第26回スクエアFreeセミナー：テーマ1

SaaS型Webアプリケーション ファイヤーウォール（WAF）Scutum

～Webサイトへの攻撃は通常のファイヤーウォールでは防げません～

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 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！

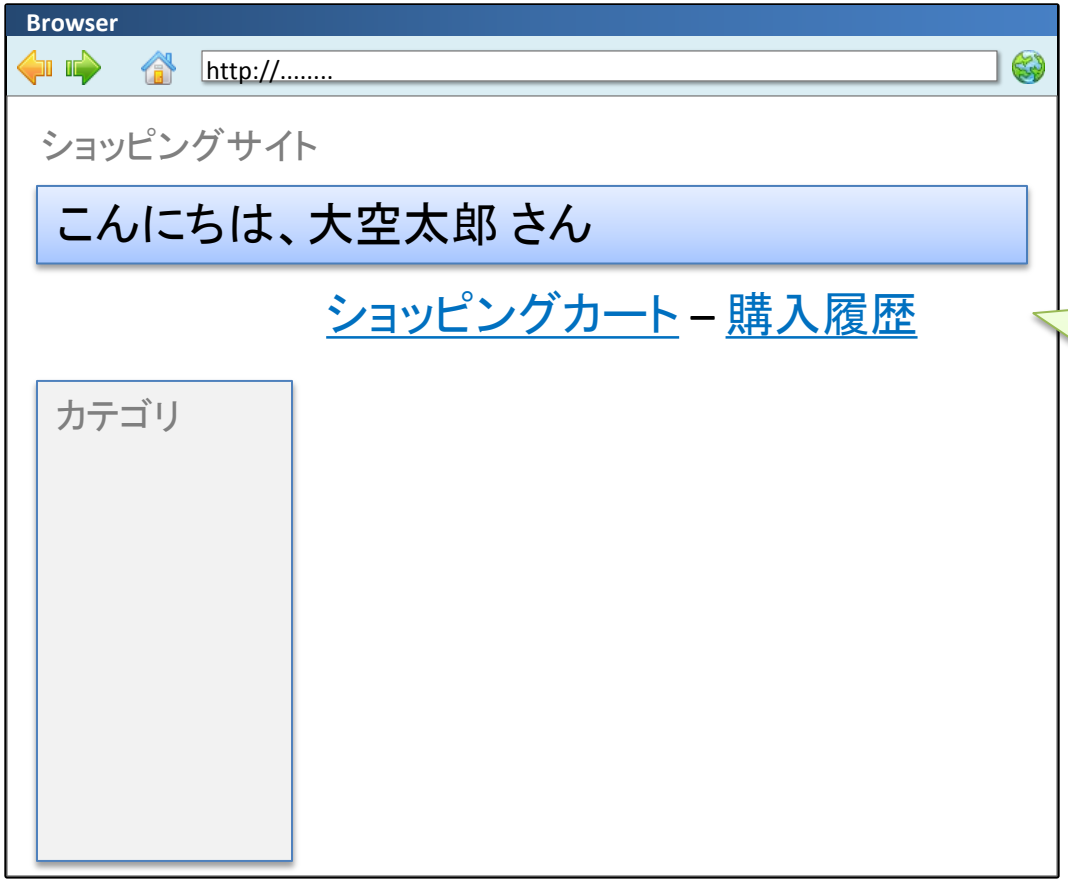
Internet &
Communication
Innovator

はじめに
Webアプリケーションの脆弱性基礎講座。
これがあると超やばいっ！
SQLインジェクション

SQLインジェクションとは

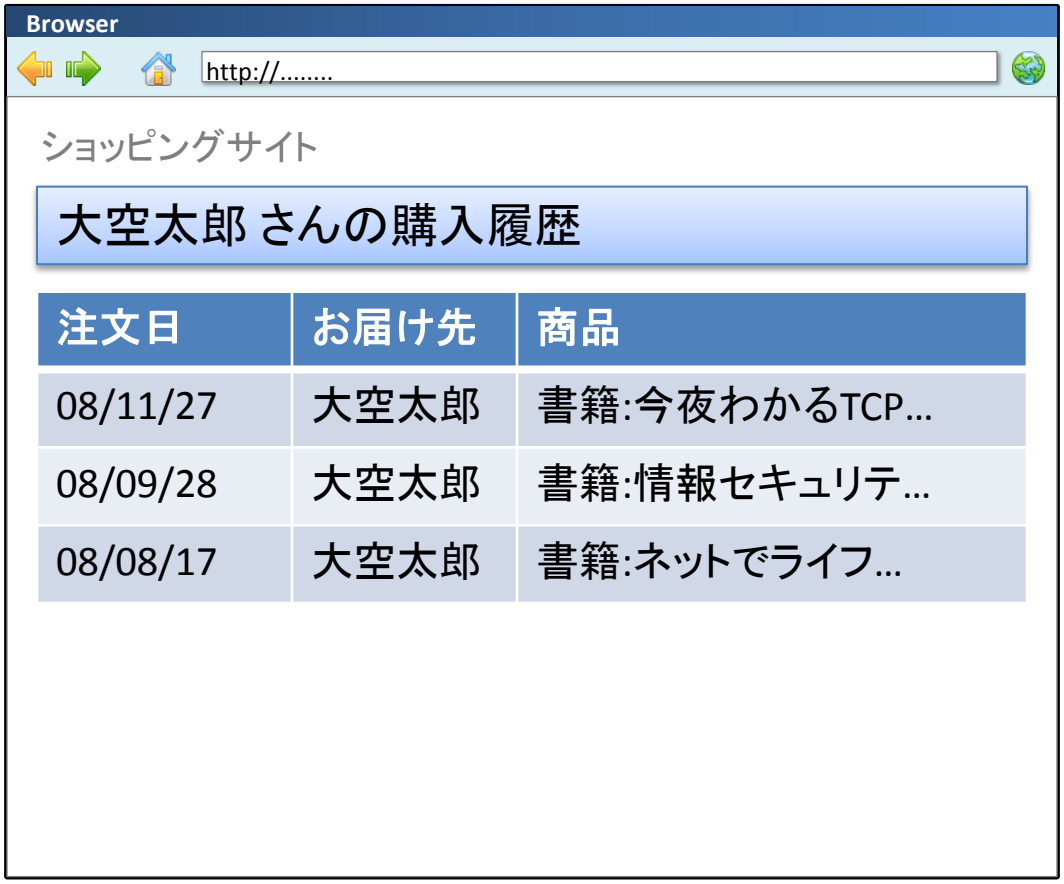
- 不正な入力により任意のSQL文を実行させる
  - Webコンテンツやユーザー入力値を格納するデータベースに対する攻撃
  - 想定される影響
    - 顧客情報の改ざん・流出
    - コンテンツの改ざん
    - 認証の回避
    - 認証情報の書き換え
    - テーブル破壊など

