

WAF (Scutum) ご紹介資料

富士通クラウドテクノロジーズ株式会社(FJCT)



会社名	株式会社セキュアスカイ・テクノロジー
所在地	〒101-0048 東京都千代田区神田司町2-8-1 PMO神田司町2F
事業内容	Webアプリケーションに特化したセキュリティサービス ・脆弱性診断サービス ・セキュリティ教育・支援サービス ・クラウド型WAFサービス ・その他、セキュリティコンサルティング
創業	2006年3月15日（決算月 12月）
従業員数	47名（非常勤を除く）



■ 事例／傾向（Webサービスからの個人情報の窃取）

● チケット販売のWebサイトに不正アクセス

最大約15万5,000件の個人情報が漏えいした可能性
Apache Struts2の脆弱性を悪用

● 登山情報サイトに不正アクセス

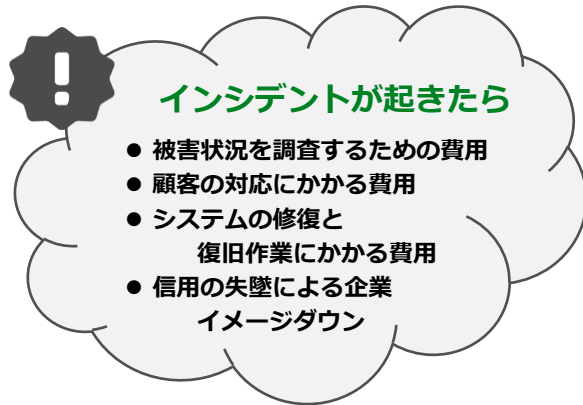
氏名やメールアドレス等、約1,160件の情報漏えい
開発プログラムにSQLインジェクションの脆弱性

● 都税クレジット支払いサイトに不正アクセス

約72万件のクレジットカードに関する情報が漏えいした可能性
不正アクセスは、Webサービスで広く利用されているApache Struts2の脆弱性を悪用

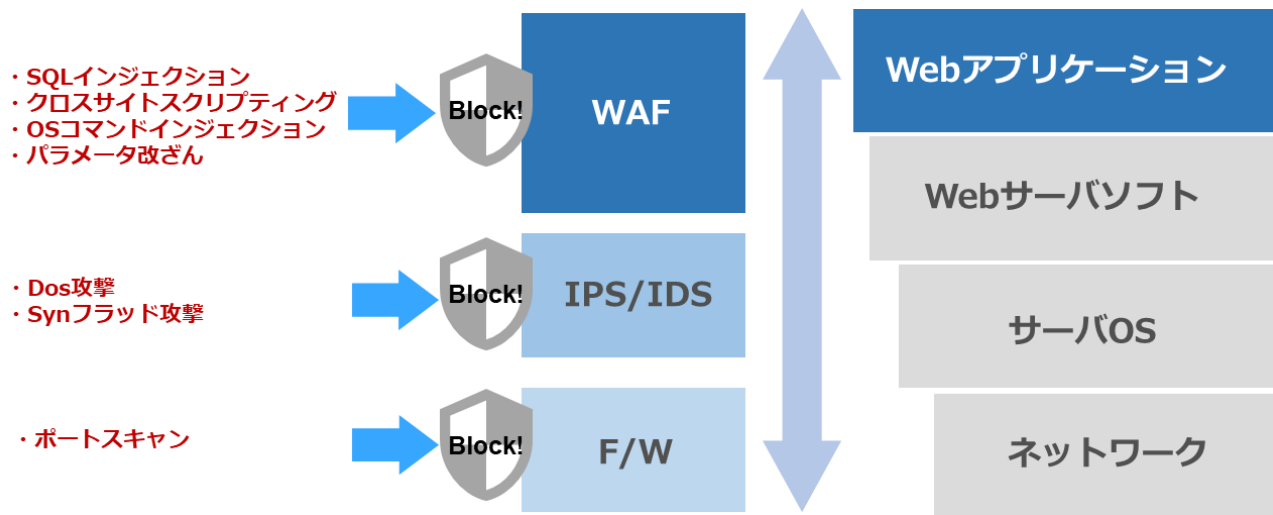
● テレビ局に不正アクセス

Webサイトが不正アクセスを受け、約1,270件の氏名とメールアドレスを流出した可能性
サーバーに存在する脆弱性を悪用され不正アクセスされた可能性



情報セキュリティ10大脅威2018 ～2章 情報セキュリティ10大脅威 組織編～
情報セキュリティ10大脅威2018 ～2章 情報セキュリティ10大脅威 個人編～
独立行政法人情報処理推進機構より

