



colorkrew

Azure WAFのご紹介

Security Project

confidential



Azure WAFとは

Azure WAFとは



- Application GatewayとFront Doorに導入可能なAzure純正のWAFです。
- OWASPコアルールセット、カスタムルール、Bot保護ルールセットなどが用意されています。

■OWASP (The Open Web Application Security Project) コアルールセット

OWASPとは、Webアプリケーションセキュリティの課題解決を目的とした、国際的なオープンコミュニティです。コアルールセット (CRS) は、Webアプリケーションへの攻撃を検知するためのルールセットで、OWASPがCRSをメンテナンスしています。

■カスタムルール

- IPホワイトリストとブロックリスト
- 地理ベースのアクセス制御
- HTTPパラメータベースのアクセス制御
- リクエスト方式ベースのアクセス制御 (GET、PUT、HEADなど)
- サイズの制約 (クエリ文字列、URI、リクエスト本文など)

※以下は、Front Doorのみ

■レート制限ルール

上記のカスタムルールの条件にしきい値を設定することができます。

例) 「RequestUri」に「/wp-admin/」が含まれるリクエストが、1分間に100回あった場合。

■Bot対策のルールセット

Botには、Bad/Good/Unknownの3つの分類があり、WAFプラットフォームによって管理され動的に更新されます。Bad Botは悪意のあるIPからのBotや、IDを改ざんしたBotが含まれます。悪意のあるIPは、1時間毎に更新されます。Good Botには検証済みの検索エンジンが含まれています。Unknown Botはどちらとも判別のつかないBotです。

Azure WAFとは



OWASP_3.1

すべて展開 ✓ 有効化 ○ 無効化

名前	説明	状態
General		有効
200004	Possible Multipart Unmatched Boundary.	有効
REQUEST-911-METHOD-ENFORCEMENT		有効
911100	Method is not allowed by policy	有効
REQUEST-913-SCANNER-DETECTION		有効
913100	Found User-Agent associated with security scanner	有効
913101	Found User-Agent associated with scripting/generic HTTP client	有効
913102	Found User-Agent associated with web crawler/bot	有効
913110	Found request header associated with security scanner	有効
913120	Found request filename/argument associated with security scanner	有効
REQUEST-920-PROTOCOL-ENFORCEMENT		有効
920100	Invalid HTTP Request Line	有効
920120	Attempted multipart/form-data bypass	有効
920121	Attempted multipart/form-data bypass	有効
920130	Failed to parse request body.	有効
920140	Multipart request body failed strict validation: PE %(REQBODY_PROCESSOR_ERROR), BQ ...	有効

Azure Portal

- コアルールセット
チェックボックスをON/OFFにすることで、CRSの適用を有効化/無効化します。

カスタム規則

保存 × 破棄 最新の情報に更新

カスタム作成規則を使用してポリシーを構成します。規則が一致すると、規則に定義された対応するアクションが要求に適用されます。この一致が処理されると、優先度の低い規則はそれ以上処理されません。規則の優先度が小さいほど優先度が高くなります。 [詳細情報](#)

+ カスタム ルールの追加

優先度	名前	アクション
2	blockEvilBot	ブロック

カスタム ルールの編集

一致の種類 ○
文字列

一致変数
RequestHeaders

一致変数 * ○
ヘッダー名 ○
User-Agent

+ 別の一致変数を追加

操作
 次である 次ではない

演算子 *
次の値を含む

変換
Lowercase
変換を選択

一致する値
evilbot
一致を評価する値を入力してください

- カスタムルール (例)
「RequestHeaders」の「User-Agent」に「evilbot」という文字列があればブロック。



Application GatewayのWAFの注意点

■必須ルールの存在

- 必須ルールは、下記の条件を満たすと検知/防御を行います。
 - ファイルアップロードなしの、要求本文のデータ長が、128KBを超えている場合。
 - ファイルアップロードを含む、要求本文のサイズが、750MBを超えている場合（WAF V2の場合）。
 - 要求本文が何らかの要因で読み取れず、文字列の解析ができない場合。
 - WAF エンジンで内部エラーが発生した場合。
- このルールが検知/防御されると「200002」のアラートがでますが、「WAFポリシー」の「管理されているルール」にはこの番号がないため、このルールのみを無効にすることはできません。
「WAFポリシー」の「ポリシー設定」で「要求本文の検査」を「オフ」にすると無効にできますが、HTTPリクエストの「Request Body」の検査が無効になるため注意が必要です。

グローバルパラメーター	
要求本文の検査 ⓘ	<input checked="" type="radio"/> オン <input type="radio"/> オフ
要求本文の最大サイズ (KB) * ⓘ	<input type="text" value="128"/>
ファイル アップロードの最大サイズ (MB)	<input type="text" value="100"/>