（例）通常の動作

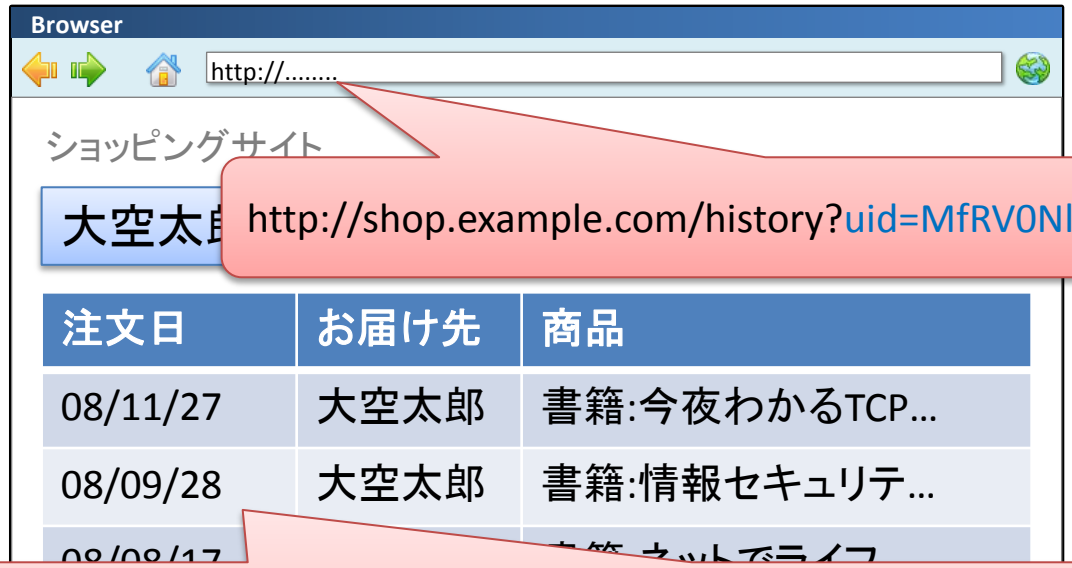


ログイン中のユーザーの
購入履歴が表示される
機能

（例）通常の動作



内部の処理



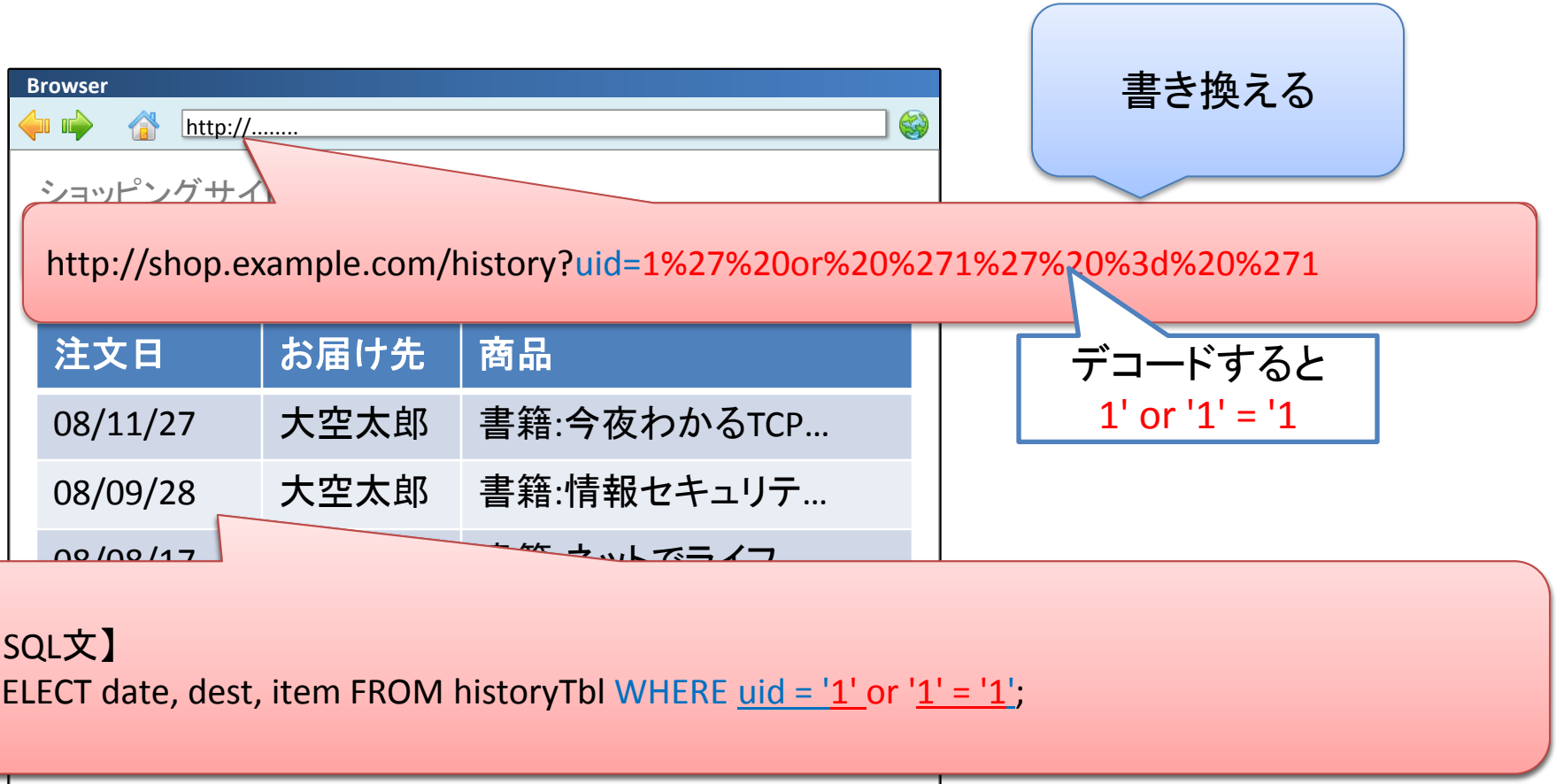
http://shop.example.com/history?uid=MfRV0Nl5VlK3vYy0

MfRV0Nl5VlK3vYy0は、
大空太郎さんのuid

【SQL文】
SELECT date, dest, item FROM historyTbl WHERE uid = 'MfRV0Nl5VlK3vYy0';

データベース historyTblから、uid= 'MfRV0Nl5VlK3vYy0' が含まれる行のdate, dest, itemのデータを表示しなさい

SQLインジェクション



データベース historyTblから、uid='1'、または条件'1'='1' が成り立つ行の
date, dest, itemのデータを表示しなさい

内部の処理

historyTbl

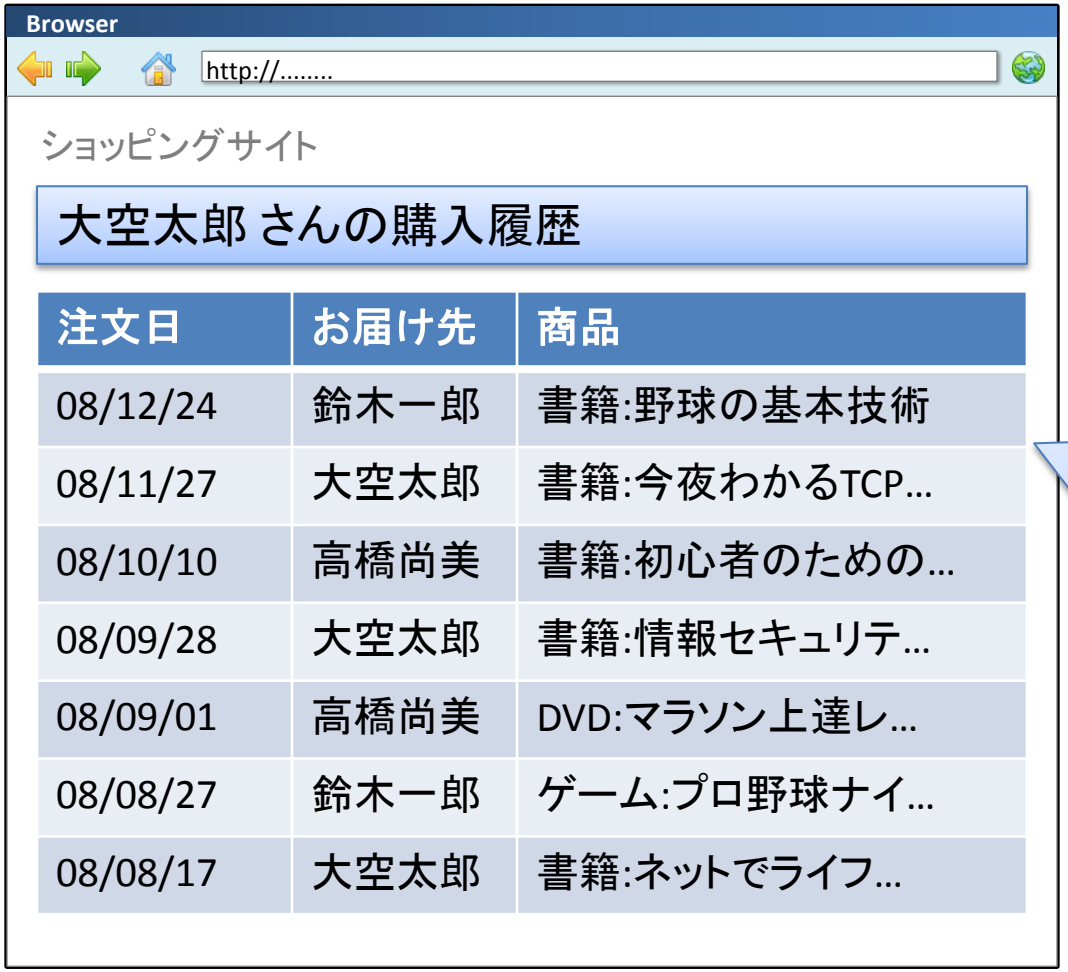
uid	date	dest	item
LfhllUTwqFZaa6Sm	08/12/24	鈴木一郎	書籍:野球の基本技術
MfRV0Nl5VlK3vYy0	08/11/27	大空太郎	書籍:今夜わかるTCP…
Hbgcfus2leCRGl1R	08/10/10	高橋尚美	書籍:初心者のためのマラソン
MfRV0Nl5VlK3vYy0	08/09/28	大空太郎	書籍:情報セキュリテ…
Hbgcfus2leCRGl1R	08/09/01	高橋尚美	DVD:マラソン上達レッスン
LfhllUTwqFZaa6Sm	08/08/27	鈴木一郎	
MfRV0Nl5VlK3vYy0	08/08/17	大空太郎	

