Scutum クラウド型（SaaS型）WAFサービス 【スキュータム】

クラウド時代の、新しいWebアプリケーションファイアウォール。

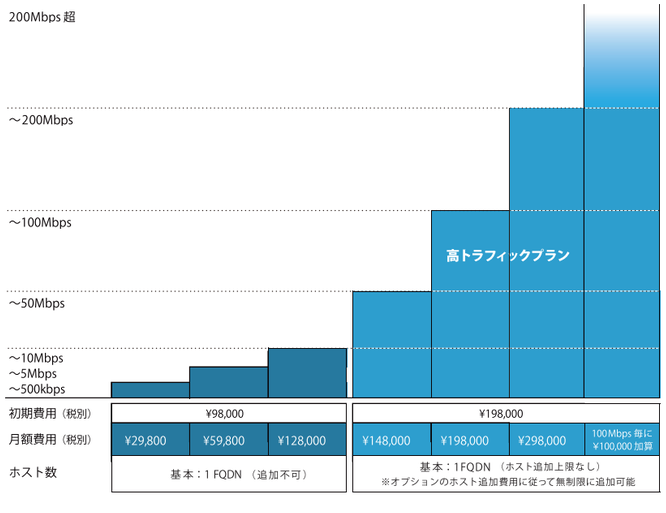
サービスメニュー／料金表

Scutum は月額制です。
小規模サイトから、100Mbps 以上の高トラフィックサイト、クラウド環境まで、柔軟に対応したセキュリティをご提供いたします。

基本料金

ピーク時トラフィックの目安	初期費用	月額費用	基本ホスト数	ホスト追加
～500kbps	¥ 98 ,000	¥ 29 ,800	1FQDN ※SSL/TLS利用可	不 可
～5Mbps		¥ 59 ,800		
～10Mbps		¥ 128 ,000		
～50Mbps	¥ 198 ,000	¥ 148 ,000	1FQDN ※SSL/TLS利用可	ホスト追加上限なし ※オプションのホスト追加費用に従って無制限に追加可能
～100Mbps		¥ 198 ,000		
～200Mbps		¥ 298 ,000		
200Mbps 超		100Mbps毎に ¥100,000 加算		

※ピーク時トラフィックは、プラン内で利用する全ホストの合計トラフィックとなります。
※プラン合計のトラフィック基準にかかわらず、1 ホストあたりのピーク時トラフィック上限の目安は 200Mbps ～ 300Mbps となります。（トラフィックが多い場合、事前にテストを実施してください）
※トラフィック算定基準はあくまでも目安となります。実際のご利用状況により異なる場合がございます。
※上記金額は税抜です。別途消費税が加算されますのでご了承下さい。



オプション

▼高トラフィックプラン（ピーク時 10Mbps 超）用オプション

オプション内容	月額費用（1FQDNあたり）
ホスト追加（SSL/TLS利用含む）	¥ 5,000

※SSL/TLS 利用について、SNI 非対応端末にはデフォルトでは対応しておりません。別途お問い合わせください。
※ホスト追加 / 変更の際は、一度に追加 / 変更する FQDN 数に応じて下記の初期費用が必要です。
・1FQDN のみ追加 / 変更：¥98,000
・2 ～ 10FQDN を追加 / 変更：¥198,000
・11FQDN 以上を追加 / 変更：¥198,000 に、10 を超える FQDN 1 件当たり ¥19,800 を加えた金額
※上記金額は税抜です。別途消費税が加算されますのでご了承下さい。

▼各プラン共通オプション

オプション内容	月額費用
月次報告書	1ホスト(FQDN)につき ¥ 20,000
Scutum DDoS 対策オプション	個別お見積り
キャプチャ認証追加機能	1サイトにつき ¥ 500 ,000 月額費用 ¥ 50 ,000 (3箇所まで認証設置可能)
Scutumケア	1サイトにつき ¥ 500 ,000