参考

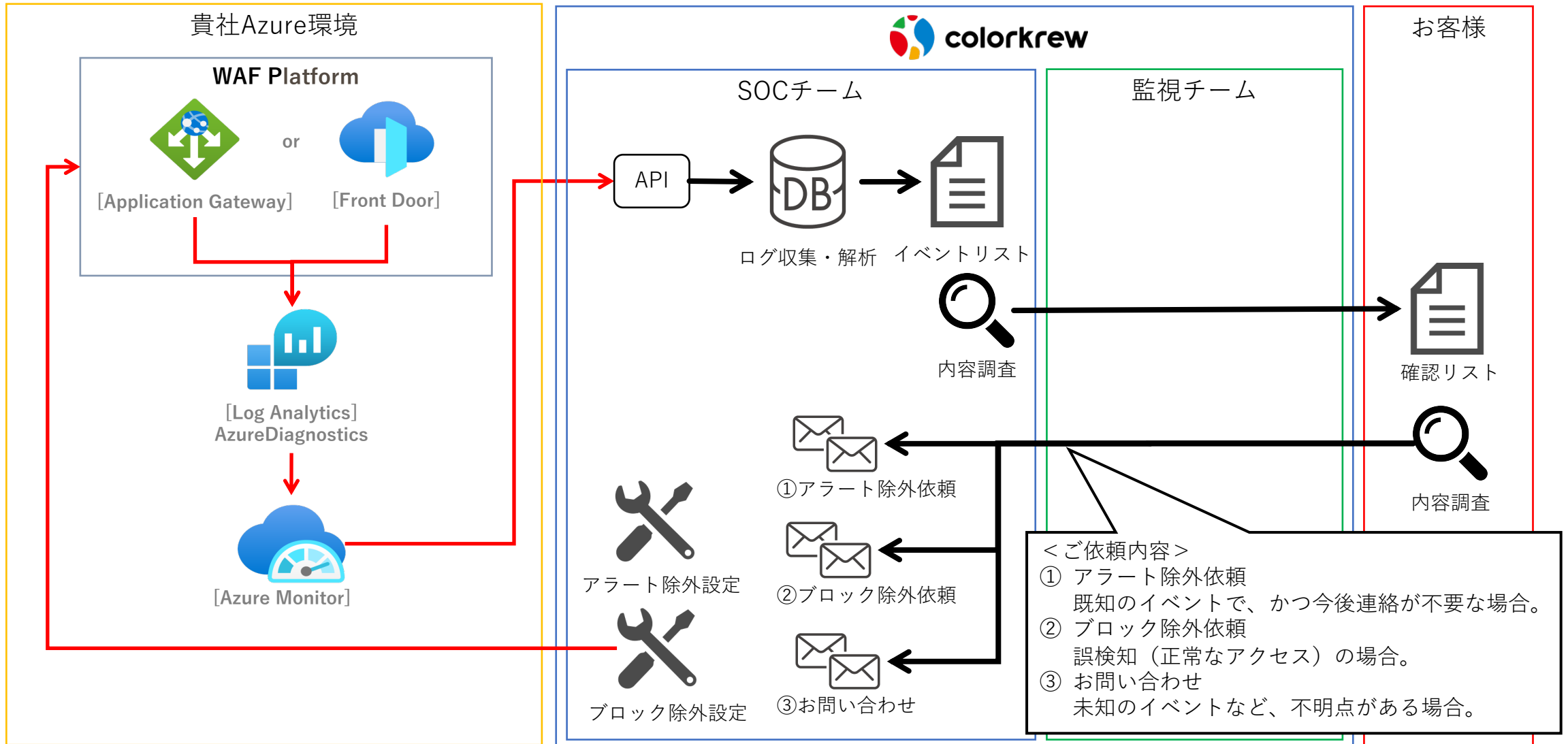
<https://docs.microsoft.com/ja-jp/azure/web-application-firewall/ag/application-gateway-customize-waf-rules-portal>

<https://docs.microsoft.com/ja-jp/azure/web-application-firewall/ag/application-gateway-waf-configuration>