「条件'1'='1'」は常に
どの行でも成り立つ

つまり、

データベース historyTblから、uid='1'、または全ての行の
date, dest, itemのデータを表示しなさい

SQLインジェクション



本来ならば表示されない
他のユーザーの購入履歴
も表示されてしまう

SQLインジェクションの対策

ユーザから入力された値を元にして、データベースへの問い合わせを行なう場合、データベースへの問い合わせを行なう段階で、**入力された値の中に不正な文字列が含まれていないかをチェックし**、その結果としてエラー処理や無害な文字列に変換するなどの処理を行なってください。

また、パラメータの種類を考えて特定の文字しか受け付けない（記号は受け付けない）ようにしておくことでより安全なものとなります。

セキュリティ先進企業に聞く
セキュリティ対策の考え方

ISMSの罠にはまるな！

セキュリティ担当の悩みごと

標的型攻撃や遠隔ウイルスとか怖いな

ハッカーのアノニマスってうちにも攻撃するのかな

中国との関係悪化で攻撃増えてると聞いてるし

クラウドサービスを活用したいけどセキュリティ大丈夫なのかな

不正アクセスによる情報漏えい事件増えてるな

うちのWebサイトを開発してる会社はセキュリティの知識あるのかな？

国もサイバー攻撃に備えて部隊作るしやばいのかな

モバイルパソコンのHDD暗号化くらい必要かな？

ISMSやプライバシーマークの審査員から、内部セキュリティについて情報管理などいっぱやる事あるな

PCのウイルス、マルウェア対策しないとな

入退室装置もそろそろ導入しないと

そもそもセキュリティ専任じゃないし・・・、メインの仕事あるし・・・

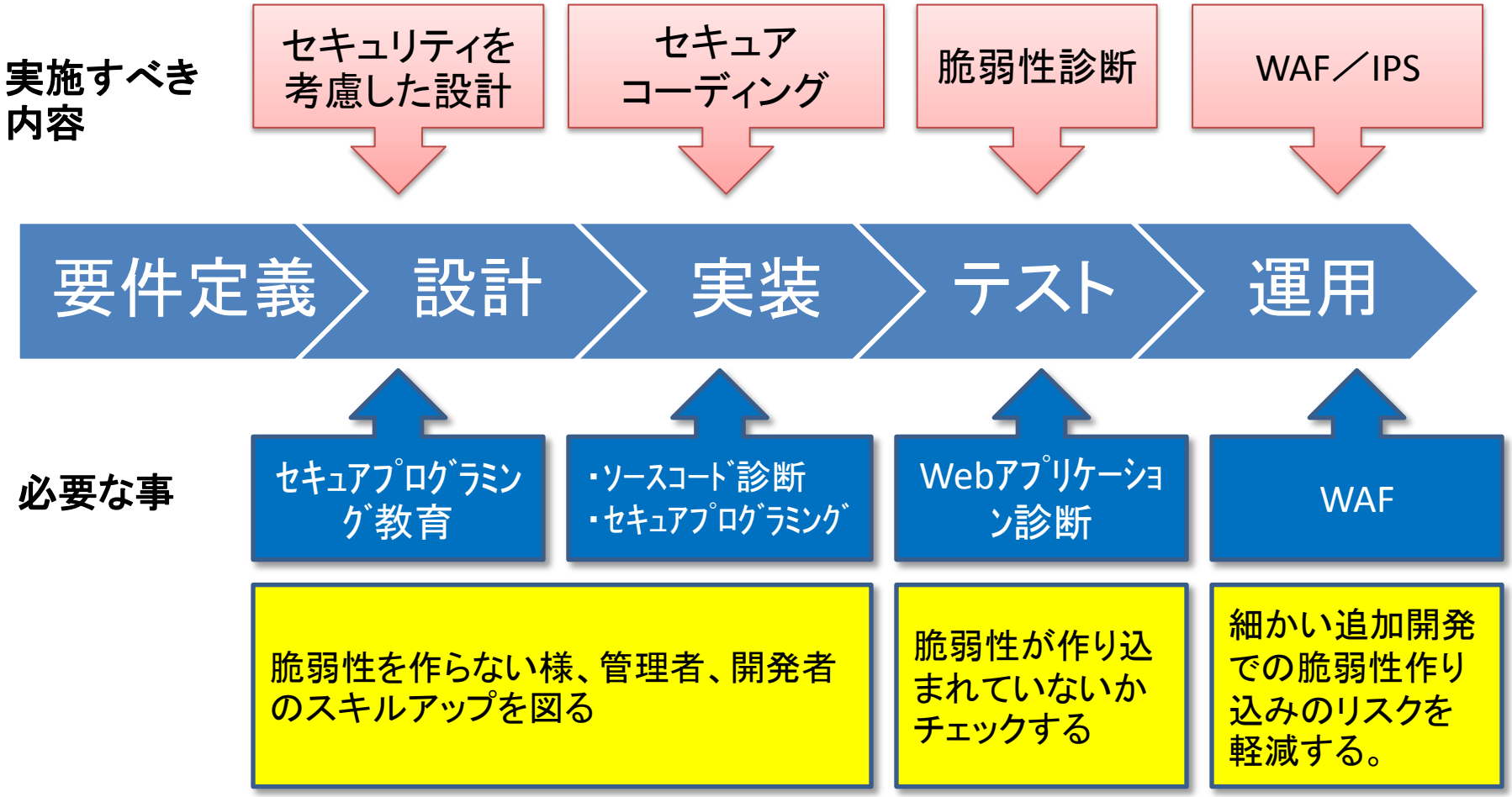
顧客情報DB大丈夫かな、持ち出しとか不安

Webサイト運営部署にセキュリティルール守るように言ったら嫌われそう・・・

セキュリティの専任知識ないし・・・

Webサイトのセキュリティ対策

- それぞれのフェーズですべき対策

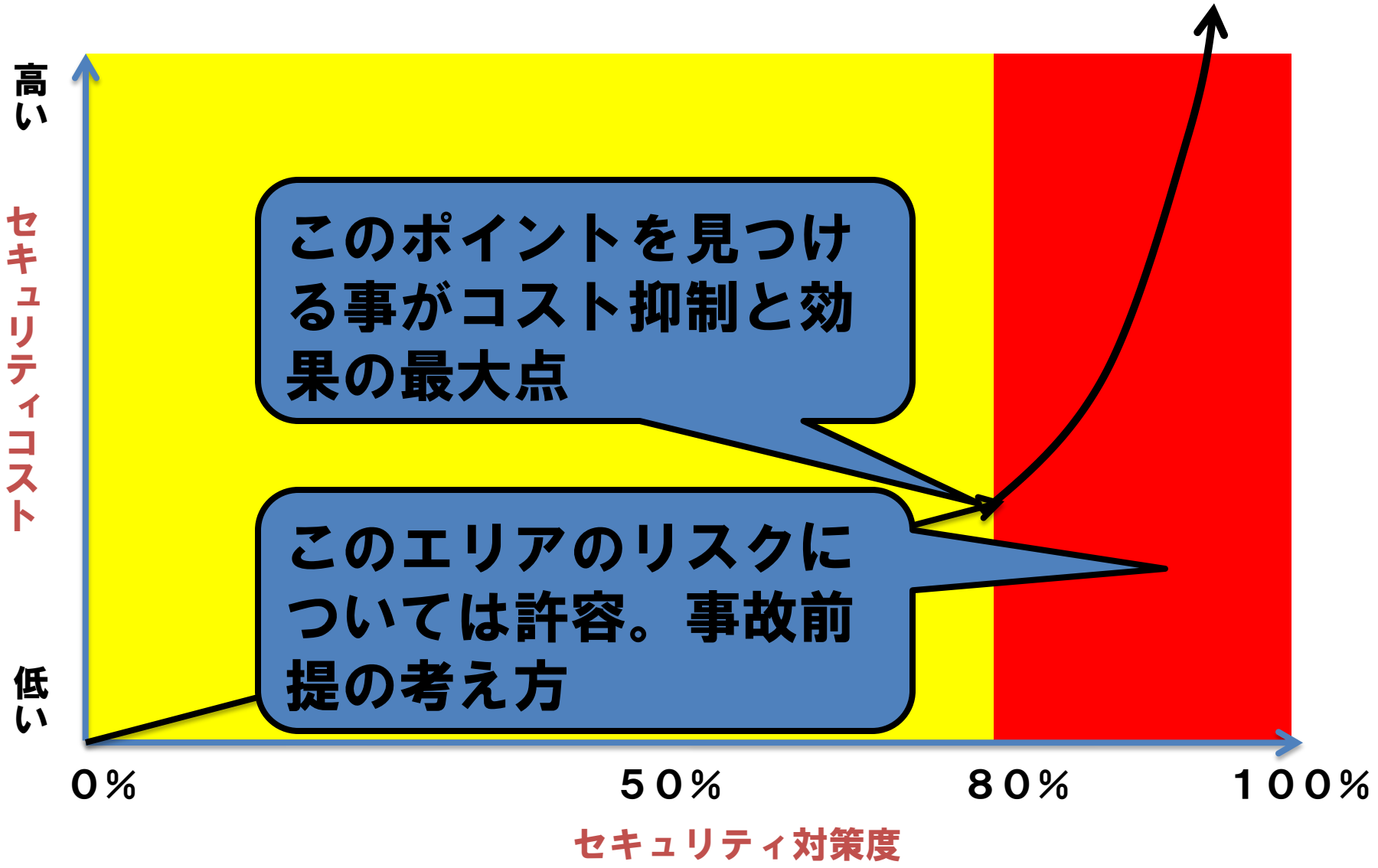


先進企業からのアドバイス

◆セキュリティ対策を行うパワー配分は、
イントラセキュリティ：公開Webセキュリティ＝１：９
で考える

- インターネットWebサイトで顧客情報や重要情報を持つWebサイトを最優先で考えなさい。
- イントラセキュリティは、PC対策と顧客情報DBに絞って対策、この２点以外でISMSで必要と言われることは無視しなさい。
- １００点を目指してもダメ、費用対効果がリニアに上がる８０点を目指しなさい。
- 残るセキュリティリスクは許容する、事件が起こる前提で考えなさい。

