Colorkrew

くらまね™ Cloud Management Security

セキュリティ対策・運用監視サービスのご紹介

Security Project

目次

- くらまね Securityとは
- サービス概要
- ゲートウェイ型WAFのご紹介
- ホスト型IPS/IDSのご紹介
- ゲートウェイ型IPS/IDSのご紹介

くらまね Securityとは

くらまねSecurityとは

◆インターネットに公開したWebサイトの99%以上が、サイバー攻撃のリスクに晒されます。

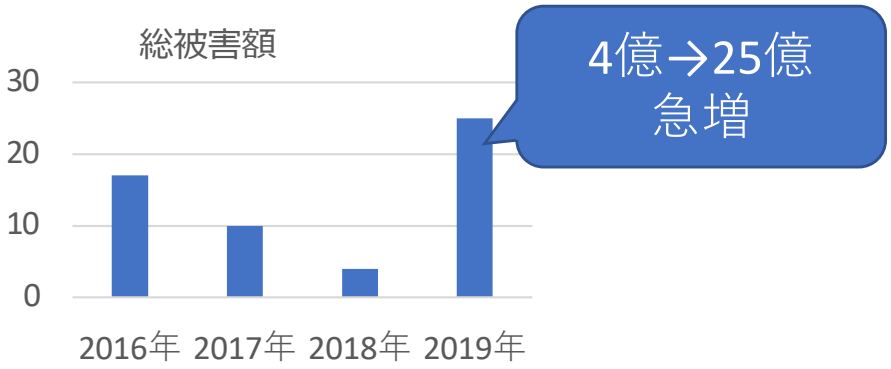
増加するサイバー攻撃
年間攻撃ログ数（日本国内）：**1億件** ※1

中小企業への攻撃が多い
50~199人規模の中小企業への攻撃：**約6割** ※1

⇒ ほぼ全ての企業が攻撃の対象

インターネットバンキング不正送金

※2



個人情報漏えい

2018年度個人情報漏洩の想定損害賠償総額 ※3

2,684億5,743万円

1件あたり想定損害賠償額

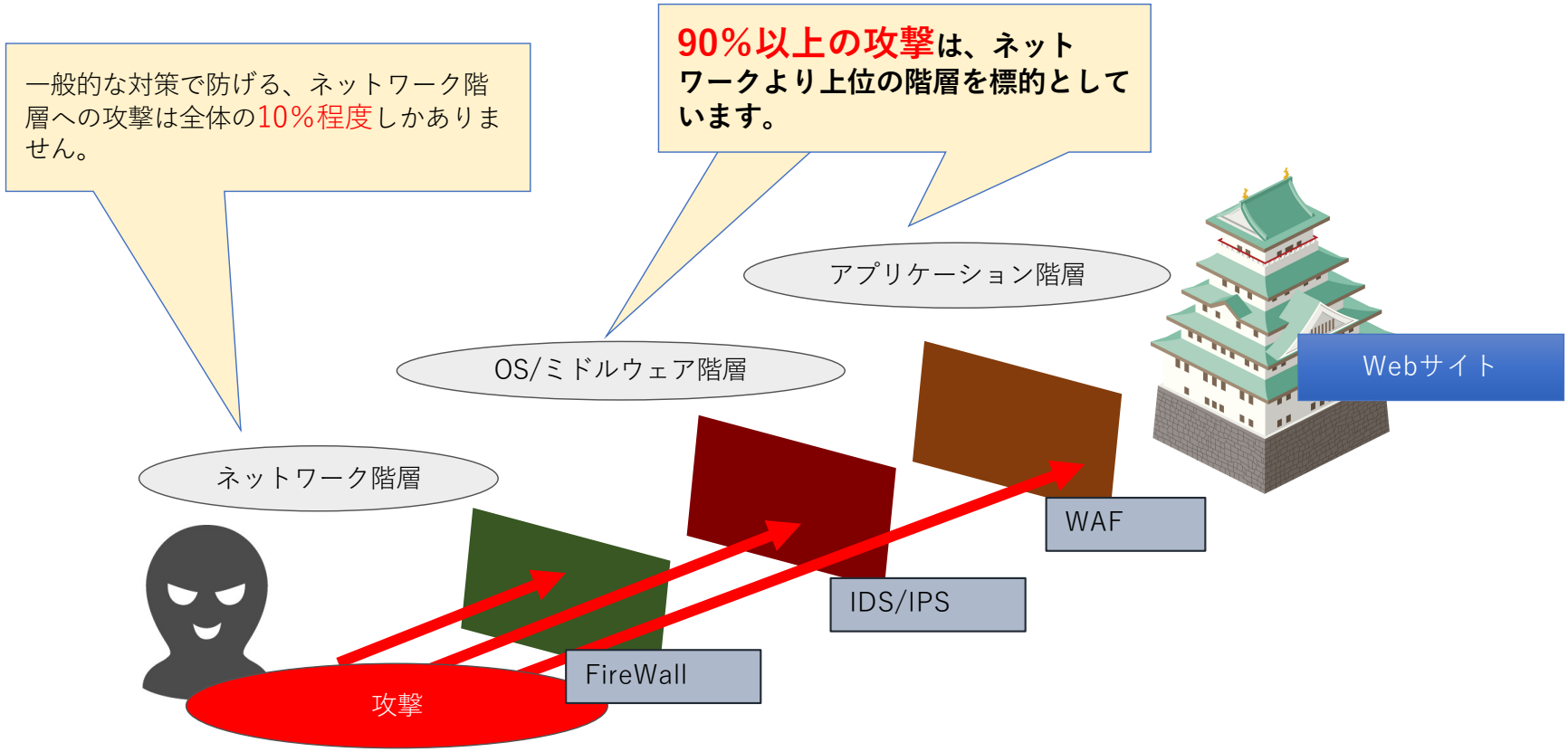
6億3,767万円

攻撃を受けた際の被害額も年々増加しています。

※1：サイバー攻撃白書 2018年度攻撃分析レポート
※2：警察庁調べ
※3：日本ネットワークセキュリティ協会 2018年 情報セキュリティインシデントに関する調査報告書

くらまねSecurityとは

◆攻撃の方法は年々多様化しており、Webサイト側も様々な対策を行う必要があります。



「Webサイト改ざん」などの攻撃を、FireWallだけで防ぐことは困難です。
それぞれの階層に適した商品を組み合わせて、セキュリティレベルを上げる事が重要です。

