colorkrew

Azure WAFのご紹介

Security Project

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。

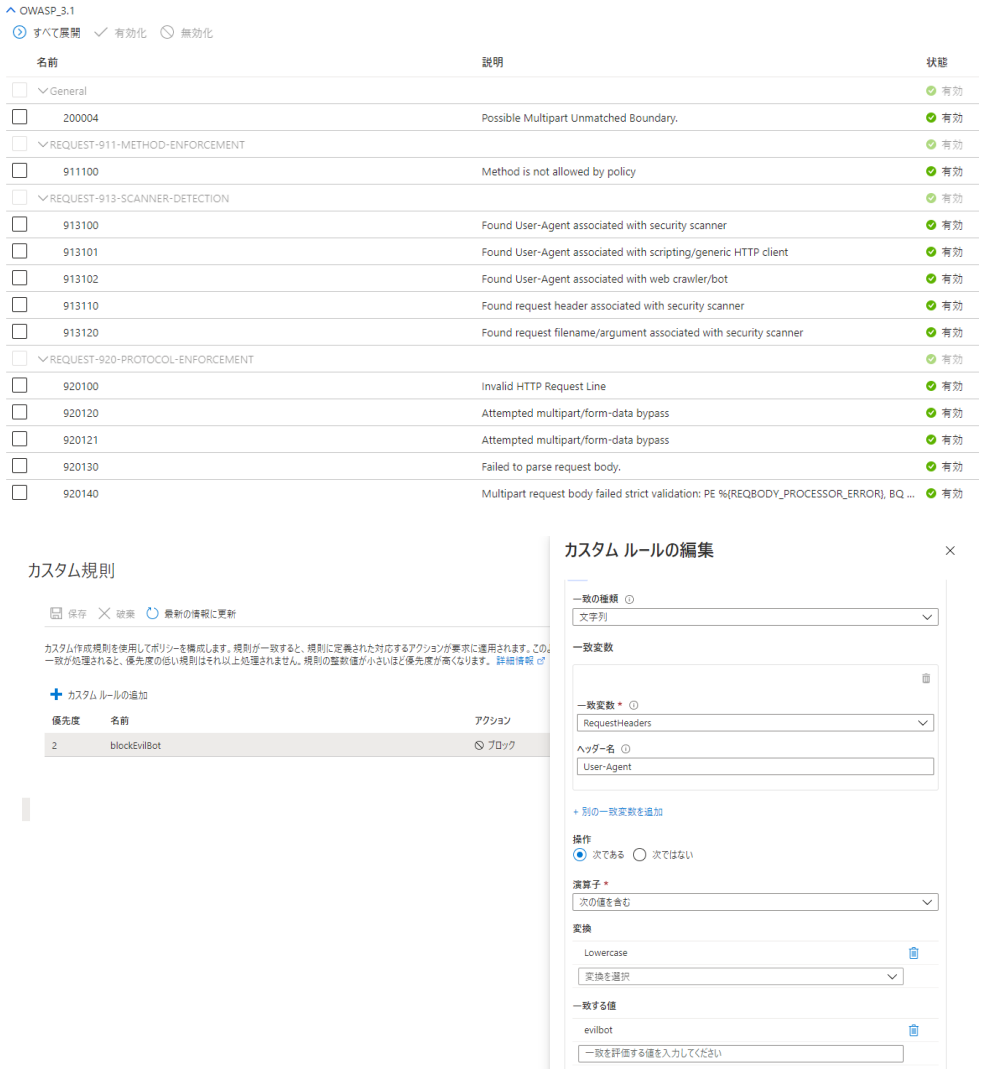
■OWASP（The Open Web Application Security Project）コアルールセット
OWASPとは、Webアプリケーションセキュリティの課題解決を目的とした、国際的なオープンコミュニティです。
コアルールセット（CRS）は、Webアプリケーションへの攻撃を検知するためのルールセットで、OWASPがCRSをメンテナンスしています。