セキュリティ対策度とコストの相関イメージ

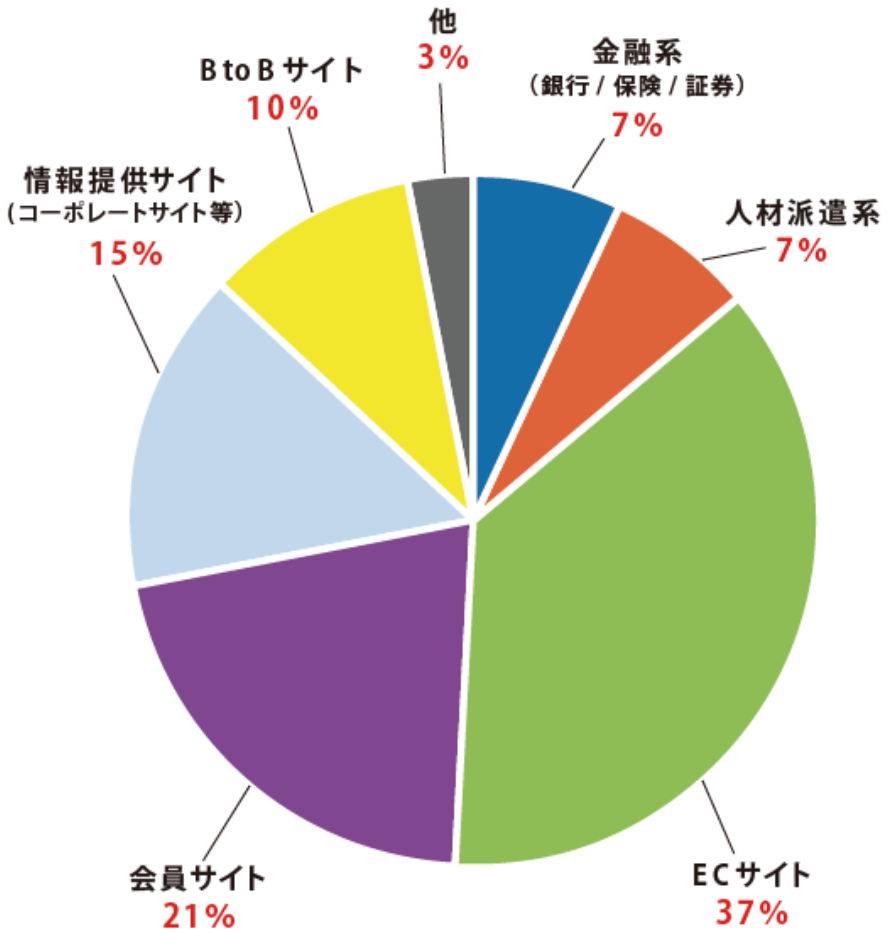


本日お薦めしたいWebアプリケーション脆弱性対策サービス

SaaS型WAFサービス：Scutum

Scutum SaaS型WAFサービス 【スキュータム】

ご利用業種の分布



ご利用実績：300サイト以上（2012年12月現在）

導入企業様の一例

- ディップ株式会社様
- 株式会社転送コム様
- 株式会社カフェグループ・ソリューションズ様
- 学校法人　大妻学院様

OEM　提携先

- 株式会社インターネットイニシアティブ（IIJ）様
- 株式会社電通国際情報サービス（ISID）様

販売代理店

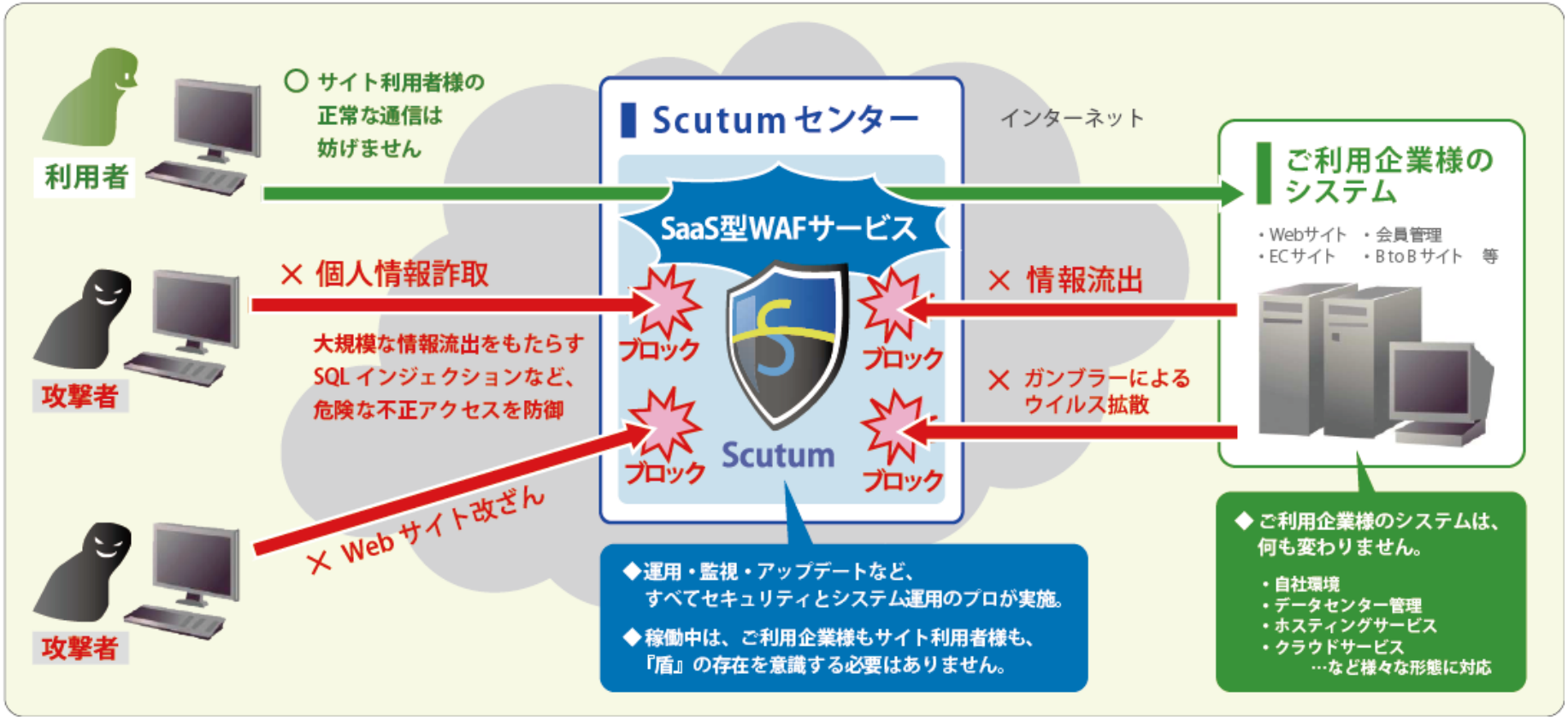
- 株式会社アイ・シー・アイ
- 株式会社イーツ
- 日本ベリサイン株式会社
- プロフェッショナル・ネットワーク・コンサルティング株式会社

Scutum 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）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。



Scutum 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）のサービス特徴／コンセプト

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。

Scutum のベースとなるソフトウェアは 2004 年に日本人により開発されました。複数のセキュリティ専門家に高評価を受けたそのソフトウェアを SaaS 用に再開発したものが Scutum です。豊富な利用実績と経験に基づいて運営されています。

導入が容易

導入は DNS を変更するだけ。※
事前調整も現地作業も不要です。

通常はアプライアンスを設置したり、ソフトウェアをインストールする必要があります。データセンタの入館調整や、電源の確保、現地調整、当日作業の付き添い、もし問題が発生した場合の切り戻し対応…。スムーズに導入できたとしても相当な作業量が発生します。
Scutum は DNS に登録してある Web サーバの IP アドレスを Scutum で用意する IP アドレスに変更するだけで切り替え作業は終了します。現地調整も入館手続きも、もちろん電源の心配も全く必要ありません。

※ SSL 通信を利用する場合は、証明書のインポート作業も必要になります。

低価格

Scutum は月額約３万円から利用できる手軽なサービスです。
WAF のアプライアンスを購入するとどうしても数百万円以上の費用となるため、
初期投資額は明確に異なります。

私たちは、「Web サイトを安全に運用するためには大きな投資が必要」という現状に全く満足しておりません。この WEB サイトセキュリティの分野でも、技術革新はめざましいものがあります。現在提供されている WAF のアプライアンスを、例えば 3 年や 5 年の償却期間を前提に購入する場合、利用期間の後半には性能面・機能面で見劣りがし、結果的に無駄な投資となる危険性を伴います。
Scutum は、一定の月額のままサービス自体が常に進化を続けるため、このような過剰投資の心配がありません。

安定性

Scutum のエンジン部分は、ネットワークやセキュリティ分野において著名な金床（株式会社ビットフォレスト取締役／株式会社セキュアスカイ・テクノロジー技術顧問）によるもので、Web アプリケーションファイアウォールの製品として 7 年以上の稼働実績があります。