くらまねSecurityとは

◆くらまね Securityのポイント

- インターネット環境におけるセキュリティ対策は、もはやFireWallだけでは十分とは言えません。
- しかし、あらゆるセキュリティ対策を制限なく施していては膨大なコストが発生します。
- 最善のセキュリティ対策とは、システムの環境や利用目的、コスト感によって変化するはずです。
- 「くらまね」では、お客様のご要件をヒアリングさせていただき、お客様に合ったセキュリティプランをご提案させていただきます。

サービス概要

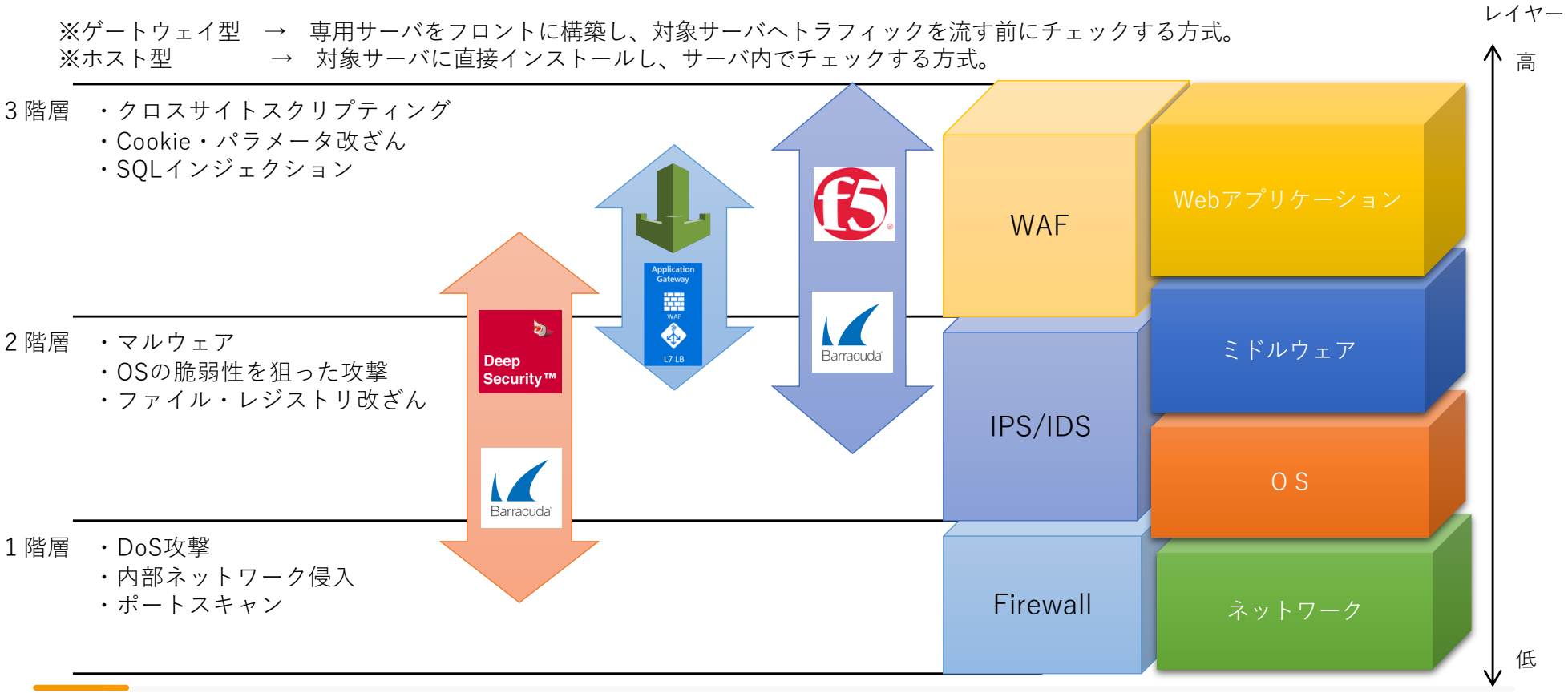
セキュリティ製品の特徴

◆セキュリティ製品には、得意分野があります（※）

※）多くの製品がネットワークからアプリケーション層までを幅広くカバーしていますが、すべての機能を網羅した製品はありません。

【提供するセキュリティ製品】
・BIG-IP ASM、Barracuda WAF・・・ゲートウェイ型WAF。導入・運用は困難だが、高度なカスタマイズが可能。
・AWS WAF、Azure WAF・・・・・・ゲートウェイ型WAF。導入・運用は手軽だが、高度なカスタマイズは困難。
・Deep Security・・・・・・・・・・ ホスト型IPS/IDS。WAFとしても機能するため、幅広い層をカバーできる。
・Barracuda NGF・・・・・・・・・・ ゲートウェイ型IPS/IDS。サンドボックスなど、高度なエンドポイント機能も持つ。

※ゲートウェイ型　→　専用サーバをフロントに構築し、対象サーバへトラフィックを流す前にチェックする方式。
※ホスト型　　→　対象サーバに直接インストールし、サーバ内でチェックする方式。



Colorkrewが提供するセキュリティ製品

◆クラウド純正からサードパーティー製品まで、ラインナップは豊富です。

WAF

豊富な機能、繊細なチューニング

Barracuda WAF

BIG-IP ASM(WAF)

リーズナブルな価格とシンプルな操作性

Azure WAF

AWS WAF

IDS/IPS

幅広い階層をカバー
Trend Micro Deep Security

エンドポイントのマルウェア対策も可能
Barracuda NG Firewall

製品比較

		IPS/IDS		WAF	
階層	攻撃名	Deep Security	Barracuda NGF	AWS WAF /Azure WAF	BIG-IP ASM /Barracuda WAF
アプリケーション	ブルートフォース/リストアタック	-	-	-	◎
	L７Dos攻撃	-	-	-	◎
	Cookie・パラメータ改ざん	-	-	-	◎
	カード情報漏洩	-	-	-	◎
	クロスサイトスクリプティング	△	△	○	◎
	SQLインジェクション	△	△	○	◎
	OSコマンドインジェクション	△	△	○	◎
	ディレクトリトラバーサル	△	△	○	◎
OS・ミドルウェア	既知のマルウェア	◎	◎	-	-
	未知のマルウェア	-	◎	-	-
	ゼロデイ攻撃	◎	◎	○	◎
	IP/Webレピュテーション	○	○	○	○
	ファイル・レジストリ改ざん	◎	-	-	-
	パーミッション改ざん	○	-	-	-
ネットワーク	ポートスキャン	○	◎	-	◎