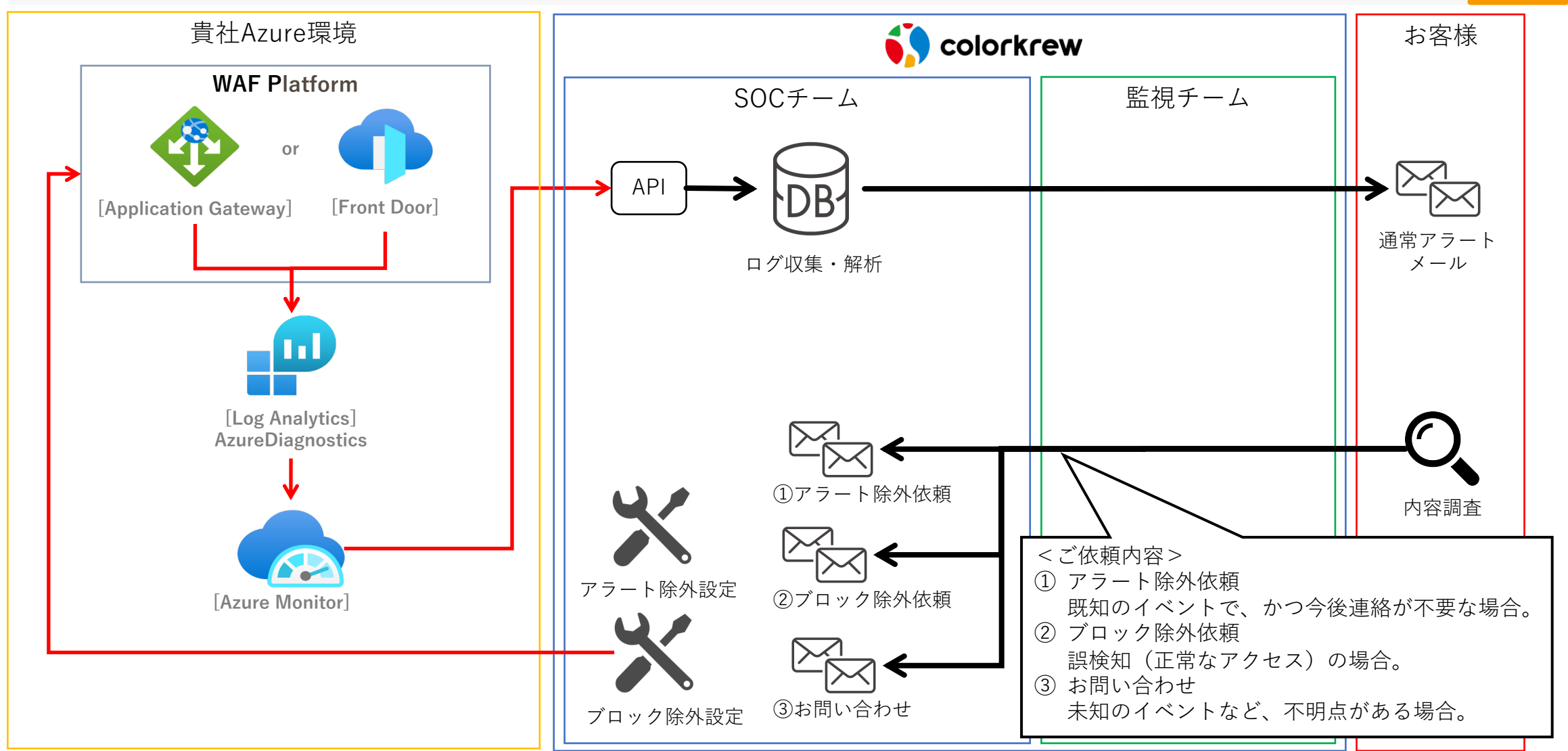


SOCとは

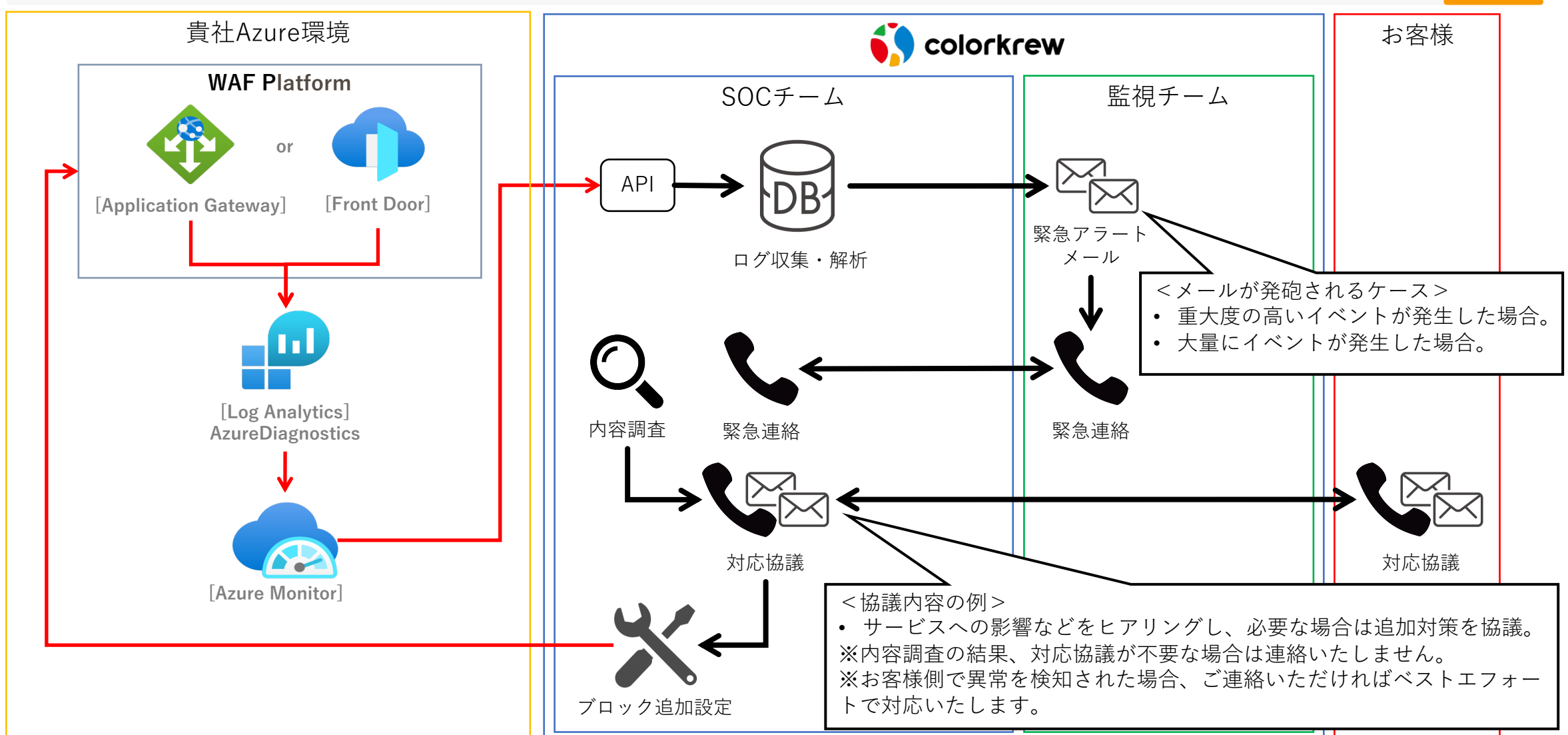
SOC導入時のフロー



SOC通常運用時のフロー（営業時間内）



SOC緊急運用時のフロー（24時間365日）



アラートメール（サンプル）



株式会社Colorkrew
ご担当者様

お世話になっております。
Colorkrewの監視チームです。
セキュリティアラートが発生いたしましたので、ご報告いたします。
24件あります。

```
<001/024>-----  
[TenantId : XXXXXXXXXXXX]  
[TimeGenerated : 2020-09-08 04:26:18.115000]  
[ResourceId : /SUBSCRIPTIONS/ XXXXXXXXXXXX]  
[Category : ApplicationGatewayAccessLog]  
[Resource : WAF-V2-01]  
[ResourceType : APPLICATIONGATEWAYS]  
[OperationName : ApplicationGatewayAccess]  
[requestUri_s : /webapp/index.asp]  
[originalRequestUriWithArgs_s :  
/webapp/index.asp?id=%22%3E%3Cscript%3Ealert(1);%3C/script%3E]  
[originalHost_s : XXX. XXX. XXX. XXX]  
[Type : AzureDiagnostics]  
