

2011 年 4 月 19 日  
株式会社セキュアスカイ・テクノロジー  
株式会社ビットフォレスト

**国内の Web サイト 99%以上※1に対応！**

**セキュリティをトレードオフにせずクラウドを利用できる WAF ソリューション**

**被害報告増加中の大規模 SQL インジェクション攻撃(LIZAMOON)にも対応**

**セキュアスカイ・テクノロジー、  
SaaS 型ウェブアプリケーション・ファイアウォール(WAF)サービス  
「[Scutum](http://www.scutum.jp/index.html)」(<http://www.scutum.jp/index.html>)の新サービスを発表**

ウェブアプリケーションセキュリティのスペシャリストである、株式会社セキュアスカイ・テクノロジー(本社:東京都文京区、代表取締役社長:乗口雅充、以下 SST)と株式会社ビットフォレスト(本社:東京都新宿区、代表取締役:高尾都季一、以下ビットフォレスト)は、SaaS(Software as a Service / 必要な機能を必要な分だけサービスとして利用できるソフトウェア)型ウェブアプリケーション・ファイアウォール(WAF)サービス「Scutum(スキュータム)」の処理能力を改善し、対応トラフィックを従来の 10Mbps から 100Mbps 以上へと、大幅に拡充した新サービスの追加を発表しました。4 月から報告されている大規模 SQL インジェクション攻撃(LIZAMOON)へも対応しております。

### **<新サービスの特長の概略>**

- 今まで「Scutum」のメニューでは対応できなかった「10Mbps～100Mbps 以上」への対応を拡充し、国内 Web サイトの 99%以上※1 が利用できるようになりました。
- 「セキュリティの確保」と「クラウドサービスを利用・クラウドサービスへの移行」を両立できるため、クラウドへの移行にともなうセキュリティの低下が原因となる「セキュリティ意識が高い企業ほど、クラウド化に踏み切れない」という問題を解決します。
- 従来一般的だった「アプライアンス型 WAF」と比較して、コストをおよそ 50%減らせます(5年間利用の場合)。

※1 国内主要サイトのアクセス数推定をもとに SST が独自に算出。トラフィック量以外の理由による導入適否は考慮しておりません。

## ＜大規模 SQL インジェクション攻撃(LIZAMOON)への対応＞

- 現在報告されている大規模 SQL インジェクション攻撃(通称 LIZAMOON)は、「Scutum」で防御可能です。
- 各機関から報告されている攻撃内容は、「Scutum」が以前から標準で提供しているシグネチャですべて防御可能なものでした。
- LIZAMOONと思われる攻撃リクエストは「Scutum」でも観測されましたが、すべてのリクエストはブロックされていました。

### 「Scutum」とは？

2009 年 6 月のサービス開始から約 22 ヶ月が経過し、累計利用サイトも約 120 を超える世界初の SaaS 型 WAF「Scutum」。非常に高い信頼性(2010 年 12 月までの 18 ヶ月間の平均稼働率は約 99.997%※)と低価格、低運用負荷によってご利用ユーザー様からご好評をいただいております。このたび、特にご要望が多かった処理能力を増強した新サービスを提供いたします。

今までのサービスでは、ピーク時のトラフィックが回線速度として約 10Mbps のウェブサイトがご利用対象だったため、主に中小規模のウェブサイトでご利用いただいていた WAF「Scutum」ですが、約 1 年間の研究開発と実機検証の結果、WAF サービスの処理能力を大幅に増強することに成功しました。これにより、従来のアプライアンス型 WAF と遜色ない処理能力を実現できます。

昨今ではウェブサイトの競争力向上のため、クラウドサービスの利用がビジネス上必須になっていますが、従来のアプライアンス型 WAF を利用しているウェブサイトの場合、クラウド上でアプライアンス型 WAF を利用することができないため、クラウド利用がセキュリティレベルの低下と直結してしまい、セキュリティ意識が高い企業ほどクラウド利用を推進できない問題がありました。SST にも、そのような相談を多数いただいております。

特に EC サイトでは情報漏洩事件の多発によりユーザーのセキュリティ意識が急速に高まっています。IMJ モバイルが 2010 年 12 月 13 日に発表した『EC サイトに関する利用実態調査』(※2)によれば、EC サイトを利用する際のポイントとして「価格」「送料」の次に「安心・信頼」が挙げられており、ウェブサイトの安全対策はビジネスを成功させるための最優先事項になっています。

※2 株式会社 IMJ モバイル『EC サイトに関する利用実態調査』

<http://www.imjmobile.co.jp/news/file/pdf/report/20101213.pdf>

WAF「Scutum」の新サービスでは、「セキュリティの確保」と「クラウドサービスを利用・クラウドサービスへの移行」を両立可能にし、さらなるビジネスの発展をアシストします。また、従来の一般的なプライアンス型 WAF と比較しておよそ50%減のコストで利用可能です(5年間利用の場合)。