◎・・・トップレベルの機能がある　　○・・・優れた機能がある　　△・・・機能がある
※この対比表は指標であり、各機能の優越を正確に保証するものではありません。

継続したセキュリティ運用の必要性

セキュリティ製品を導入したら終わり？

いいえ、継続的なセキュリティ運用が必要です。

なぜ？

機械は万能ではないので、以下のチェックが定期的に必要です。

・誤検知はないか？正常なサービスを止めていないか？

アプリの変更があった場合や、ポリシーの変更があった場合に発生するかもしれません。

・防御漏れはないか？攻撃をスルーしていないか？

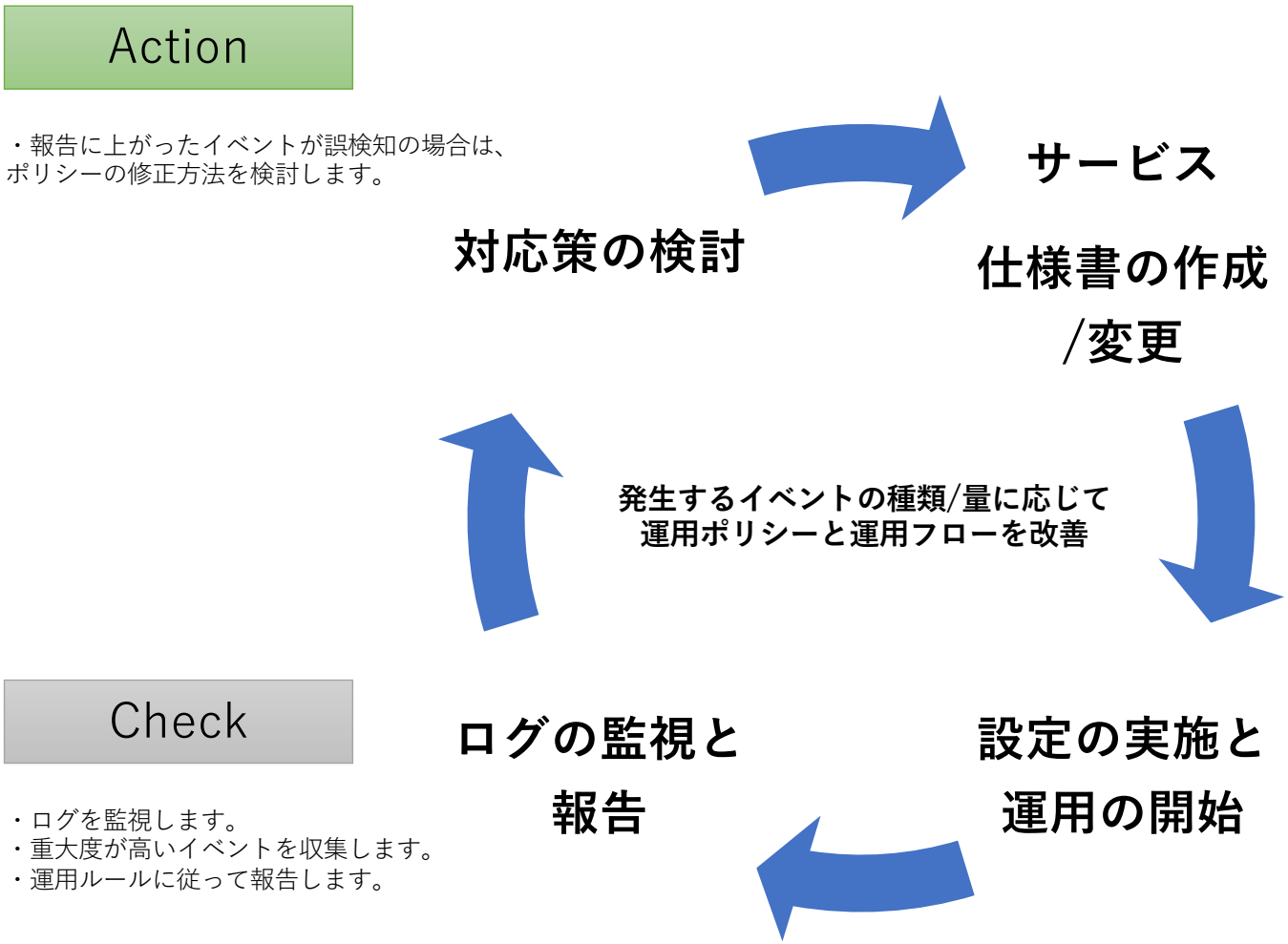
ポリシーの設定漏れがあれば、明らかに攻撃と分かるものを通しているかもしれません。

