日　10:00～18:00

TEL：03-3525-8828

E-mail：scutum-support@securesky-tech.com