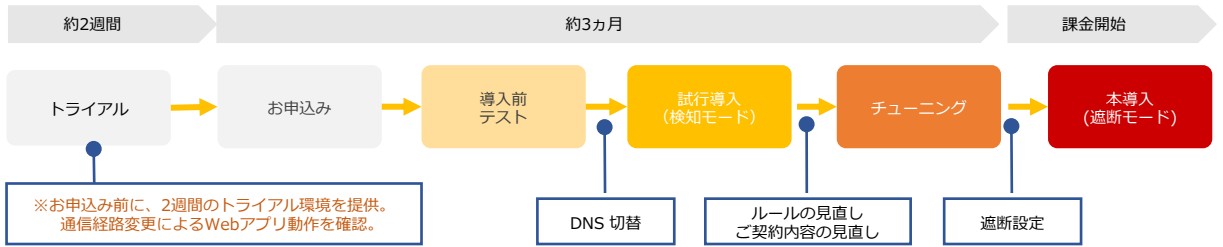


導入までの流れ（標準スケジュール例）



※上記 5 ステップそれぞれのタイミングにおいて、お客様に実施いただく作業がございます。
※お申込み翌月から最大3ヵ月後には、導入状況に関わらず月額料金が発生します。

※DNS 切替後の実績を踏まえ
配信データ量等の見直しをご提案します

提供機能

標準機能

攻撃防御 ●各種攻撃通信を遮断（下記を参照） ●DDoS 攻撃防御（帯域無制限）

アクセス制御機能（要申請） ●特定 URL 除外 ●特定 IP アドレスの拒否/許可

通知機能 インシデント発生時には通知すべき内容を精査の上、メールでお知らせ

※専門アナリストによる分析結果や対策案をご提示

ログ機能 アクセスログの取得が可能（FTPS/SSH 利用）

※保存容量はご契約内容に依存

月次レポート機能 配信データ量の推移グラフ、およびホストごとの防御実績、
検知イベント一覧、攻撃種別の円グラフなどが閲覧可能

オプション機能

HTTPサイト接続保護 HTTP通信のみを行う Origin サイトへの直接アクセスを禁止する場合に必要

※アクセス制限自体は、お客様ファイアウォールにて実施

ログの保存容量の拡張 ログの保存容量を拡張させたいお客様向けのオプション（1GB単位で拡張可能）

※基本サービスのサイト費用には1GB分のログ保存容量を含む

通知メールサンプル

弊社D.e-WAFにてWAFのアラート通知が上がりましたので連絡致します。
只今イベントデータ解析中ですので、
結果は後ほどメールにてご報告いたします。

解析結果が完了するまで、お客様にてお願いする対応はございません。

本イベントが収束するまでに、新たなアラート通知が発生した場合には
本件にて対応致します。
アラートの詳細は以下の通りです。

ALERT DETAILS

Notification: P3 High Warned Rate Activity

Start Date and Time: 2018/05/21 04:55 GMT (2018/05/21 13:55 JST)

Host: www.example.co.jp

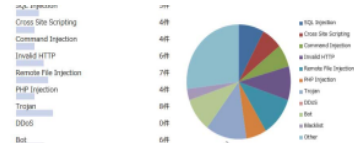
;
(以下省略)

レポート画面サンプル

■ 日別配信データ量・アクセス数



■ 検知イベント



検知・防御可能な不正通信の例※

分類	主な攻撃概要
認証	●総当たり ●パスワードリスト攻撃
クライアント側での攻撃	●クロスサイトスクリプティング ●コマンドインジェクション
コマンド実行	●バックオーバーフロー ●SQLインジェクション ●リモートファイルインクルージョン ●SSL インジェクション ●XPath インジェクション ●OS コマンドインジェクション ●URL エンコード攻撃 ●Apache Struts 1 & 2 を利用した攻撃
情報公開	●ディレクトリインデクシング ●情報漏えい ●バストラバーサル ●リソース位置を推測
サービス妨害	●DoS/DDoS 攻撃

※すべての攻撃を防ぐことを保証するものではありません

記載されている会社名、製品名およびサービス名称は各会社の商標または登録商標です。
記載内容は2019年1月現在のものです。記載された仕様は予告なく変更する場合があります。



株式会社トヨタシステムズ 営業本部

TEL : 050-3142-7889 Mail : helpdesk01@tns.toyotasystems.com

URL : <https://www.toyotasystems.com>



2019年第1版