システムは既に安定しており、高い防御効果を評価されたエンジンです。

Scutum 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。

提供企業の信頼感

SSTが有する、300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。

また、Stucumで対応できない脆弱性に対しては、診断サービスを併用した個別対応が可能です。

新しい脆弱性への対応

最新の脆弱性への対応もスピーディー。脆弱性検査で新しく検出された脆弱性はScutumで防御できるかチェックを行います。

まだScutumで対応できていない問題が見つかった場合には、防御シグネチャの見直しを行い、できるだけ早くScutumで対応できるような体制を用意しています。

実績・事例

金融機関や公的機関等でもご利用いただいております。2012年12月現在、300サイト以上に導入済みです。

またScutumのWebサイトでは、ご利用企業様よりいただいた導入後のご感想の一部を紹介しております。ECサイトや企業サイト等で、いままでのセキュリティ対策とは全く異なる経験をされていることがご理解いただけることでしょう。

サポート体制

Scutumの思想は効率化で貫かれています。できるだけ少ない投資でWebサイトに安全をもたらすためこの姿勢は譲ることはできません。ただし、サポートに関しては若干異なる考え方を持っております。

Scutumは低コストのサービスですが、障害対応はもちろん24時間365日、お電話での連絡にもお応えします。御社のWebサイトをお守りする運用体制は万全です。

いつでもやめられる

ご利用は1ヶ月からOK。短期間だけ利用するキャンペーンサイトにも導入可能です。

また、もし機能に満足いただけない場合でもすぐに別のソリューションに切り替えることができます。

クラウド対応

これからのWebサイトは、やはりクラウド環境で構築されることが一般的になるでしょう。

Scutumは設計当初から、クラウドインフラへの対応に大きなリソースを割いてきました。2011年8月の時点で正式対応クラウドは3つ。正式には対応を表明していないまでも利用が可能なクラウドはほかにも多数あります。

今後より良いクラウドサービスが発表されたら是非教えてください。いち早く私たちの対応クラウドに追加されることでしょう。

Scutum 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

スキュータムは月額制です。
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	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

オプション

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
Scutum CDNオプション	初期費用 無料 月額費用 無料（100GB/月まで利用可能）

（※）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。**
- **金額は税別です。別途消費税が加算されますのでご了承下さい。**
- **お客様のご要望により Amazon EC2上にScutum環境を構築してサービスをご提供する場合、当料金表とは異なるプランをご提案させていただく場合がございます。**