- WAF（Web Application Firewall）とはWebアプリケーションの脆弱性を悪用した攻撃からWebサイトを守るためのセキュリティ対策です。
- ネットワークF/WやIPS/IDSでは対応できない攻撃を検知・遮断することができます。



- 誤検知・過検知のチューニングを定常的にする必要があるため、効果的な防御をするのが難しい

- 社内運用の場合、セキュリティに詳しいエンジニアが必要

- 導入コストが高い

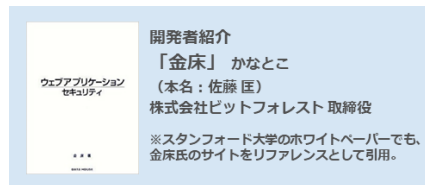
アプライアンスのWAFの導入費用は安くても数百万。また、運用コストも必要。

■ 圧倒的な防御性能

データサイエンス技術とシステム実装、運用技術の高度な融合により、誤検知が少なく新たな攻撃にも対応しやすい、最先端のWAFエンジン（ベイジアンネットワーク技術を活用した人工知能）を搭載しました。

■ WEBセキュリティの専門企業が開発・運用

100社以上・年間500サイト以上の脆弱性診断実績から得たノウハウを活用し、効果的な防御効果を実現します。



■ 純国産

技術開発者が日本人であることから、様々なトラブルへの迅速な対応が可能なほか、マルチバイト（日本語等）特有の特性にも柔軟に対応しています。

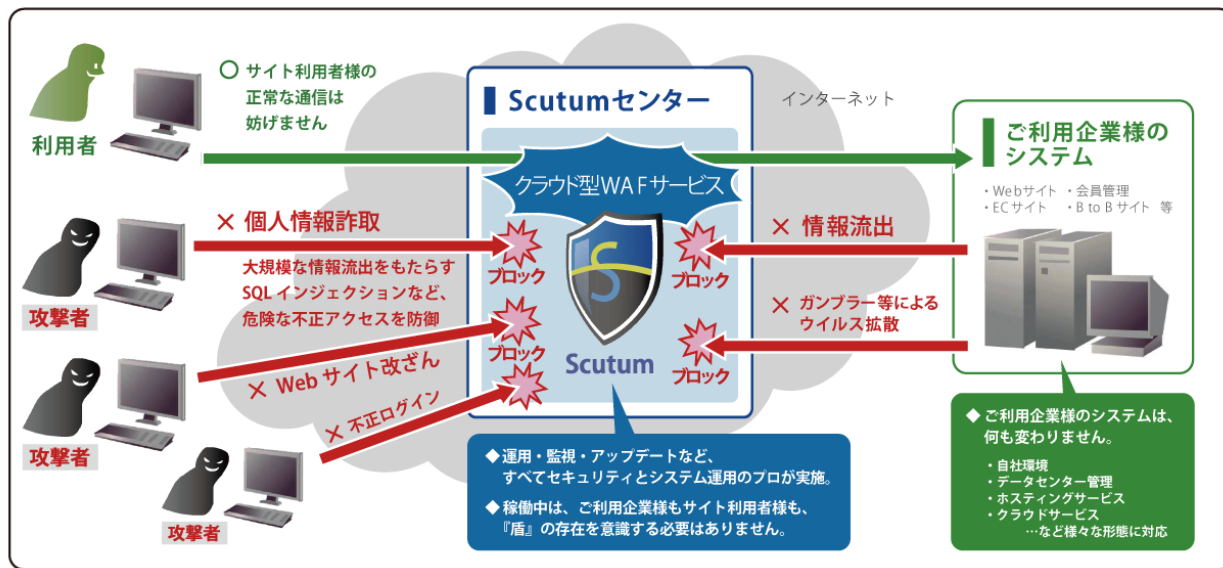
■ 簡単な導入・おまかせ運用

WAFサービスの運用は全てScutum側で実施します。専門のセキュリティ技術者を置く必要はありません。

■ 最短1週間、お客様の環境に合わせた価格で導入可能

※初期費用やプランごとで異なるため、価格詳細はサービスページをご確認ください。

- Scutumは、エンドユーザーからお客様サイトへの通信をDNS変更によりそのままScutumセンターで中継し、その過程で不正な通信を監視・遮断します。



- Webアプリケーションの脆弱性に対する主要な攻撃をカバーしています。

	攻撃名称
認証	総当たり
	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) ※有償カスタマイズとなります。
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
情報公開	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
	リソースの位置を推測
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
	SSL BEAST攻撃
マルウェア拡散	ドライブバイダウンロード攻撃 (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)

脆弱性への対応（OWASP Top10）

- OWASPTop10は、世界中のセキュリティ専門企業や個人の協力を得て10万以上のWebアプリケーションやAPIから集めた脆弱性について調査した結果を基にまとめたものです。
- Scutumは、SQLインジェクションやクロスサイトスクリプティング、OWASPの「Webアプリケーションで最もセキュリティリスクが高いと発表されている全項目」をカバーしています。

OWASP Top 10 - 2017
A1 : 2017-インジェクション
A2 : 2017-認証の不備
A3 : 2017-機微な情報の露出
A4 : 2017-XML 外部エンティティ参照 (XXE)
A5 : 2017-アクセス制御の不備
A6 : 2017-不適切なセキュリティ設定
A7 : 2017-クロスサイトスクリプティング (XSS)
A8 : 2017-安全でないデシリアライゼーション
A9 : 2017-既知の脆弱性のあるコンポーネントの使用
A10 : 2017-不十分なロギングとモニタリング

【OWASP TOP10 2017より】

OWASPとはWebをはじめとするソフトウェアのセキュリティ環境の現状、またセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的としたプロフェッショナルの集まる、オープンソース・ソフトウェアコミュニティです。