・標的型攻撃に晒されていないか？

本格的な攻撃を受ける前（偵察時）に発見することが重要です。

『くらまね Security』がこれらをお手伝いします。

セキュリティ運用イメージ



ゲートウェイ型WAFのご紹介

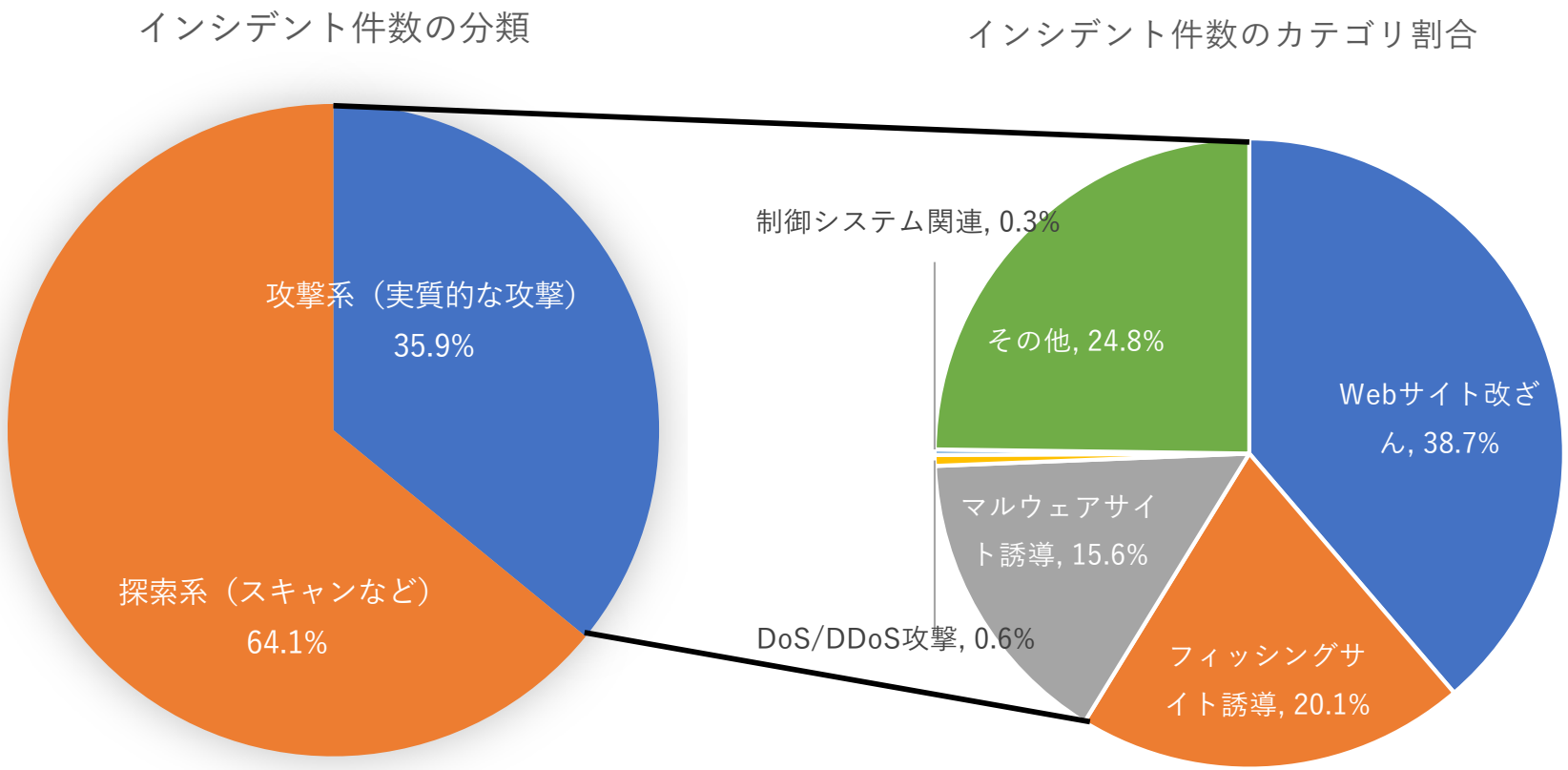
F5 BIG-IP ASM

Barracuda WAF

AWS WAF

Azure WAF

Webアプリケーションの脅威



JPCERT/CC インシデント報告対応レポート[2015年10月1日～2015年12月31日]

多様化する攻撃の中でも、Webサイトにおける実質的なサイバー攻撃は、
Webアプリケーションへの攻撃が大半を占めます。
これらの攻撃を防ぐためには、WAFは不可欠です。

WAFの特徴

◆WAFはアプリ層を狙った攻撃から、大事なシステムやデータを守ります。

シグネチャの精度が高い

シグネチャとは、サイバー攻撃のパターンを識別するファイルのことで、クロスサイトスクリプティング、SQLインジェクション、OSコマンドインジェクションなどの攻撃を検知/防御します。
IPS/IDSの中にも、このシグネチャを使ってこれらの攻撃を検知/防御できる製品もありますが、WAFのシグネチャと比べると、その質と量が圧倒的に劣ると言われています。
また、WAFのシグネチャは頻繁にアップデートされます。

SSL/TLSで暗号化された通信をチェックできる

SSL/TLSの複合化をWebサーバーで行っている場合、通信内容が暗号化されているため、IPS/IDSでは攻撃を検知できません。
WAFの場合、WAF自身に複合化機能があるため、暗号化された通信でもチェックが可能です。