■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



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。

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

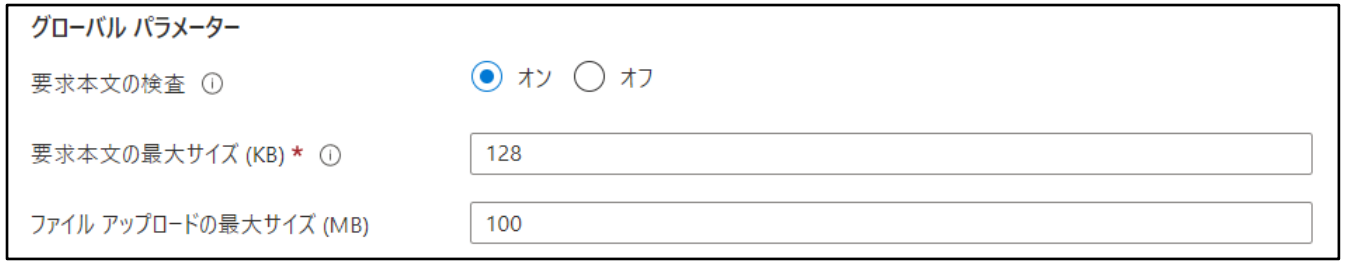
Azure WAFとは

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。
  1．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。
  2．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）。
  3．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。
  4．WAF エンジンで内部エラーが発生した場合。

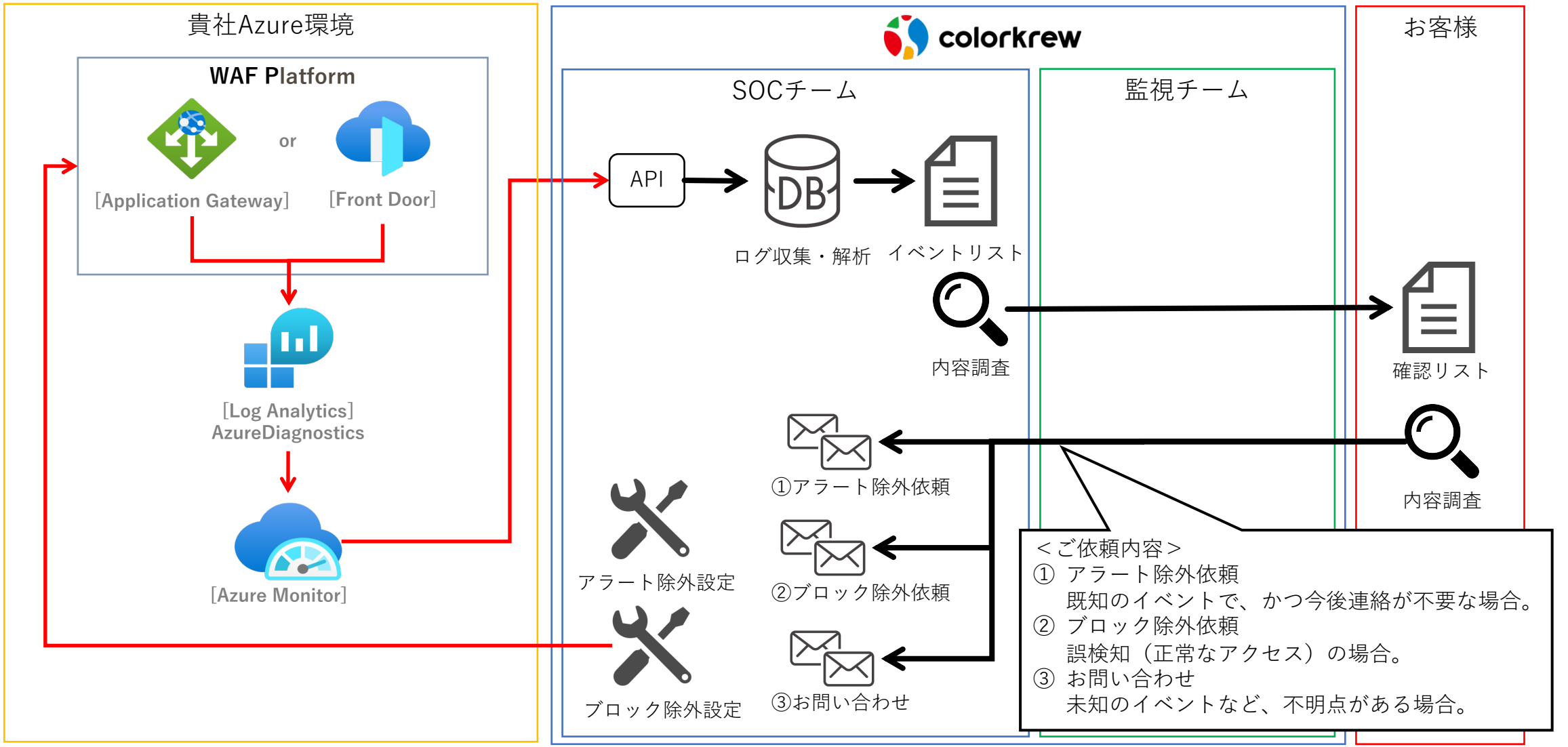
- このルールが検知/防御されると「200002 」のアラートがでますが、「WAFポリシー」の「管理されているルール」にはこの番号がないため、このルールのみを無効にすることはできません。
  「WAFポリシー」の「ポリシー設定」で「要求本文の検査」を「オフ」にすると無効にできますが、 HTTPリクエストの「Request Body」の検査が無効になるため注意が必要です。



