事例：OSSを用いた大容量ログの保存＋可視化

オープンソース・ソフトウェアを組み合わせて大容量ログの保存及び可視化を実現
この事例のお客様は金融機関であり、内規によりセキュリティアプライアンス (UTM) のログを1年間以上保存したい、というご要望がありました。また、収集したログを解析、集計、検索することも要件となっていました。

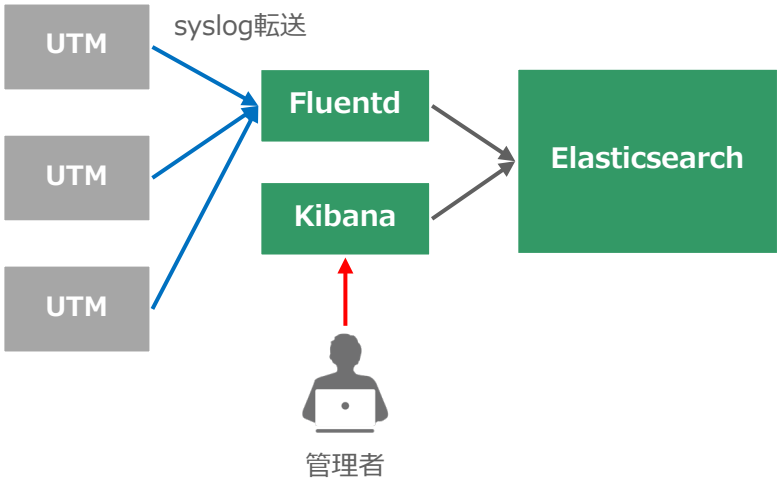
通常サーバやネットワーク機器のログを収集する際には syslogという標準規格を用いて外部のサーバに転送するというのが一般的ですが、Linux定番の syslogサーバでは受信と保管のみで、検索や集計には他のツールと組み合わせる必要があります。また、ファイルベースでの検索ではファイル数やファイルサイズが大きくなるとパフォーマンスが低下します。

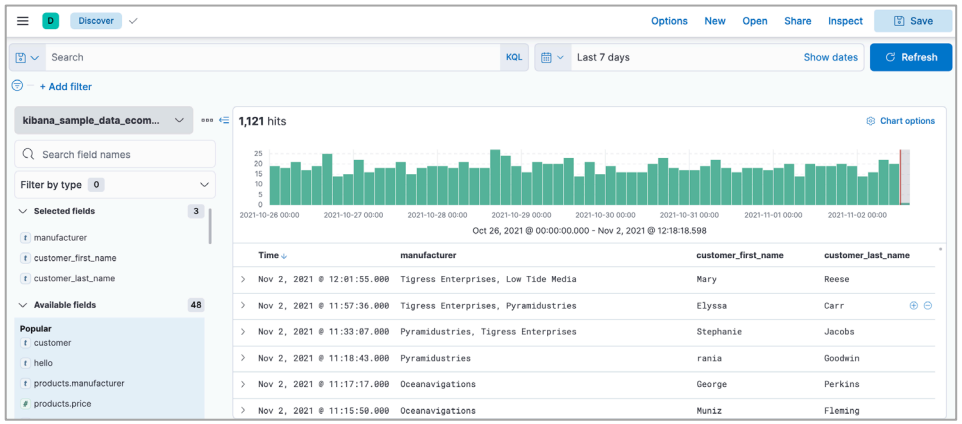
本事例ではお客様要件に対応するために以下のOSS（オープンソース・ソフトウェア）を採用しました。

- Elasticsearch：全文検索に最適化されたデータベース。大容量データの高速な全文検索が可能。
- Kibana： Elasticsearchの開発元である Elastic社が開発するElasticsearchのフロントエンド。
- Fluentd：様々な形式のデータに対応したデータコレクタ。

商用製品を利用する場合には高額な初期・ランニング費用が必要ですが、これらのOSSを組み合わせることで低予算で大容量ログの保管・解析・検索ができる環境を構築することができました。

導入年		2018
ユーザ業種		金融
担当工程	PM	○
	基本設計	○
	詳細設計	○
	開発	○
	構築	○
	導入	○
	保守	○





Kibana 画面サンプル
（Elastic Guide より引用）