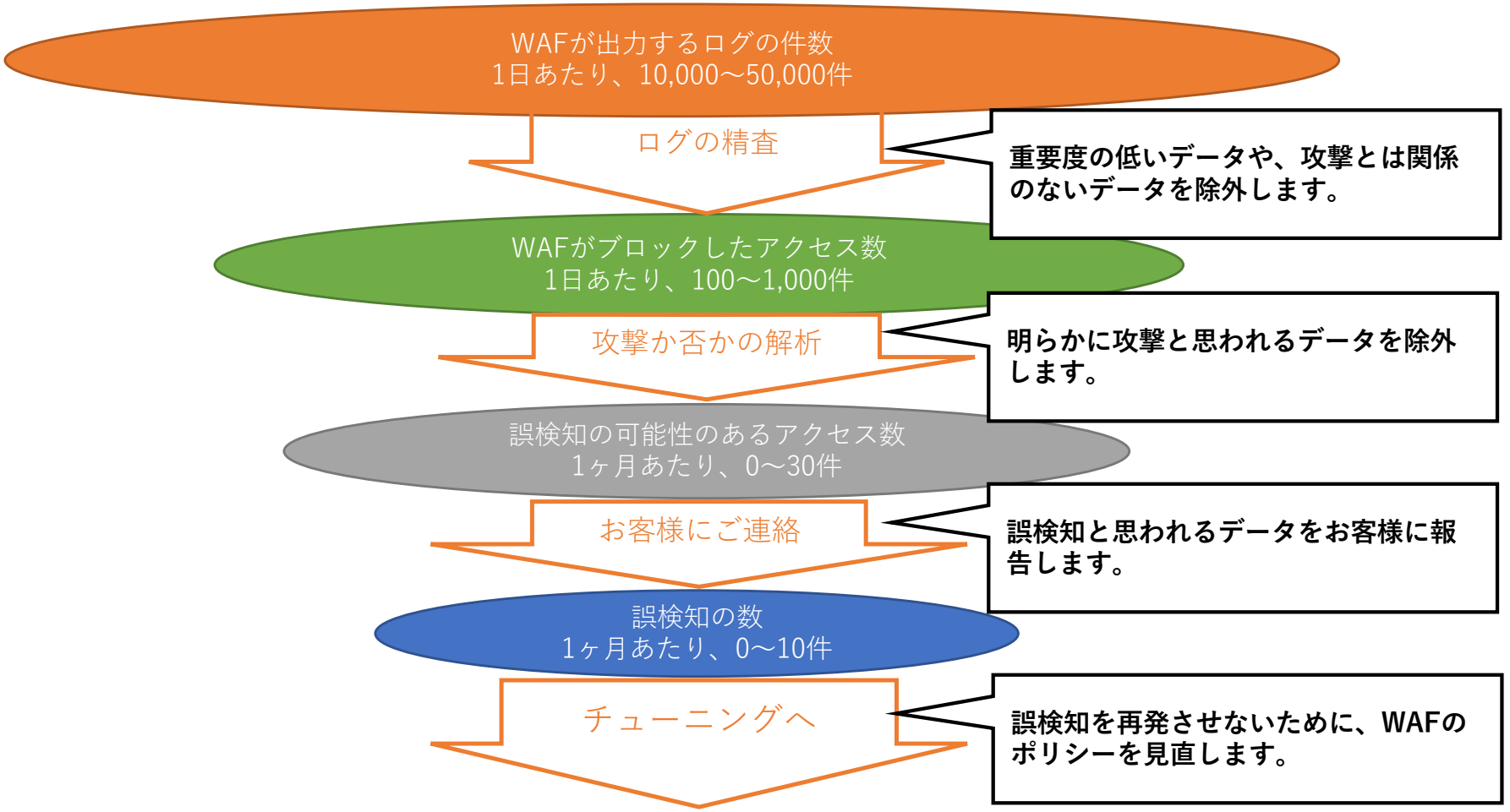
個人情報の漏洩を防ぐ　※AWS WAF、Azure WAFは除く

クレジットカード番号漏洩、セッションハイジャック、ブルートフォース/リストアタックなど、個人情報の搾取を目的とした攻撃に対する対策が充実しています。
例えば、クレジットカード番号が抜かれた場合、アプリケーション側でマスキング処理が施されていなくても、WAF自身にクレジットカード番号のマスキング機能があるため、クレジットカード番号が漏洩することはありません。

WAFの運用

一般的に、WAFの運用は面倒と言われます。

例）誤検知のチェック（約2,000PV/日規模の動画配信サイト）



WAFの運用

１．ログの解析

（１）誤検知のチェック

- **正常なアクセスを止めていないかチェックします。**
- **アプリケーションの変更やWAFのポリシー変更があると、とくに発生しやすくなります。**

（２）防御漏れのチェック

- **ポリシーの設定漏れやアップグレードを怠っていないかチェックします。**

（３）標的型攻撃のチェック

- **特定の攻撃者から執拗な攻撃を受けてないかチェックします。**

２．WAFのチューニング

（１）除外設定

- **誤検知の原因となったポリシーをカスタマイズしたり、一部のルールを無効化することで、誤検知の再発を防ぎます。**

（２）追加設定

- **ポリシーに新たなルールが配布された場合は、そのルールを検証し、追加します。**

Colorkrewが提供するWAF

WAF

BIG-IP ASM(WAF)

- 特徴
  Azure、AWS、GCP用のVirtual Editionが用意されています。
  Azure WAFやAWS WAFに比べて多機能であり、繊細なチューニングが可能です。
  保証帯域が大きいため、大規模サイトにも対応可能です。
  豊富なシグネチャが用意されており、頻繁にアップデートされています。
  シグネチャのアップデート後に、アップデートしたシグネチャだけを検知モードにして運用する機能があります（※）。

※ 通常の運用では、シグネチャのアップデート後は誤検知が発生しやすいため、一度すべてのシグネチャを検知モードで運用した後、防御モードに変更します。

Colorkrewが提供するWAF

WAF

Barracuda WAF

- 特徴
  Azure、AWS用のVirtual Editionが用意されています。
  Azure WAFやAWS WAFに比べて多機能であり、繊細なチューニングが可能です。
  BVM（Barracuda Vulnerability Manager）と呼ばれる脆弱性診断を行えば、セキュリティホールを発見し、最適なポリシーを自動生成してくれます。
  誤検知（※）が発生した場合、誤検知の元となったルールをボタンひとつで解除することが可能です。

※　正常なアクセスをWAFが間違ってブロックしてしまうこと。

Colorkrewが提供するWAF

WAF

AWS WAF

- 特徴
  CloudFrontもしくは、ALB(Application Load Balancer)の機能として提供されています。
  Conditionと呼ばれる5つの機能（XSS対策、SQLインジェクション対策、文字列チェック、IPアドレス制限、サイズ制限、地域制限）が用意されており、利用者はこのConditionをカスタマイズしてRuleにセットします。防御にするか検知にするかはRule単位に行います。
  Ruleの集合体をACLと呼びます。
  AWSの仕様による制限事項（※）があります。