- 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。
- 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実現することが可能です。

最新の脆弱性対策を常に反映 ゼロデイ攻撃にも対応の実績



Struts2などを中心にインタビューしていただいた記事が
日経BP社「すべてわかるセキュリティ大全2018」

『知るほどに怖くなる！？Struts2脆弱性のメカニズム』
に掲載されています。

<http://itpro.nikkeibp.co.jp/atcl/column/14/346926/051100966/>

「WAF Tech Blog 技術者ブログ」もご覧ください。

https://www.scutum.jp/information/waf_tech_blog/index.html

脆弱性への対応一覧例

脆弱性	注意喚起	Scutum対応
Apache Struts2 の脆弱性を利用した攻撃への対応 (S2-057、CVE-2018-11776)	2020年8月14日 JPCERT/CC	2020年8月14日 ※シグネチャ適用
Ghostscriptの -dSAFER オプションの脆弱性への対応	2020年5月21日 JPCERT/CC	2020年5月21日 ※既存の防御機能により、公開前から防御できていることを確認
Apache Struts2 の脆弱性 (S2-052、CVE-2017-9805) について	2019年6月19日 JPCERT/CC	2020年6月20日 ※一部の特殊な攻撃パターンについても防御可能な像帯に更新。
Apache Struts2 の脆弱性を利用した攻撃への対応 (CVE-2017-9791、S2-048)	2018年8月23日 JPCERT/CC	2018年8月23日 ※OGNLインジェクション防御機能により、公開前から防御できていることを確認
Apache Struts2 の脆弱性を利用した攻撃への対応 (追加報告) (S2-046)	2018年8月22日 JPCERT/CC	2018年8月23日 ※シグネチャ適用
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年9月6日 JPCERT/CC	2017年9月6日 ※シグネチャ適用
WordPress の REST APIの脆弱性を利用した攻撃への対応	2017年7月10日 JPCERT/CC	影響なし ※Struts2のOGNLインジェクションを幅広く防止する機能を実装
PHPMailerの脆弱性への対応 (CVE-2016-10033、CVE-2016-10045)	2017年3月21日 JPCERT/CC	2017年3月21日 ※シグネチャ適用
意図しない「index_old.php」設置による改ざん	2017年3月9日 JPCERT/CC	影響なし ※既存のシグネチャで防御できていることを確認
Apache Struts2 の脆弱性 (CVE-2016-4438、S2-037)	2017年2月6日 JPCERT/CC	2017年2月6日 ※シグネチャ適用
Apache Struts2 の脆弱性 (CVE-2016-3081、S2-032)	2016年12月28日 JPCERT/CC	2016年12月28日 ※シグネチャ適用
HTTP.sysの脆弱性 (CVE-2015-1635)	2016年11月14日 JPCERT/CC	2016年11月17日 ※レスポンスをチェックし、無害化
SSL3.0の脆弱性 (通称: POODLE) (CVE-2014-3566)	2016年6月20日 IPA	2016年6月16日 ※シグネチャ適用
bashの脆弱性 (CVE-2014-6271 等)	2016年4月28日 IPA	2016年4月27日 ※シグネチャ適用
OpenSSL 1.0.1に含まれる脆弱性 (通称: Heartbleed)(CVE-2014-0160)	2015年4月16日 IPA	2015年4月15日 ※攻撃コードを参考にし、シグネチャ適用