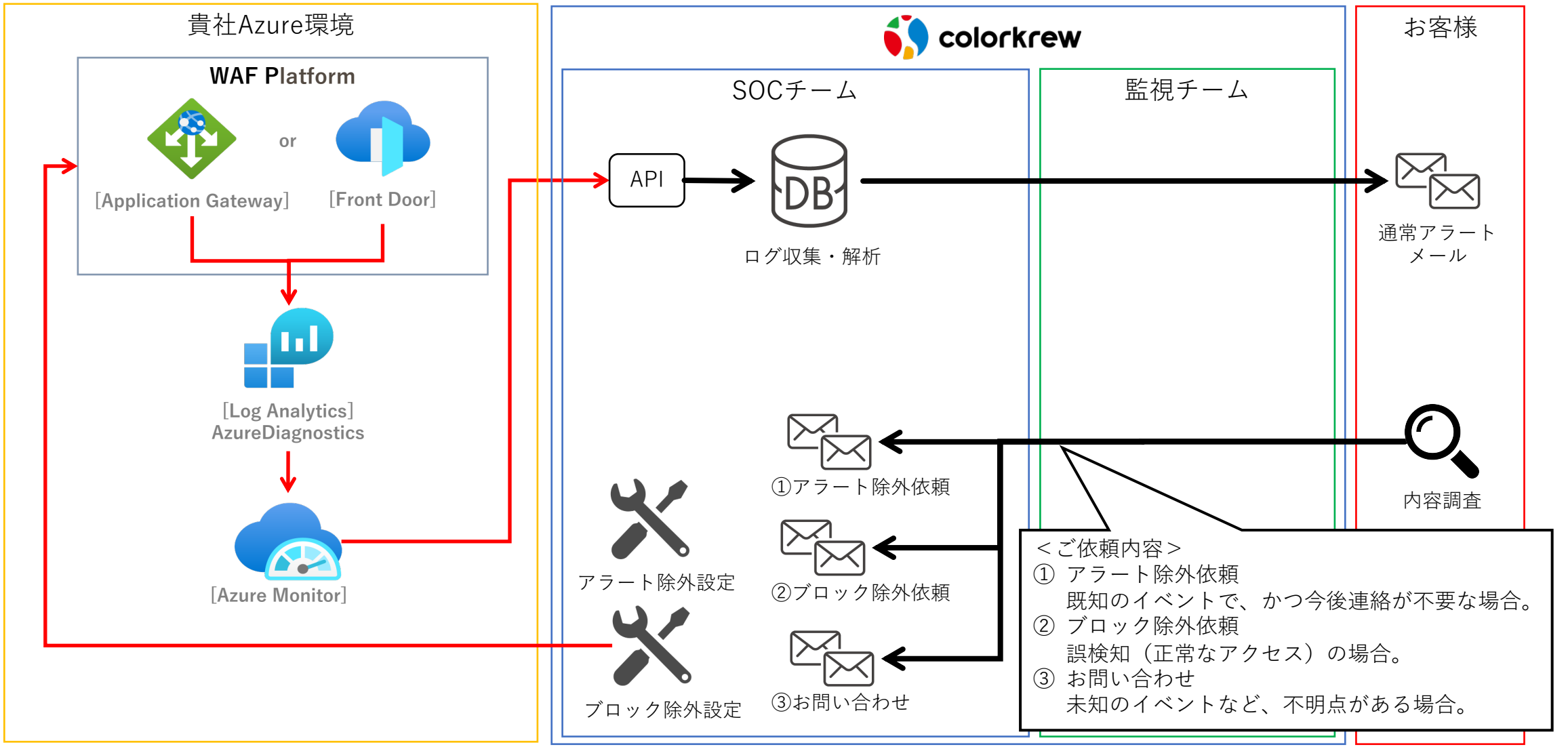
- 参考
  https://docs.microsoft.com/ja-jp/azure/web-application-firewall/ag/application-gateway-customize-waf-rules-portal
  https://docs.microsoft.com/ja-jp/azure/web-application-firewall/ag/application-gateway-waf-configuration