※　AWS管理画面上のログ保存期間は3時間です。
　　1度に100件までのアタックログしか取得できません。
　　POSTメソッドの中身は見ることができません。

Colorkrewが提供するWAF

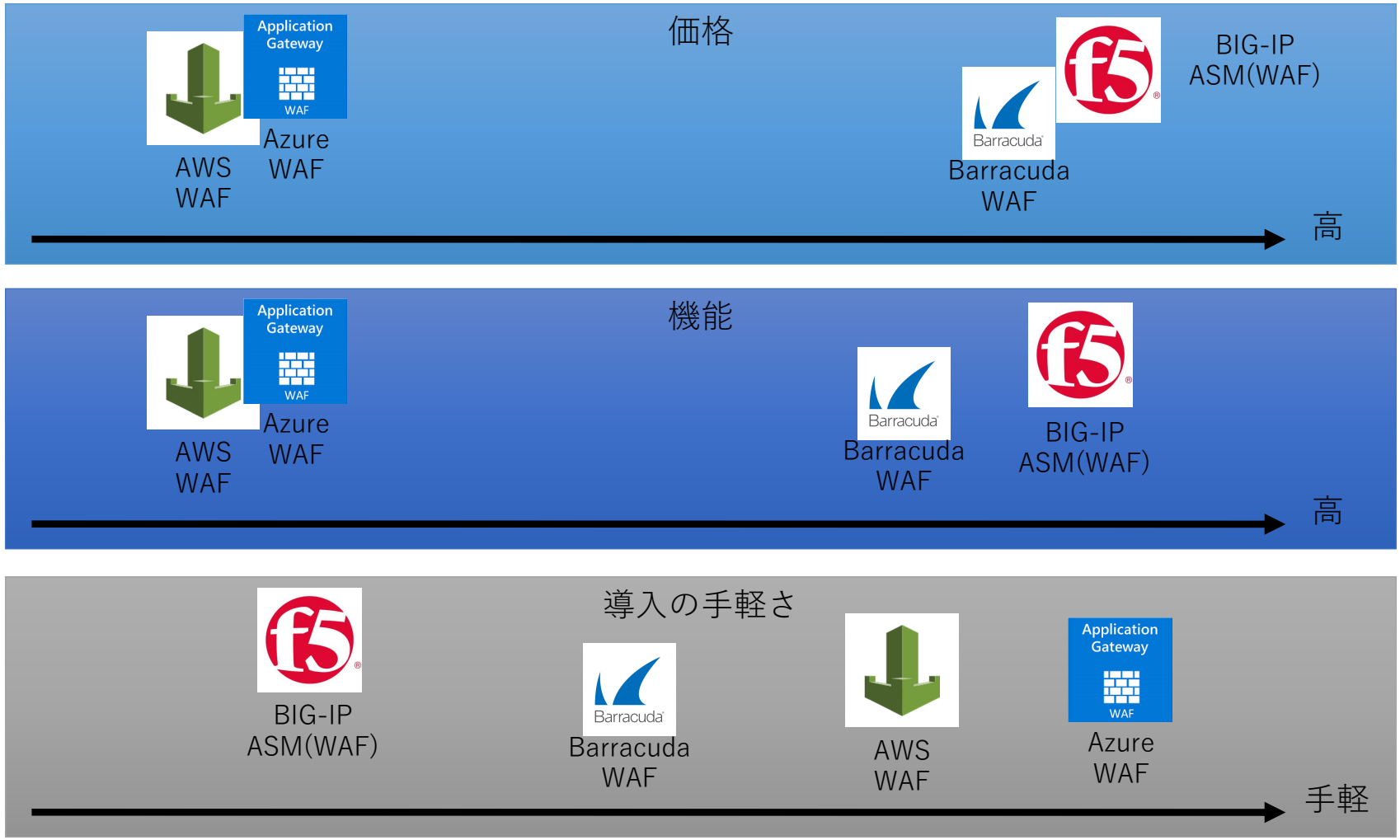
WAF

Azure WAF

- 特徴
  Application Gatewayの機能として提供されています。
  ModSecurity（※）をベースにしたWAFで、原則チューニングはルールのオン/オフだけというシンプルな設計です。
  標準でLog Analyticsという便利なログ解析ツールも使用できるため、比較的手軽に導入が可能です。

※ オープンソースで開発されているWAFで、Core Rule Set（CRS）という攻撃を検知するためのルールセットが用意されています。
OWASPというセキュリティの課題解決を目的としたオープンコミュニティが、主にこのCRSをメンテナンスしています。

WAF比較（参考）



価格は機能と比例するので、目的に合った製品を選択することが重要です。

ホスト型IPS/IDSのご紹介

Deep Security

Deep Securityの概要

Deep Securityの機能はウイルス対策だけではありません。
あらゆる脅威に幅広く対応しています。

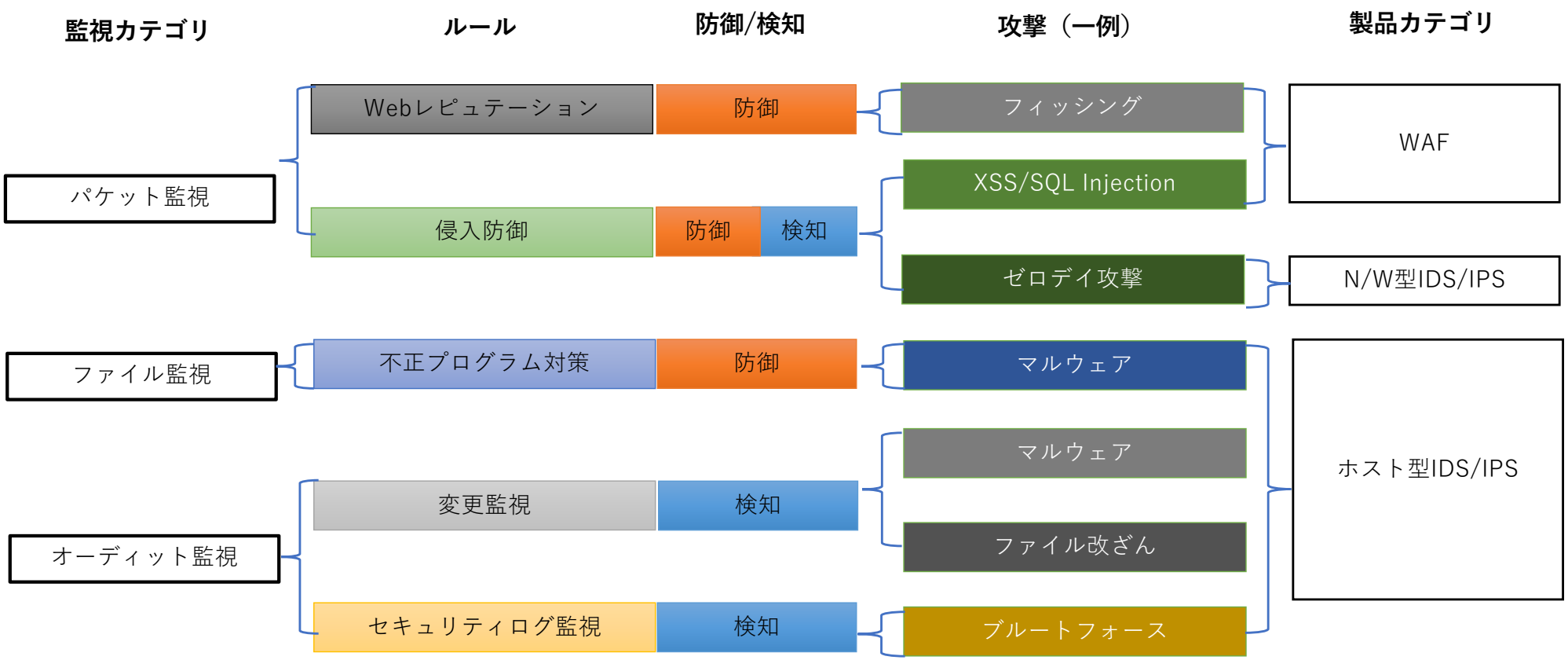
IPA(情報処理推進機構）が定める情報セキュリティ10大脅威（※組織）

		Deep Securityの機能					
	脅威の種別	webレピュテーション	侵入防御	不正プログラム対策	変更監視	セキュリティログ監視	ファイアウォール
1位	標的型攻撃による情報流出			○			
2位	内部不正による情報漏えいとそれに伴う業務停止				○	○	
3位	ウエブサービスからの個人情報の窃取	○		○	○		
4位	サービス妨害攻撃によるサービスの停止						○
5位	ウエブサイトの改ざん	○	○	○	○		
6位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用		○	○			
7位	ランサムウエアを使った詐欺・恐喝			○			
8位	インターネットバンキング、クレジットカード情報の不正利用	○		○	○		
9位	ウエブサービスの不正ログイン			○			
10位	過失による情報漏洩				○		