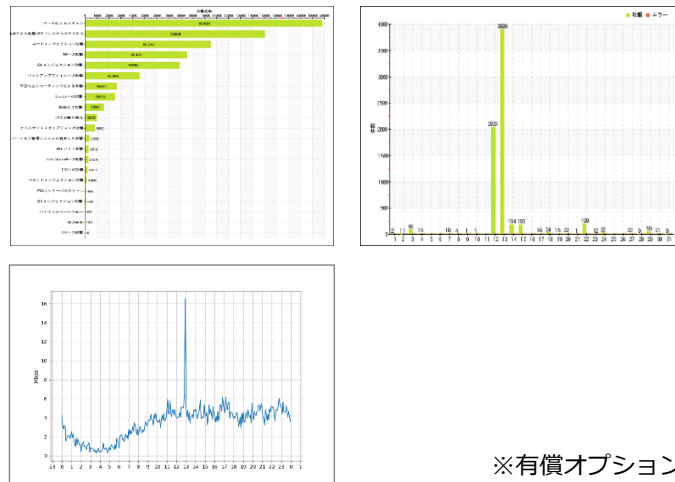
- 運用はおまかせですが、必要に応じて管理画面で攻撃情報を確認したり、月次レポートでScutum全体で観測しているサイバー攻撃の動向を知ることができます。

管理画面



Scutumの管理機能は、ご契約者様専用ページ内の個別管理画面から、Webブラウザ経由で手軽かつ安全にご利用いただけます。

月次レポート



※有償オプション

■ Scutumは、2009年のサービス開始以来、金融機関や公的機関を含む多数のWebサイトに幅広く導入いただいております。



■ 防御対象サイトのFQDNとSSL利用の有無

【例】 www.scutum.jp	SSL利用	無
secure.scutum.jp	SSL利用	有

■ FQDN数

【例】 http://www.example.com/ と http://sub.example.com/ 2FQDN
http://xxx/ xxxの部分が同じであれば1FQDN

■ トラフィック情報

- ・ 防御対象サイトのトラフィックやPV実績情報などをお知らせください。
- ・ 新規サイトの場合は想定されるページビュー数（PV）をお知らせください。

【例】 ピーク時〇Mbps程度・日別PV〇万PV程度・月間PV〇万PV程度

※PV情報をいただければ、弊社にて試算することも可能です。

■ WAF (Scutum)

■ 特徴

【かんたん導入】

サーバー側作業は不要で、通常1週間あれば稼働開始可能です。
ご利用企業様では、DNS変更とSSL証明書情報、秘密鍵の受け渡しのみで導入準備は完了です。

【おまかせ運用】

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、お客様が何もしなくても防御能力が進化。
サイト運営者は日々の管理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。