Scutum 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。

高トラフィック対応プランについて

① 100Mbps以上の帯域にも対応

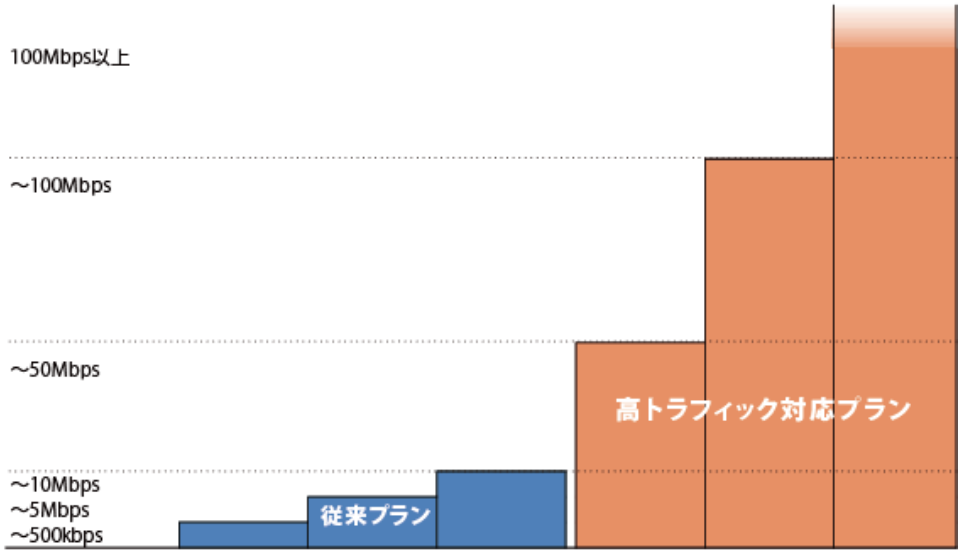
従来は、ピーク時のトラフィックが回線速度として10Mbps程度まで（**右図青色**）のウェブサイトがご利用対象でしたが、約1年間の研究開発と実証実験の結果、WAFサービスの処理能力を「100Mbps以上」と大幅に増強することに成功しました。2011年4月よりご提供を開始した高トラフィックサービス（**右図オレンジ色**）の追加により、国内Webサイトの99%以上（*1）がScutumを利用可能になり、従来のアプライアンス型WAFに匹敵する処理能力を実現しました。

② クラウドサービスとの相性も抜群

クラウドサービスを既にご利用、または今後利用を検討されている中規模・大規模Webサイトにおいて、Webアプリケーションセキュリティの品質を損なわず、クラウドサービスのメリットを最大限に引き出すことが可能となります。
「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」というこれまでのジレンマを解決します。

③ 大幅なコスト削減が可能に

これまでもご好評いただいていた「簡単に導入・運用できる」というScutum最大のメリットはそのままに、高トラフィックにも対応できるため、大規模サイトで従来一般的だったアプライアンス型のWAFと比較してコストの大幅削減が可能です（*2）。



初期費用（税別）	¥98,000			¥198,000		個別お見積
月額費用（税別）	¥29,800	¥59,800	¥128,000	¥148,000	¥198,000	
運用可能ホスト数	1 FQDN			10 FQDN （※）		別途ご提案

（※）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。

*1 国内主要サイトのアクセス数推定を元に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。

*2 アプライアンスWAFの標準的な保守サービスを5年間利用する場合を想定したSST試算。

Scutum 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	認証	クライアント側での攻撃	コマンドの実行	情報公開	マルウェア対策
攻撃名称	総当たり	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 情報漏洩 パストラバーサル リソースの位置を推測	ガンブラー（Gumblar）によるウイルス拡散 その他

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。

※ SQLインジェクションを用いて行われる大規模攻撃、通称「LIZAMOON」（ライザムーン）についても当初より対応しております。

新しい脆弱性への対応

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ので、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。

Scutum 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

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。
お客様側で必須となる作業は、
赤文字の３ステップとなります。

	お客様側の流れ	弊社での作業
お申込	対象サイトの情報をご準備 ・サイトのURL ・サイトのトラフィック情報	ご提案書／お見積 契約関連資料準備
1	ヒアリングシートのご記入 ※ 弊社担当がお手伝い／補足させていただきます。	Scutumの設定 （約３営業日）
2	お試し利用（hostsテスト） ※ まずはお客様サイトのサービスに影響のない範囲で、「Scutum」の利用を実感していただきます。	お試し利用方法のご案内 管理画面利用方法のご案内
3	SSL証明書／秘密鍵のご準備 ※証明書をご準備して頂き、管理画面よりアップロードして頂きます。	Scutumにお客様固有のSSL証明書を設定 （約3営業日）
4	DNSの変更 ※弊社担当が変更方法をアナウンスします。	DNS変更情報のご案内
5	モニター運用の開始 ※ 正常通信の誤検知を避ける為、まずはブロックをしない運用にてスタートします。	正常通信の誤検知調整
運用開始	防御開始	24時間365日の運用窓口を提供

Scutum SaaS型WAFサービス 【スキュータム】

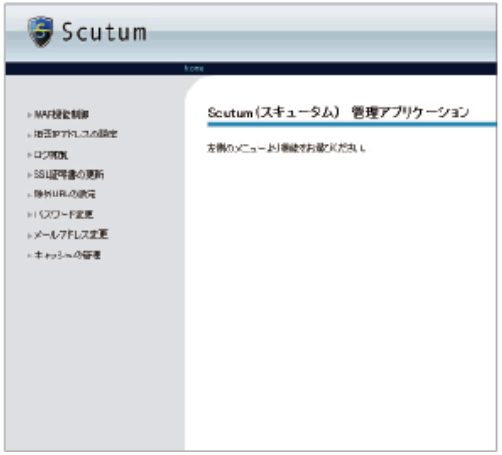
クラウド時代の、新しいWebアプリケーションファイアウォール。

管理画面について

スキュータムの管理機能は、ご契約者様専用ページ内の個別管理画面から、
ウェブブラウザ経由で手軽かつセキュアにご利用いただけます

管理者機能一覧

管理画面 TOP



① WAF 設定機能

- **WAF機能 ON/OFF設定**
  不正な通信を遮断するモードとモニタリングするモードの変更が可能です。
- **拒否IPアドレスの設定**
  設定したIPアドレスからのアクセスを拒否することが可能です。
- **除外 URL の設定**
  防御対象外にするディレクトリまたはファイルを指定することが可能です。

② 防御ログ確認機能

- **防御ログ閲覧**
  防御／モニタリングしたログを、一覧と詳細で確認することができます。防御ログをダウンロードすることも可能です。
- **攻撃元TOP5**
- **攻撃種別TOP5**
  過去30日間の傾向を把握していただくための情報です。

③ その他管理機能

- **証明書／秘密鍵のアップロード**
  SSL通信に使う証明書と秘密鍵を、安全にアップロードいただけます。
- **管理者アカウント管理**
  メールアドレスやパスワードの変更を行います。

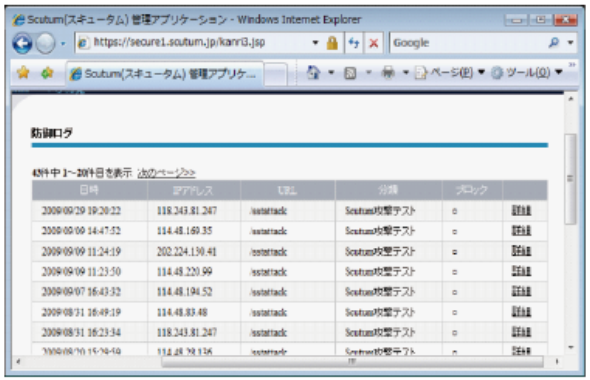
Scutum SaaS型WAFサービス 【スキュータム】

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。

防御ログ確認機能の詳細

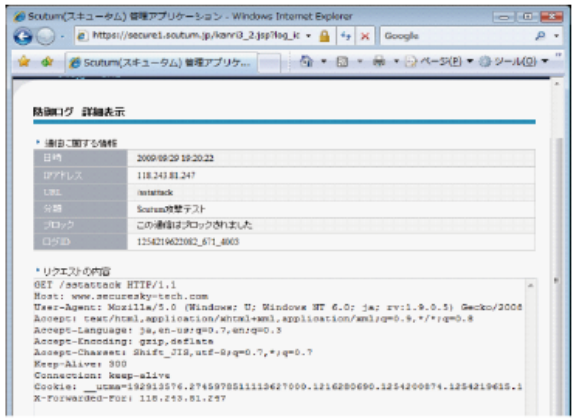
防御ログ閲覧画面

【一 覧】



- **日時**
  攻撃のあった日時を示します。
- **IPアドレス**
  攻撃元 IP アドレスを示します。
- **URL**
  攻撃を受けた URL を示します。
- **分類**
  攻撃種別を示します。
- **ブロック**
  ブロックをしたか、
  モニタリングをしたかを示します。
  ※ ブロックされていた場合は “○”