※ Scutum の利用規約に加え、IIJ 社「Web サイト不正アクセス遮断ソリューション」の利用規約にもご同意いただくことが必要です。
※ DDoS 対策オプション利用料金は個別お見積となります。詳細はお問い合わせください。
※ 設置箇所の変更には別途費用が必要となります。詳細はお問い合わせください。
※上記金額は税抜です。別途消費税が加算されますのでご了承下さい。

https://www.scutum.jp
サービス提供： 株式会社セキュアスカイ・テクノロジー
技術提供： 株式会社ビットフォレスト

netforest https://www.netforest.ad.jp/
販売代理店 株式会社ネットフォレスト
〒221-0052 横浜市神奈川区栄町5-1 横浜クリエーションスクエア16階
Tel 045-548-5548／Fax 045-548-5502
Mail nwd-sales@netforest.ad.jp

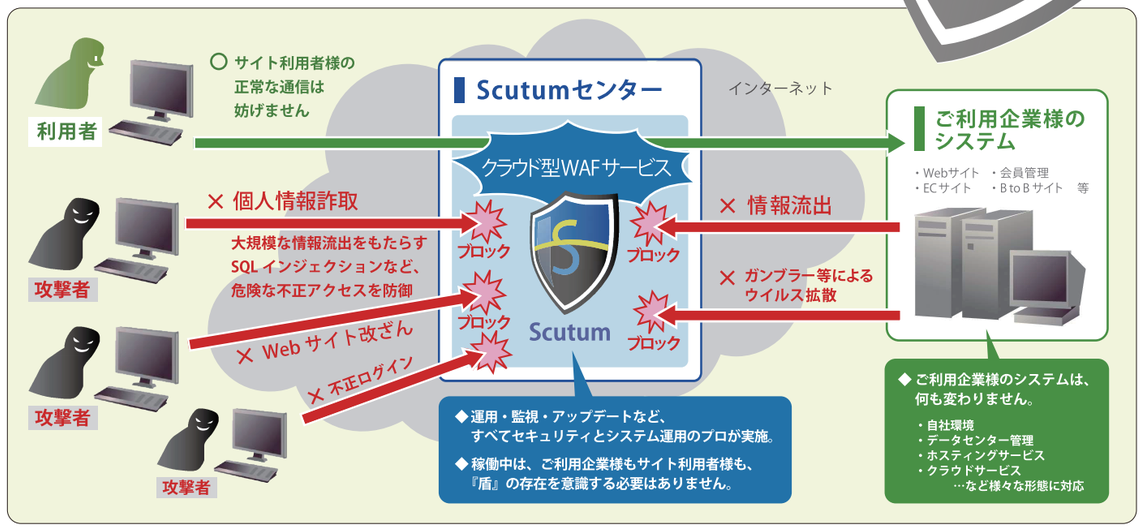
クラウド時代の、新しいWebアプリケーションファイアウォール。

Scutum クラウド型（SaaS型）WAFサービス 【スキュータム】

月額 29,800 円からのWebサイトセキュリティ対策。
個人情報／顧客情報の流出防止、サイト改ざんの防止に！

Scutum （スキュータム）とは

インターネット上で『盾』となって、御社が運営する Web サイトを不正アクセスから守るセキュリティサービスです。
運用負荷もなく、低コスト。余計な自前の設備を一切持つことなく、より安全な Web サービスの提供が可能です。



1 かんたん導入

約 **1** 週間

- **サーバ側作業は不要。約 1 週間～の短期間で導入可能**
- **緊急対応の場合、最短 3 日間での導入も可能**
  ※緊急対応の際は追加料金が必要となる場合がございます。
  ※ご利用環境 / 条件によって緊急対応の所要期間は変動します。
- **ご利用企業様では、DNS 変更と SSL 証明書情報のアップロードのみで導入準備完了**
- **小規模サイトから大規模 EC サイトまで柔軟に対応します**
- **クラウド環境上のサイトにも最適**

2 おまかせ運用

24 / 365

- **セキュリティとシステム運用のプロが 24 時間 365 日フルサポート**
- **アップデートも自動的に行われるため、放っておくだけで防御能力が常に進化**

運用 **不要**

- **基本的に、サイト運営者様の日々の管理は不要**
- **必要に応じて、管理画面やレポートで攻撃状況とプロの分析を確認可能**
  ※レポートご提供はオプションです。