[_ResourceId : /subscriptions/ XXXXXXXXXXXX]  
[log_datetime_jst : 2020-09-08 13:26:18.115000]  
[clientIp : XXX. XXX. XXX. XXX]
```

※一部省略しています。

SOC価格表



初期費用

費用計	備考（作業内容）
¥300,000 ※Application GatewayもしくはFront Door 1台あたりの価格です。	<ul style="list-style-type: none">• Azure WAFの設定• アラートの設定• 初回チューニング

月額運用費用

セキュリティ監視	備考（作業内容）
¥100,000 ※Application GatewayもしくはFront Door 1台あたりの価格です。	<ul style="list-style-type: none">• WAFログの監視• グレーゾーン（誤検知/攻撃）の報告• クリティカルな攻撃の報告• WAFルールの有効化/無効化

- セキュリティイベントログ：5,000件以内/月を想定した価格です。これを超える場合は別途お見積りとなります。
- セキュリティに関わる監視です。死活監視、リソース監視などは含まれません。
- Azure WAFには、回避不能なルール（誤検知の際、Azure WAF側で除外設定できないルール）があります。このような場合は、アプリケーション側の改修をお願いいたします。
- Azure 利用料は含まれません。
- 契約期間は、最低6か月とさせていただきます。



colorkrew

Let's Go Inspire the World