【個別の管理画面で管理】

管理機能は、ご契約者様専用ページ内の個別管理画面から、ブラウザー経由で手軽かつセキュアにご利用いただけます。

■ 仕様

1、主要機能

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、該当通信を遮断する機能
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、該当通信を記録する機能（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、閲覧できる機能
ソフトウェア更新機能	Scutumの防御機能などを向上させるため、ソフトウェアを更新する機能
シグネチャ更新機能	防御効果の向上を図るため、不正な通信パターンを随時最新の状態に更新する機能
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する機能
レポート機能	下記の内容を管理画面（ブラウザー利用）上で報告する機能 ・統計機能（攻撃元、攻撃種別、アクション） ・攻撃元、攻撃種別の上位集計など
IPアドレス拒否機能	特定のIPアドレスからの通信を拒否する機能

SSL通信機能	暗号化された通信においても解読し、防御する機能
API	Scutum管理画面で利用できる機能の一部をAPIにて利用可能 ※ご利用にあたってはScutum管理画面より、APIキーを発行する必要があります

2、オプション機能

月次報告書	攻撃の傾向を月次でご報告します。
キャプチャ認証追加機能	任意の箇所にキャプチャ認証を導入できます。

3、防御できる主な攻撃

攻撃区分	攻撃名称
認証	・総当たり
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）※別途、設定費用が発生します。
コマンドでの実行	・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
情報公開	・ディレクトリラインデクシング ・情報漏洩 ・パス トラバースル ・リソースの位置を推測
マルウェア対策	・ドライブバイダウンロード攻撃（ガンブラーによるウイルス拡散など） ・その他

■ WAF (Scutum)

■ 特徴

低トラフィックプラン

【基本ホスト数：1FQD (SSL/TSL利用可)、ホスト追加：不可】

ピーク時トラフィックの目安	初期費用 (税込)	月額費用 (税込)
～500kbps	107,800円	32,780円/月
～5Mbps		65,780円/月
～10Mbps		140,800円/月

高トラフィックプラン

【基本ホスト数：1FQDN (SSL/TSL利用可)、ホスト追加：上限なしで可能 (有償) ※1】

ピーク時トラフィックの目安	初期費用 (税込)	月額費用 (税込)
～50Mbps	217,800円 + 10FQDNを超えた 1FQDNあたり 21,780円	162,800円/月
～100Mbps		217,800円/月
～200Mbps		327,800円/月
200Mbps～		327,800円 + 200Mbpsを超えた 100Mbps毎に110,000円

※詳細な費用や注意事項、料金例、制限事項につきましては、サービスページの最新情報をご確認ください。

※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、1FQDN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。

■ ご利用方法



約10営業日

1. 申し込み

本サービスのお申し込み、設定変更、解除については、下記フォームよりお申し込みください。

※ニフクラIDとパスワードの入力が必要です。

※お申し込み時にログインされたニフクラIDでのご登録となります。

■お申込みフォーム：https://inquiry.nifcloud.com/webeg/pub/cloud/waf_auth

2. 事前準備

事前準備として以下の資料をお客様からご提出いただきます。

- ・サイト情報を記入したヒアリングシート

3. 環境設定

提出いただいた資料をもとに、センターにてお客様環境の設定を行います。

なお、環境設定からサービス開始まで10営業日程度かかります。

4. サービス開始

お客様環境にてDNSを変更していただき、Scutum経由での通信を開始となります。

5. モニタリング・検証

1か月間モニタリングを行うことで正常な通信を止めていないか検証を行います。必要であれば設定変更を行います。

■ 正式利用の前に、トライアル利用を行うことができます。

- 期間：1か月
- 正式利用への移行：不可

※トライアル環境をそのまま正式環境として利用することができません。

※正式利用が決定した場合は、新たに環境を構築していただく必要がありますので、あらかじめご了承ください。

- 制限事項：
 - HOSTSファイルでの切替で実施
 - 高トラフィックプランは選択不可
 - 1FQDNのみ

トライアルのお申し込みについては担当営業へお気軽にご相談ください。

■ お気軽にご相談ください

契約／お申し込みに関する内容、サービス概要、導入にあたっての疑問点や、お見積りの依頼など、お電話又はサイトでのお問い合わせをお待ちしております。

ニフクラ導入相談窓口

サイト <https://pfs.nifcloud.com/inquiry/>

電話 0120-22-1200

受付時間：平日9:00～17:45
※携帯電話・PHSからのご利用可能

Thank you