【詳 細】



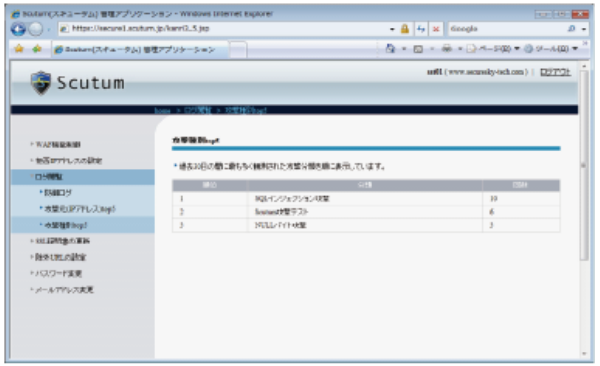
それぞれの通信の詳細のリクエストを見ることが可能です。

攻撃元(IPアドレス) TOP5

過去30日間で攻撃が観測されたIPアドレスTOP5を表示します。

攻撃種別 TOP5

過去 30 日間で観測された攻撃種別の TOP5 を表示します。



Scutum 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。

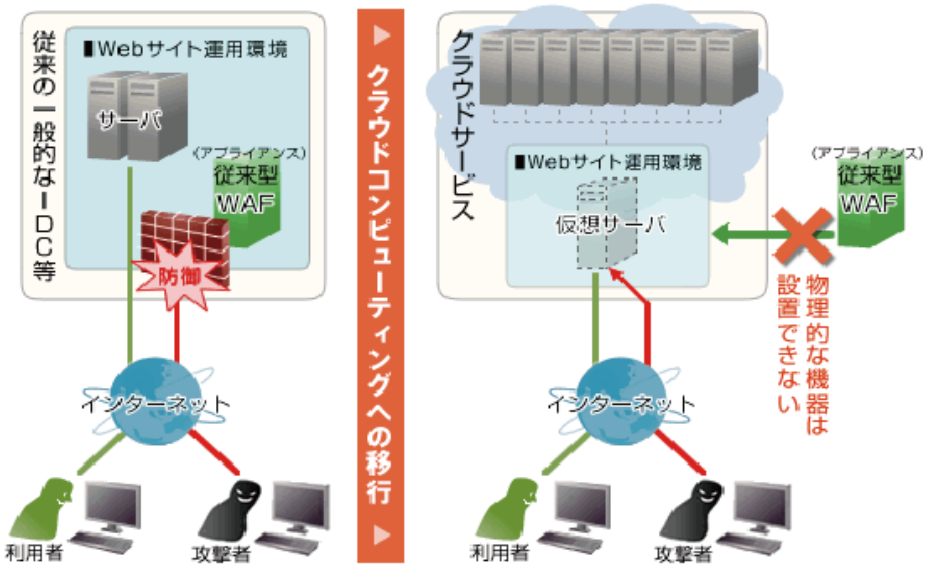
クラウド環境にも最適

SaaS型WAFのスキュータムなら、これまで物理的なセキュリティ機器を設置できなかったパブリッククラウド上のサーバ環境にも、かんたんにWAF機能を導入できます。

従来型Webサイトセキュリティの限界

多くのパブリッククラウド環境では、クラウドサービスを提供する事業者がサーバ本体 / 周辺ハードウェア / ネットワーク接続の全てを統一的にコントロールおり、利用者は独自に物理的な機器を設置することができません。

そのため、従来多く利用されてきたアプライアンス型の WAF ではハードウェアの設置自体が困難です。ソフトウェアインストール型 WAF の場合も、クラウド上では必要な環境整備が難しいことも多く、導入の障壁となっています。



Scutum 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。

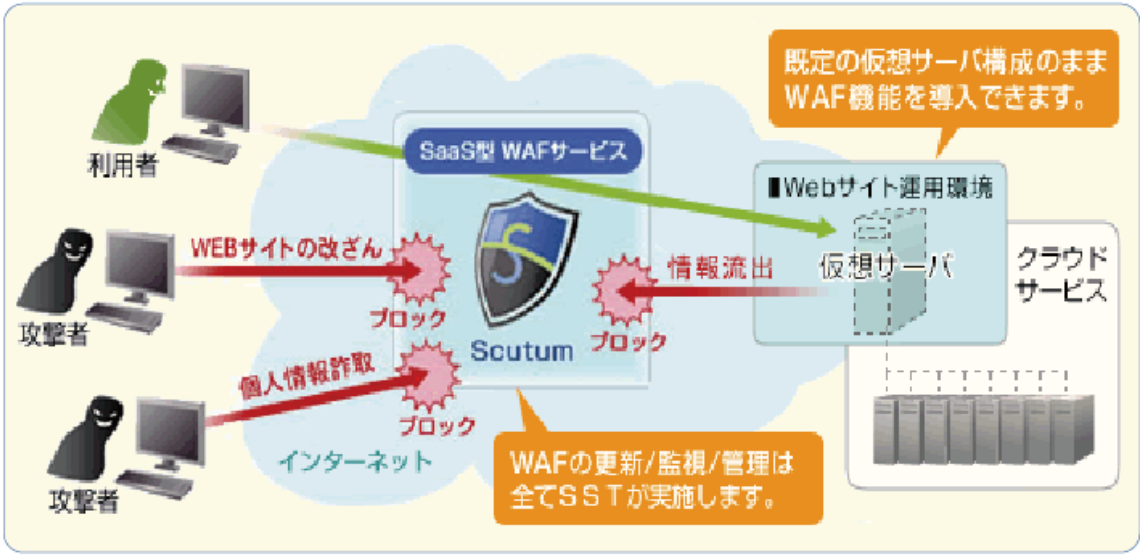
SaaS型のスキュータムは環境を選びません

Scutum は SaaS 型のため、既定の仮想サーバ構成でしか利用できないパブリッククラウド環境上の Webサイトにも、WAF機能の導入が可能となりました。

しかも、

- 導入までのスピード
- 自前のインフラを持たない
- 初期費／運用費とも小さい
- スケールアウトが容易
- 短期利用が可能
- 管理者不要

など、クラウド本来のメリットを最大限に引き出すことが可能なセキュリティサービスです。



主要クラウドサービスに続々対応

企業様がご利用中のクラウド環境上の近くに、仮想サーバの一つとしてScutumを配置する提供形態にも注力しております。

対象 Web サービスと同一クラウド環境上で構築することで、レイテンシーの影響を最小限に抑えることが可能です。

対応可能なクラウドサービス例（2011年8月現在）	
IIJ GIO	株式会社インターネットイニシアティブ（IIJ）
NIFTY Cloud ニフティ クラウド	ニフティ株式会社
Amazon EC2	amazon.com