○：脅威に対して有効な機能

サーバーを狙った攻撃にも、様々な種類があります。
Deep Securityの持つ６つの機能で、主要な脅威に対して、対策を施す事が可能です。

Deep Securityの概要



※攻撃ではない様々な種類の通信や変化を監視することで攻撃を検知する。

※特定端末からの大量のコネクションを、 IP等で送信元を制御することで防御する。

ゲートウェイ型IPS/IDSのご紹介

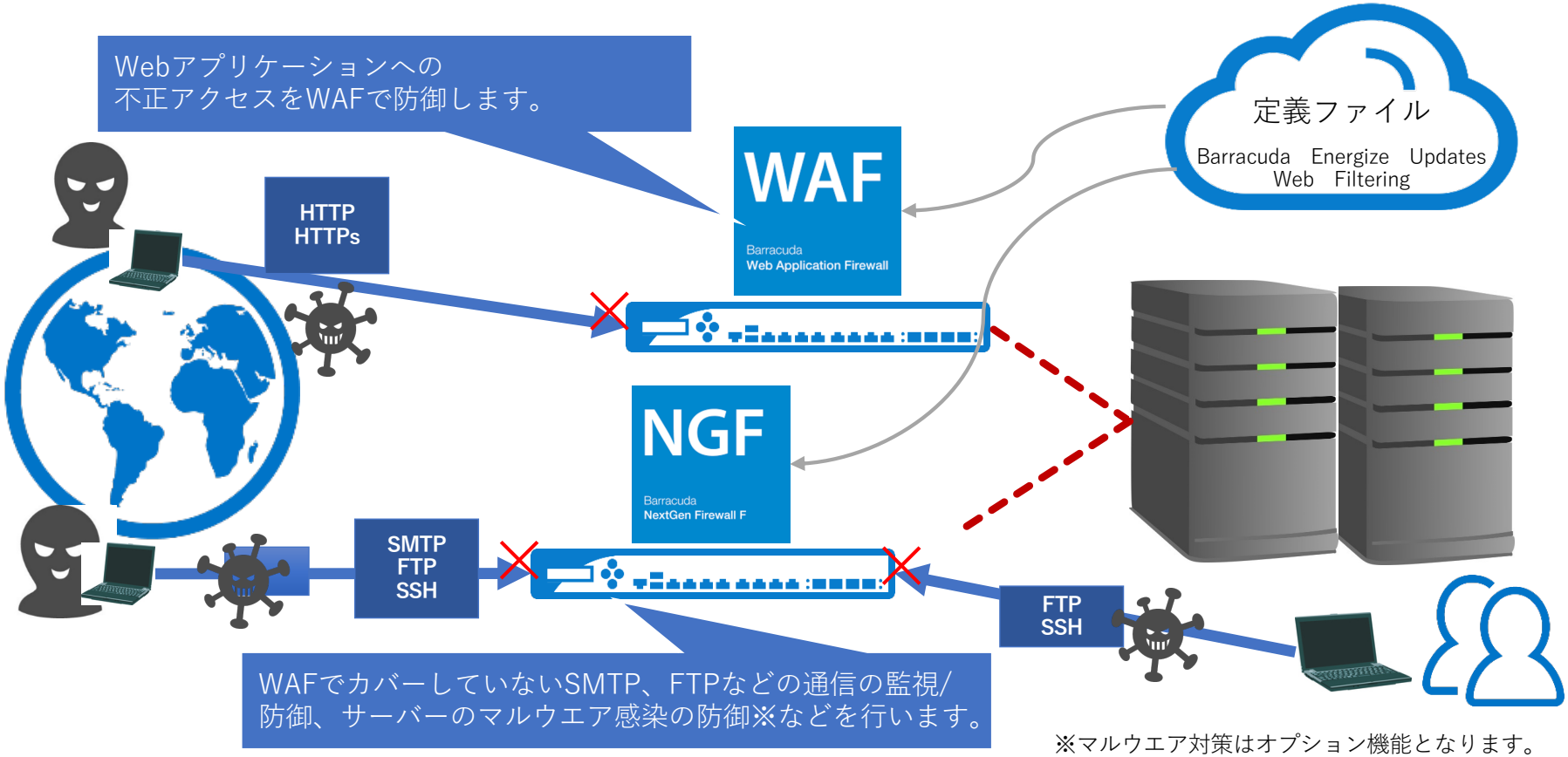
Barracuda NextGen Firewall

Barracuda NextGen Firewallのご紹介

■機能面における特徴

NGFの監視領域

NGFはネットワークの挙動を幅広く監視します。WAFでカバーできない、HTTP/HTTPs以外のプロトコルにも対応し、包括的なセキュリティ対策を実現します。



※マルウエア対策はオプション機能となります。

Barracuda NextGen Firewallのご紹介

■機能面における特徴

NGF機能概要

NGFには多くの機能があります。そのうち、以下機能の利用を想定しています。

機能	概要	Colorkrewセキュリティ監視対象
IDS/IPS	ネットワーク上の通信（HTTP/SMTP/FTP/SSH)を監視、SQLインジェクション、バックドア、ワーム、スパイウエアなどの不正なアクセスをブロックします。	○
Dos/DDos対策	SYNフラッド攻撃など、サーバーのリソースを枯渇させるタイプのDDos攻撃をブロックします。	○
マルウエア防御（オプション）	ネットワーク上（HTTP/SMTP/FTP/SSH)のファイル送受信を監視し、シグネチャ情報と照合し、既知のマルウエアを検知/隔離します。	○
サンドボックス（オプション）	シグネチャ情報と、サンドボックスでの解析、コード解析などを組み合わせて、ゼロデイ攻撃に用いられる、未知のマルウエアを検知/隔離します。	○
メールゲートウェイ＆スパムフィルタ（オプション）	メールサーバーへの通信をチェックし、迷惑メール・スパムメールをブロックします。	×
アプリケーションコントロール	接続されている業務端末で稼働しているアプリケーションを把握し、監視・制御します。	×
webフィルタリング	定義ファイルを参照し、ネットワーク内の端末からの、悪意のあるサイトや、特定ジャンルのサイトへのアクセス制限を実施します。	×

メールやファイル送信等の通信がある場合は利用を検討。
※「（Advanced Threat and Malware Protection Bundle」ライセンスが必要となります。

エンドポイントからのアクセスがある場合は利用を検討。

Barracuda NextGen Firewallのご紹介

■非機能面における特徴

高度な検知率　　※オプション機能

一般的なウイルスソフトで検知できるマルウエアは40%程度と言われます。

Barracuda「Advanced Threat Detecion」では、25万台以上のエンドポイントから収集されたシグネチャ情報と、サンドボックスでの解析を組み合わせて、ゼロデイ攻撃に用いられる、未知のマルウエアをブロック、95%以上の検知率を実現します。