SOCとは

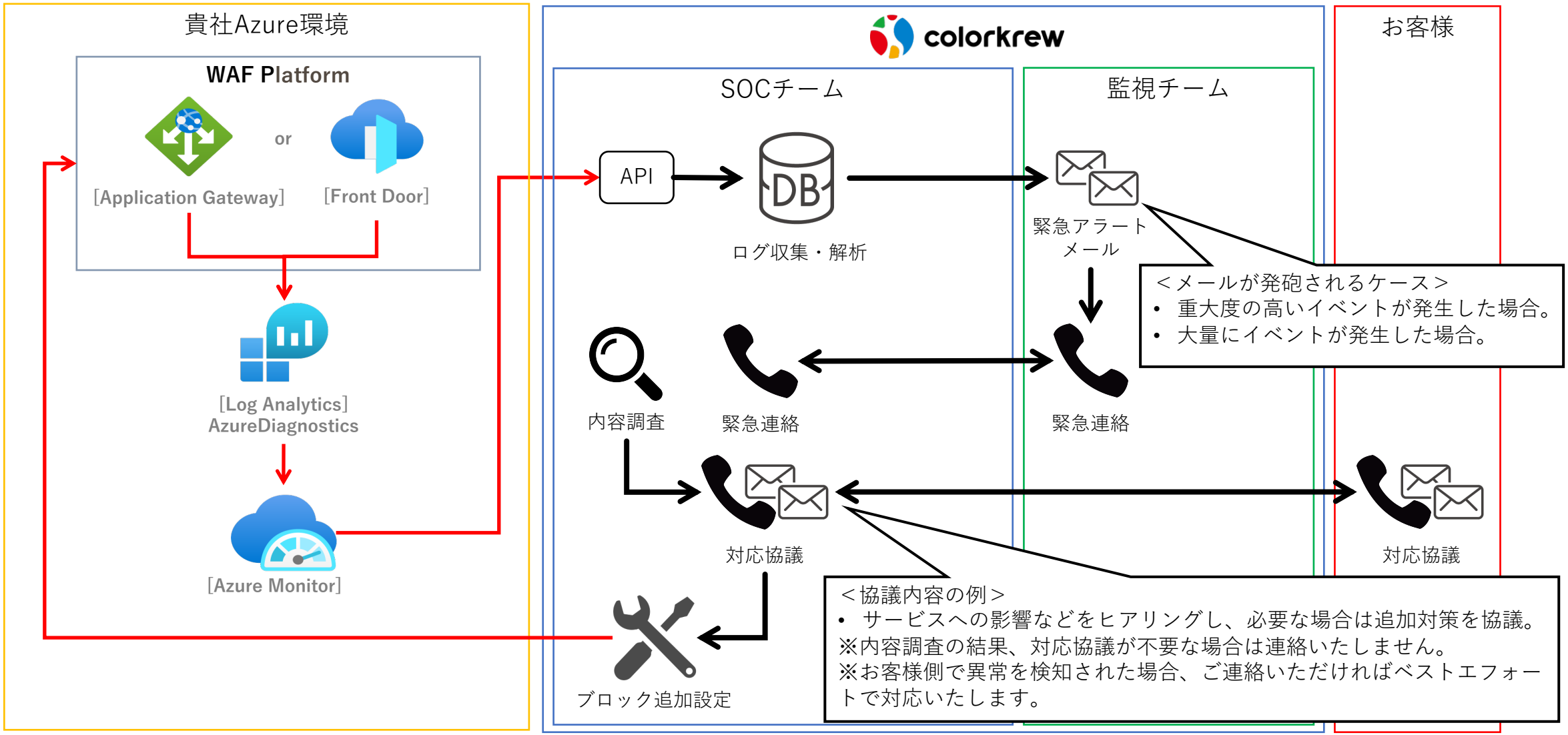
SOC導入時のフロー


貴社Azure環境
WAF Platform
or
[Application Gateway]
[Front Door]
[Log Analytics]
AzureDiagnostics
[Azure Monitor]
colorkrew
SOCチーム
監視チーム
お客様
API
DB
ログ収集・解析
イベントリスト
内容調査
確認リスト
内容調査
①アラート除外依頼
②ブロック除外依頼
③お問い合わせ
アラート除外設定
ブロック除外設定
＜ご依頼内容＞
① アラート除外依頼
既知のイベントで、かつ今後連絡が不要な場合。
② ブロック除外依頼
誤検知（正常なアクセス）の場合。
③ お問い合わせ
未知のイベントなど、不明点がある場合。

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 : XXXXXXXXXX]
[TimeGenerated : 2020-09-08 04:26:18.115000]
[ResourceId : /SUBSCRIPTIONS/ XXXXXXXXXX]
[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/ XXXXXXXXXX]
[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。	・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。	・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