3 明快な料金

約 **3** 万円～

- **月額￥29,800 ～ の固定料金**
  （税抜）
  ※導入時のみ、￥98,000 または ￥198,000 の初期費用がかかります。
  ※ピーク時トラフィックを目安にあらかじめ月額費用を設定するため、従量課金はありません。

1 か月単位

- **ご利用は 1 ヵ月から OK**
- **期間限定のサイトにも最適**

4 安心の実績

99.995％以上

- **当サービス開始以降、稼働率は 99.995％以上**（2019 年までの実績）
- **最先端のクラウドサービス利用により、ご利用企業様間のインフラ影響も排除**

10 年連続シェア **1** 位

- **国内クラウド型 WAF 市場シェア 10 年連続 No.1**
  （2010 年度から 2019 年度までの実績）

年間 **500** 以上

- **年間 500 以上の脆弱性診断を行っているセキュリティエキスパート企業のノウハウがぎっしり詰まったサービスです**

https://www.scutum.jp
サービス提供： 株式会社セキュアスカイ・テクノロジー
技術提供： 株式会社ビットフォレスト

netforest https://www.netforest.ad.jp/
販売代理店 株式会社ネットフォレスト
〒221-0052 横浜市神奈川区栄町5-1 横浜クリエーションスクエア16階
Tel 045-548-5548／Fax 045-548-5502
Mail nwd-sales@netforest.ad.jp

Scutum クラウド型（SaaS型）WAFサービス 【スキュータム】

クラウド時代の、新しいWebアプリケーションファイアウォール。

Scutum （スキュータム）が防御できる主な攻撃

Scutum は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。
本資料では対応可能な攻撃について簡単にご説明いたします。より詳しい内容は「Scutum」Webサイトにてご確認ください。

対応脆弱性一覧

攻撃区分	攻撃名称
認証	総当り
	パスワードリスト攻撃
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
	CSRF（クロスサイトリクエストフォージェリ）※1
コマンドでの実行	SQL インジェクション
	バッファオーバーフロー
	OS コマンドインジェクション
	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
	リモートファイルインクルージョン
	安全でないデシリアライゼーション（Java/PHP）
情報公開	ディレクトリインデクシング ※1
	情報漏えい
	パストラバーサル
	リソースの位置を推測
	XXE の脆弱性を狙った攻撃
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（OGNL インジェクションなど）
	POODLE 攻撃
	SSL BEAST 攻撃
	HTTP リクエストスマグリング
マルウェア拡散	ドライブバイダウンロード攻撃 ※2（ガンブラーによるウイルス拡散など）
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）
	少数 IP アドレスからの DoS 攻撃（大量正常通信、Slowloris、SYN flood 攻撃など）
	[オプション対応] 多数IPアドレスからのDDoS 攻撃

※ 上記攻撃分類に該当するすべての攻撃を防御するものではありません。
※1 有償カスタマイズによる対応となります。
※2 各種攻撃への防御ロジックを有していますが、各時点での攻撃傾向分析や最新の情報収集により実効性を判断して随時調整しています。

新しい脆弱性への対応

Scutum では新たな脆弱性への対応を重視しています。随時シグネチャ更新やエンジン調整を行い、お客様側では特に意識することなく、最新のセキュリティ対策を維持することが可能です。