SST とビットフォレストは今後もこのようなセキュリティ上の問題を解決し、お客さまのインターネットビジネスの成功をサポートいたします。

### 新サービスについて

ピーク時トラフィックの目安	初期費用	月額費用	適用可能ホスト数 (FQDN数)
～500kbps	¥98,000	¥29,800	1
500kbps～5Mbps		¥59,800	
5Mbps～10Mbps		¥128,000	
10Mbps～50Mbps	¥198,000	¥148,000	10 (※)
50Mbps～100Mbps		¥198,000	
100Mbps 以上	個別お見積		個別ご提案

- (※) 2FQDN 以上で SSL をご利用になる場合はオプション料金が必要です。
- ・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。
  - ・上記金額は税別です。別途消費税が加算されます。

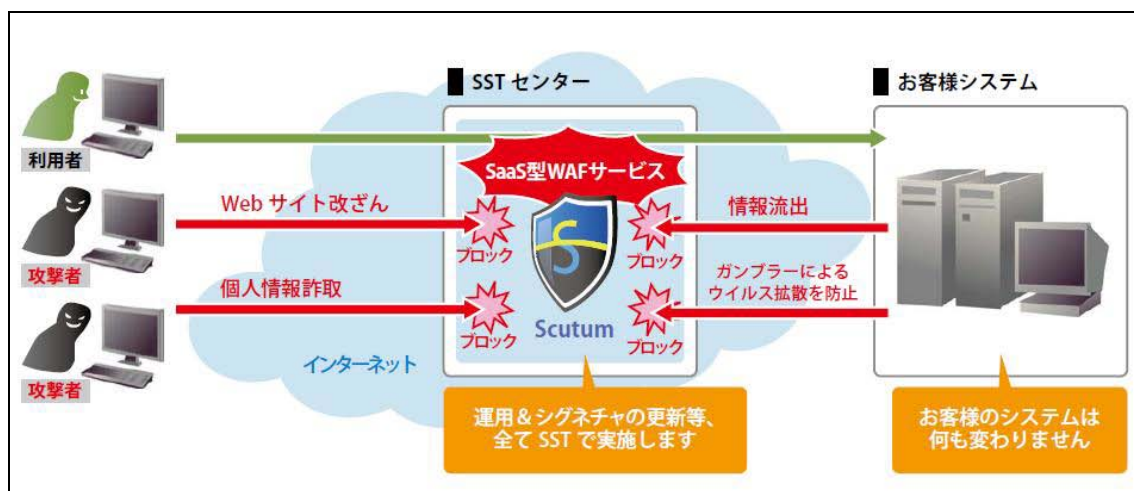
オプション内容	月額費用
SSL利用ホスト追加	1ホスト (1FQDN) 追加につき ¥10,000
月次報告書	1ホスト (1FQDN) につき ¥20,000

- ・上記金額は税別です。別途消費税が加算されます。

## WAF について

インターネットを活用したビジネスを推進するにあたり、ウェブサイトで個人情報を取り扱うことは必要不可欠となっています。個人情報がウェブサイトから漏洩することを防止するためには、これら個人情報をターゲットとした攻撃への有効な対策を講じることが重要です。個人情報を標的とした攻撃は、OS の脆弱性等をターゲットとした攻撃から、ウェブサイト上のアプリケーションをターゲットにした攻撃へと大きくシフトしています。こうした攻撃に対する最も有効な対策のひとつに、WAF が挙げられます。WAF は OSI 参照モデルのアプリケーション層に特化したファイアウォールで、SQL インジェクションなどアプリケーションの脆弱性を狙った攻撃に極めて有効な対策です。

## Scutum について



これまでの WAF は、ハードウェア型・ソフトウェア型が主流で、専任の担当者が必要であるうえ、管理コストの負担が大きいと、普及が進んでいないのが実情でした。「Scutum」は SaaS (Software as a Service / 必要な機能を必要な分だけサービスとして利用できるソフトウェア) 型で、導入の初期コストが大きく軽減され、稼働にあたっての専任の担当者も不要なため、比較的容易に導入が可能です。また「Scutum」は、最近大きな話題を集めているガンプラー (Gumbler) 攻撃への対策にも効果を発揮します。

**【株式会社セキュアスカイ・テクノロジーについて】**

Scutum サービス提供元

社名：株式会社セキュアスカイ・テクノロジー

本社所在地：東京都文京区湯島 2-4-3 ソフィアお茶の水 3F

設立：2006 年 3 月

代表者：代表取締役 乗口 雅充

事業内容：Web アプリケーションのセキュリティ診断、コンサルティング、教育

URL：<http://www.securesky-tech.com/>

**【株式会社ビットフォレストについて】**

Scutum 共同開発(技術提供)

社名：株式会社ビットフォレスト

本社所在地：東京都新宿区信濃町 3 番地 S.court 2F

設立：2002 年 2 月

代表者：代表取締役 高尾 都季一

事業内容:Web サイト構築、システム開発、企画コンサルティング

URL：<http://www.bitforest.jp/>

＜製品についてのお問い合わせ＞

株式会社セキュアスカイ・テクノロジー

Scutum 推進室:大木 [scutum-info@securesky-tech.com](mailto:scutum-info@securesky-tech.com)

＜報道機関からのお問い合わせ＞

PR 担当:常山・大木 [info@scutum.jp](mailto:info@scutum.jp)

※取材等はお気軽にご連絡ください