Scutum 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 CDNオプション

ScutumCDNオプションは、Scutumを導入しているWebサイトで手軽にCDN（コンテンツデリバリーネットワーク）機能をご利用いただけるサービスです。

CDNオプションの概要

特定の種別のファイル(画像およびPDFファイル）をCDNサーバにキャッシュとして保存し、配信することができます。

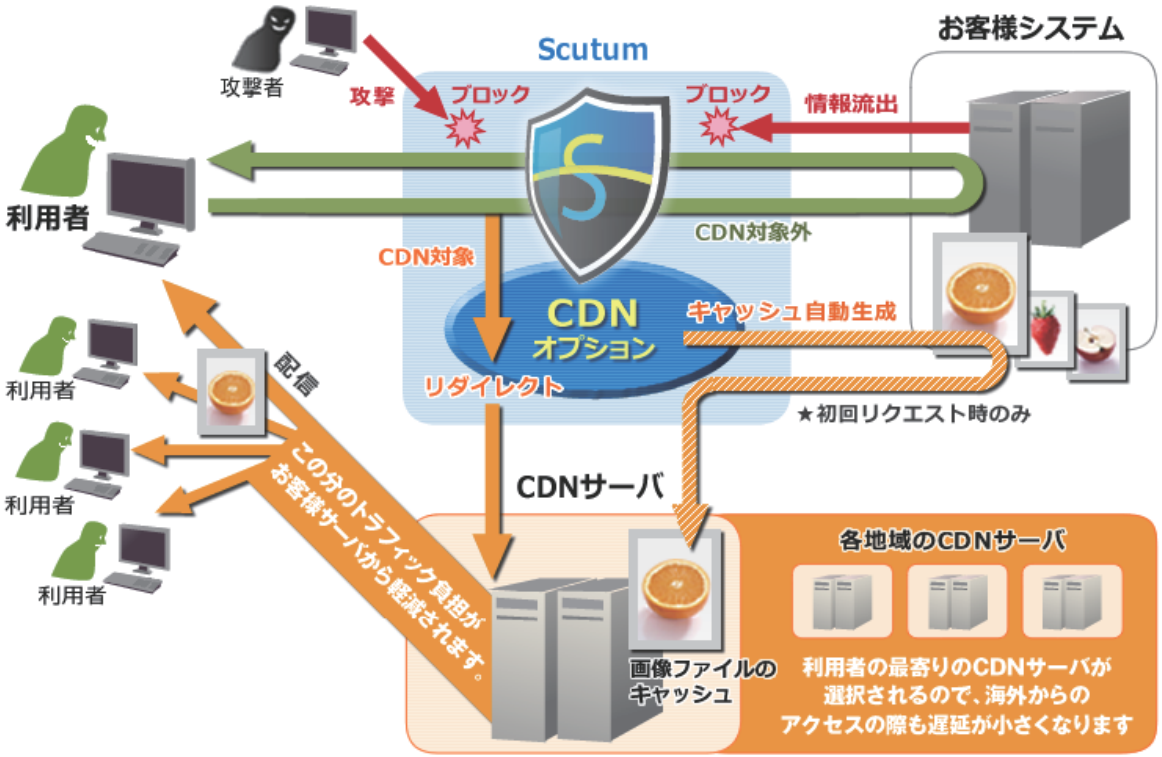
遠隔地から閲覧する場合には、接続元に近いCDNサーバから該当するファイルを配信します。

※ キャッシュ可能なファイルの種別は次の通りです。
- 画像ファイル（jpg, jpeg, 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。

※ Scutumご契約者様へのオプションサービスとなります。CDN機能のみのご提供は行っておりません。

※ CDNオプションの詳細機能やご利用方法、ご注意事項につきましては、下記連絡先までお気軽にお尋ねください。



Scutum 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。

こんなサイトに効果的です

1. ピーク時の急なアクセス増が悩み
2. 大きな画像が多いサイト
3. 海外からのアクセスが多い

◆ 素早いレスポンスとサーバ負荷軽減

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、サイトご利用者が Web 閲覧を高速かつ安定して行えるとともに、お客様サーバ / ネットワークの負荷も軽減します。遠隔地からのアクセスについては、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となります。

◆ 全世界からのアクセスに効果を発揮

Scutum で実装する CDN オプションサービスは、CDN サービスのリーディングカンパニーであるアカマイのバックボーンを利用しており、日本国内のみならず、全世界からのアクセスに対し、効果を発揮するサービスとなっております。

無償で月100GBまでご利用可能

Scutum CDNオプションは、**初期費用、月額料金とも無料！**
Scutum ご契約者様であれば、**管理画面から簡単にお申し込み**いただくだけで、**月間100GBまで**無償でCDN機能をご利用いただくことが可能です。
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よう設定することも可能です。

Scutum 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。

従来型WAFとの比較

従来のアプライアンス型、ソフトウェア型WAFの課題を克服するため、ScutumではSaaS型のサービス形態を採用しました。
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ご提供いたします。

		従来型WAF	Scutum
全般	通信形態	アプライアンス型／ソフトウェア型	SaaS型
	防御モデル	ホワイトリストとブラックリストの両方を使用することができ、高いセキュリティ要求にも対応可能。	ブラックリストを使ったシグネチャモデルのみを採用し、サイトの構成変更にも柔軟に対応可能。
	セキュリティ技術者	導入・運用時とも、お客様サイトのシステム構成とWAFを理解したセキュリティ専門技術者が必要。	導入・運用ともScutumのセキュリティ技術者が全て実施するため、お客様ではWAF用の技術者は不要。これまで通りのサーバ運営でOK。
導入	導入費用	機器購入費用、保守費用、設計・構築費用など高価な初期費用が発生する。 年毎に機器の保守費用、設定変更時にメンテナンス費用が必要となることが一般的。	初期費用：￥98,000～、月額：￥29,800～の低価格ですぐに使用可能な複数台の冗長構成をご用意。 ※金額はいずれも消費税別
	導入作業/期間	サイトに合わせて細かいパラメータ設定が必要で、導入まで半年ほど掛かる場合も。 運用開始後も、アプリケーションを変更するたびにWAF設定の変更が必要となることが多い。	お客様側の導入時作業はDNSの切替だけとなるため、即座に導入が可能。

Scutum 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。

			従来型WAF	Scutum
運用	ハードウェア	スケールアウト／スケールダウン	機器の買い替えが必要	契約変更により対応可能
		障害対応	機器交換時の立会調整及び、その間のネットワーク構成について考慮が必要	エンドユーザが意識をせず、全てScutum側で対応
	WAFエンジン	アップデート	リモートでの自動更新。エンドユーザが意識をせず対応を実施	エンドユーザが意識をせず、全てScutum側で対応
		障害対応	通常はリモート運用。障害の内容により、現地作業が必要となった場合、立会調整及びその間のネットワーク構成について考慮が必要	エンドユーザが意識をせず、全てScutum側で対応
	防御シグネチャ	アップデート	リモートでの自動更新。エンドユーザが意識をせず対応を実施	エンドユーザが意識をせず、全てScutum側で対応
		防御ログ確認	ブロックせず防御ログに記録するだけのシグネチャついては、誤報も含め、お客様が閲覧する管理画面に出力されるだけという形が一般的で、その分析や対応の実施まで標準で提供しているケースは稀。	ブロックせず防御ログに記録するだけのシグネチャについても、Scutum技術者が標準運用の範囲内で内容やリスクを分析し、必要に応じて対応を行う。
		誤検知対応	お客様にて現象を確認し、運用ベンダーに問合せ、URLやパラメータ単位でシグネチャを外す運用。 もしくは該当のシグネチャを外す等の運用になるがお客様判断が必要になってくる。 また、シグネチャ自体をOFFにする運用となる為、防御効果が落ちる。	Scutum技術者がログを確認しているので、誤検知が発生した場合、通常Scutum側から連絡する形となる。 また、誤検知によるシグネチャ調整は、お客様個別にシグネチャ自体を書き換える運用となるため、防御効果を極力落とさない運用が可能。

～キャンペーンのご案内～

「官公庁」「自治体（地方公共団体）」「教育機関」対象

ご提供期間
2013年3月末まで
先着100サイト

WAFサービス「Scutum」が掲示板への不正書き込み対策をご支援します。

CSRF対策診断・対策措置
期間限定で無償提供

- Webサイトの掲示板などについて、CSRFの脆弱性の有無を無償でチェックします。
- CSRFの脆弱性が発見された場合、WAFサービス「Scutum」で防御します。

～キャンペーン内容～

◆対象とする官公庁、自治体、教育機関のWebサイトは、
比較的セキュリティ対策度が低いのが実情です。
そして、不正アクセスの対象になりやすいのも特徴です。

◆ICI／SSTでは、横浜市ホームページへの書き込みに寄る誤認逮捕事件を受けて、掲示板のCSRF(クロスサイトリクエストフォージェリ:「リクエスト強要」)の脆弱性の有無を調査し、脆弱性が検出された場合は、
２０１３年３月までScutumを無償提供する支援を行っています。