▼ 2011 年以降の主要な対応（2021 年 3 月現在）

2020.12 Apache Struts2 の脆弱性を利用した攻撃への対応（S2-061、CVE-2020-17530）
2020.08 Apache Struts2 の脆弱性を利用した攻撃への対応（S2-060、CVE-2019-0233）
2020.05 Apache Tomcat の脆弱性を利用した攻撃への対応 (CVE-2020-9484)
2019.10 PHP の FastCGI Process Manager の脆弱性を狙った攻撃への対応（CVE-2019-11043）
2019.06 Oracle WebLogic Server の脆弱性を狙った攻撃への対応（CVE-2019-2729）
2019.04 Oracle WebLogic Server の脆弱性を狙った攻撃への対応（CVE-2019-2725）
2018.08 Apache Struts2 の脆弱性を利用した攻撃への対応（S2-057、CVE-2018-11776）
2018.08 Ghostscript の -dSAFER オプションの脆弱性への対応
2017.12 OWASP Top10 2017 全項目への対応を確認
2017.09 Apache Struts2 の脆弱性を利用した攻撃への対応（S2-052、CVE-2017-9805）
2017.07 Apache Struts2 の脆弱性を利用した攻撃への対応（S2-048）
2017.03 Apache Struts2 の脆弱性を利用した攻撃への対応（CVE-2017-5638、S2-045、S2-046）
2017.02 WordPress の REST API の脆弱性を利用した攻撃への対応
2016.12 PHPMailer の脆弱性への対応（CVE-2016-10033、CVE-2016-10045）
2016.11 意図しない index_old.php 設置による改ざん影響を無害化
2016.10 Joomla! の脆弱性（CVE-2016-8869、CVE-2016-8870）に対応
2016.07 CGI アプリケーションの脆弱性「httpoxy」を狙った攻撃に対応（CVE-2016-5385 等）
2016.06 Apache Struts 2 の脆弱性（CVE-2016-4438、S2-037）を利用した攻撃に対応
2016.06 Apache Struts 1 の脆弱性（CVE-2016-1181、CVE-2016-1182）を利用した攻撃に対応
2016.04 Apache Struts 2 の脆弱性（CVE-2016-3081、S2-032）を利用した攻撃に対応
2015.04 HTTP.sys の脆弱性（CVE-2015-1635）を狙った攻撃に対応
2015.01 SSL3.0 の脆弱性、通称「POODLE」の攻撃への更なる対応（SSL3.0 有効のまま該当攻撃に対処）
2014.10 SSL3.0 の脆弱性、通称「POODLE」の攻撃を無効化（該当暗号スイート無効化）
2014.09 bash の脆弱性 (CVE-2014-6271、CVE-2014-7169)、通称 ShellShock に対応
2014.06 「SMS 認証追加機能」を正式リリース
2014.04 「キャプチャ認証追加機能」を正式リリース
2014.04 Apache Struts2 の脆弱性 (CVE-2014-0094、-0112、-0113) を狙った攻撃に対応
2013.08 アプリケーション追加開発なしで「二要素認証」を追加できる新機能をβ版提供
2013.07 Apache Struts 2 の脆弱性を利用した攻撃への対応（CVE-2013-2251、S2-016）
2013.06 「パスワードリスト攻撃」を抑制する機能を搭載
2012.01 「hash DoS」脆弱性（CVE-2011-4885 等）を狙った攻撃の検知 / 防御機能を搭載
2011.11 SSL の脆弱性を悪用した「SSL BEAST 攻撃」に対応
2011.08 Apache HTTPD サーバの脆弱性を利用した DoS 攻撃に対応
2011.04 大規模 SQL インジェクション攻撃、通称 LIZAMOON 攻撃への対応を確認

その他、暗号スイート関連の脆弱性が発見された場合など、Scutum を経由した通信が影響を受ける可能性について速やかに検証を行っております。

SQLインジェクション対策への注力

大きな被害をもたらす事が多く発生頻度も高いSQLインジェクションについては、SQLインジェクション専用の検査エンジンを搭載することで、特にきめ細かい対策を実装しています。