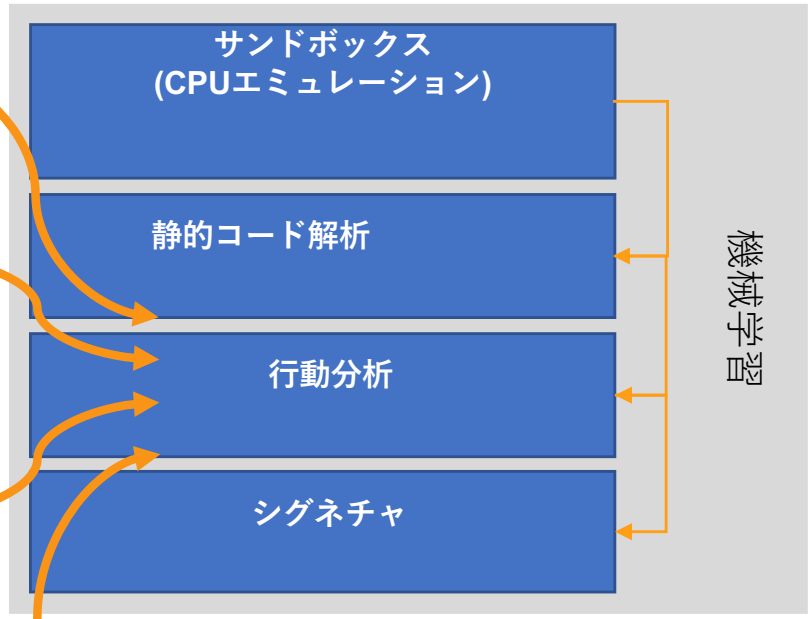
95%以上の検知

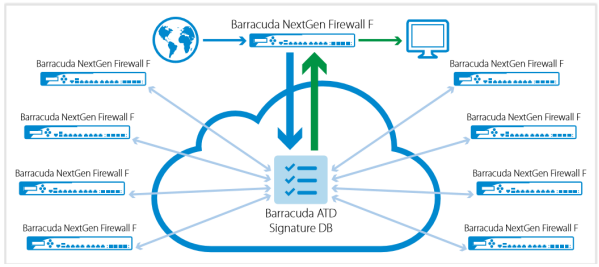
- CPUエミュレーションベースのサンドボックス
- 高度なマルウェアの解析
- 数秒内に900以上の属性をスキャン

- 実際に実行をすることなく解析を実施
- 難読化されたコードの解析
- サンドボックス前のマルウェアの事前フィルタリング

- マルウェアの活動とみられるコード/スクリプトの調査:
- ファイル上書き, 同期, レジストリへのアクセス, ファイル難読化 etc.
- 疑わしいコーディングの分析:
- 過度に長いタイマ、ループ, 数日間に及ぶ実行 etc.

- 25万にも及ぶエンドポイントより収集されたシグネチャ情報
- 多彩なアンチウイルスエンジン
- スパム、ウイルス、その他の既知のマルウェアの防御





Barracuda NextGen Firewallのご紹介

■ 「Advanced Threat Protection」がスキャン可能なファイル

- Microsoft Office files – doc, docx ,ppt, pps, pptx, ppsx, xls, xlsx
- OpenOffice – rtf, open office document extensions
- Microsoft executables – exe, msi, class, wsf
- macOS executables
- PDF documents – pdf
- Android APK files – apk
- ZIP Archives – 7z, lzh, bz, bz2, chm, cab, zip
- RAR Archives – rar4 and rar5
- TAR Archives – tar
- GZ Content – Content compressed with gzip
- Javascript – Manual scan

「Advanced Threat Protection」にてスキャンされるファイルの最大サイズは8MBとなります。

また、モデル毎に一分間内にスキャン可能なファイル数、一ヶ月内のスキャン可能なファイル数の上限が決まっております。

以下ページの「Advanced Threat Protection」箇所をご確認ください。
https://campus.barracuda.com/product/cloudgenfirewall/doc/73719706/licensing

セキュリティ製品比較

BIG-IP ASM/Barracuda WAF（以下、WAF）と、Deep Securityと、Barracuda NG Firewall（以下、NGF）の性能比較

フェーズ	攻撃	対策	対応製品
侵入前	ログインアタック	ふるまい検知	WAF
	セッションハイジャック	Cookie、ｾｯｼｮﾝ改ざんﾁｪｯｸ	WAF
	脆弱性攻撃 （XSS/SQLｲﾝｼﾞｪｸｼｮﾝ/OSｺﾏﾝﾄﾞ攻撃など）	http(s)通信チェック	WAF/Deep Security
	脆弱性攻撃 （XSS/SQLｲﾝｼﾞｪｸｼｮﾝ/OSｺﾏﾝﾄﾞ攻撃など）	非http(s)通信チェック	Deep Security/NGF
	未知のマルウェア	Sandbox（ﾌｧｲﾙ開封ﾁｪｯｸ）	NGF
侵入後	未知のマルウェア	変更監視	Deep Security
	データ改ざん	変更監視	Deep Security
	既知のマルウェア	マルウェア検知・駆除	Deep Security/NGF
	不正アクセス	セキュリティログ監視	Deep Security
犯行開始	悪質サイトへの誘導	Web・IPレピュテーション	WAF/Deep Security/NGF
	情報漏洩	クレジットカードマスキング	WAF

この表は目安です。製品によっては、対策の内容が異なる場合があります。

事例紹介

Colorkrewセキュリティ監視導入実績	
クライアント	システム概要
国際慈善事業機関	コーポレートwebサイト
国際スポーツ機関	国際スポーツイベント関連システム基盤
メガバンク	購買システム基盤
大手地方銀行	アプリサービス基盤
大手建設機器メーカー	購買システム基盤
大手不動産会社	サービス関連webサイト
大手菓子メーカー	コーポレートwebサイト/キャンペーンサイト
大手通信会社	クラウドサービス基盤
大手総合商社	駐車場決済システム基盤他２サービス
大手物流サービス企業	物流システム基盤
大手ホテル・寮運営サービス	管理システム基盤
大手ゲーム会社	サービス関連webサイト
大手ゲーム会社	会員管理/認証/課金決済システム基盤
公共施設（図書館）	検索システム基盤
中堅人事/給与アウトソーシングサービス	人事関連システム基盤
ベンチャー企業等、その他多数	コーポレートwebサイト等
大手Sier	業務システム基盤
中堅IT企業	大規模旅行予約webサイト
大手通信関連会社	サービス関連webサイト
中堅IT企業	納税関連サービスwebサイト
中堅計測・制御機器メーカー	制御システム基盤
株式会社Colorkrew	動画配信サービス「ムービーフル」
	その他多数

くらまね™ Cloud Management Security

【お問い合わせ】

株式会社Colorkrew

くらまねセキュリティProject

salesproject_all@colorkrew.com

TEL 03-5825-5713