https://www.scutum.jp
サービス提供： 株式会社セキュアスカイ・テクノロジー
技術提供： 株式会社ビットフォレスト

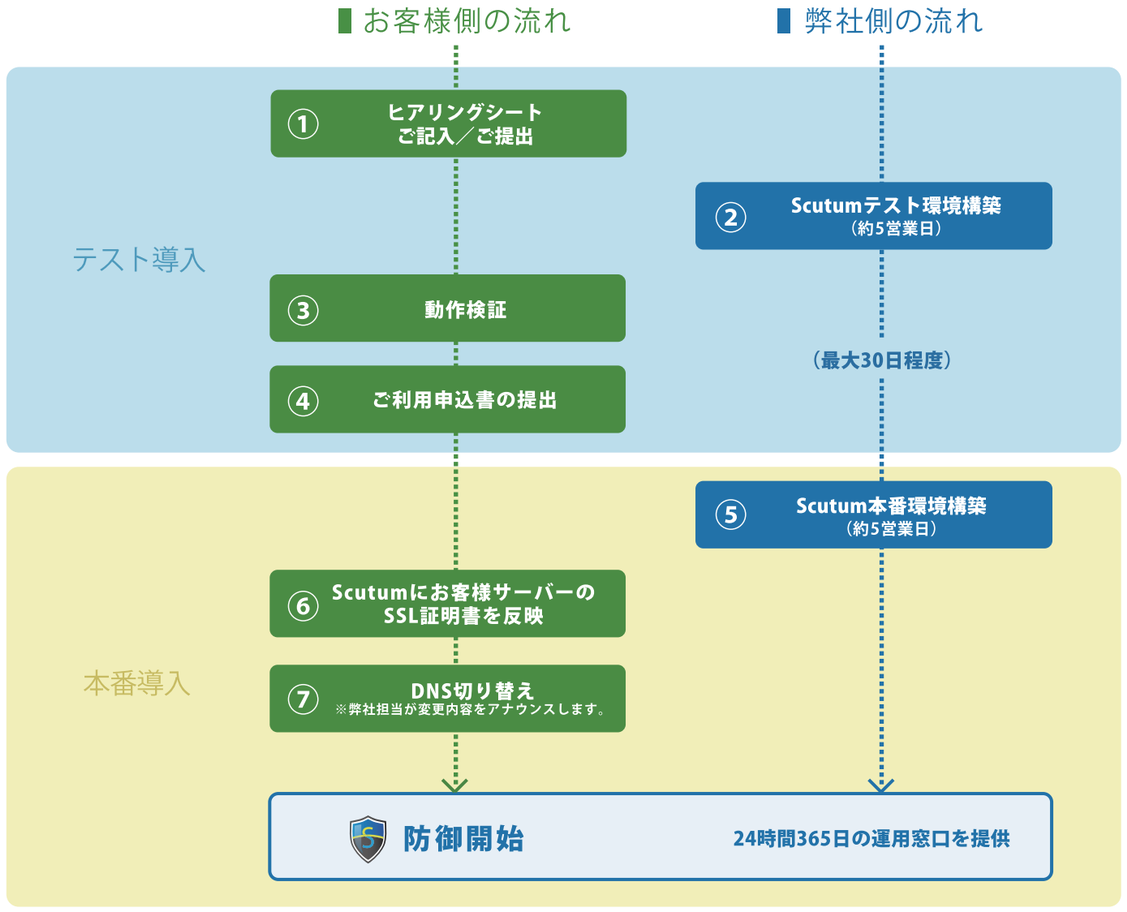
netforest https://www.netforest.ad.jp/
販売代理店 株式会社ネットフォレスト
〒221-0052 横浜市神奈川区栄町5-1 横浜クリエーションスクエア16階
Tel 045-548-5548／Fax 045-548-5502
Mail nwd-sales@netforest.ad.jp

Scutum クラウド型（SaaS型）WAFサービス 【スキュータム】

クラウド時代の、新しいWebアプリケーションファイアウォール。

導入から運用までの流れ

導入までの手順が極めてシンプル。それが Scutum の特長です。



・ヒアリングシートにご記入いただいた情報を元に Scutum テスト環境を構築し、お客様サイトのサービスに影響のない範囲で動作検証を進め、「Scutum」の使用感を確認していただきます。

・動作確認では、疎通確認、遅延検証（特にファイルのアップ / ダウンロード）、誤検知検査等を行って頂けます。その後、営業担当者に導入の旨をご連絡頂き、利用申込書をご提出いただきます。

・Scutum 本番環境の構築後、（SSL/TLS 利用サイトの場合）Scutum 管理画面から SSL 証明書の更新を行っていただきます。

・本番環境の提供の翌月から課金が開始になります。

https://www.scutum.jp
サービス提供： 株式会社セキュアスカイ・テクノロジー
技術提供： 株式会社ビットフォレスト

netforest https://www.netforest.ad.jp/
販売代理店 株式会社ネットフォレスト
〒221-0052 横浜市神奈川区栄町5-1 横浜クリエーションスクエア16階
Tel 045-548-5548／Fax 045-548-5502
Mail nwd-sales@netforest.ad.jp