# ネットワーク監視のための IBM Security QRadar SIEM 導入支援サービス

## 【概要・特徴】

- IBM Security QRadar SIEM (QRadar) により、ネットワーク機器などからログ収集を行い、動的に相関分析し、リアルタイムに問題を把握することができます。システム全体が“可視化”され、設定したルールに従って自動的に相関分析されたオフェンス（検知された攻撃情報）を受け取ることができ、セキュリティレベルを強靭化します。
- 本サービスでは、収集・分析対象とするログを確認させていただき、QRadarの設計・導入、各種ルール、オフェンスの設定を行います。

## 【サービス内容】

- 要件確認（取り込むログ、検知したい項目など)
- 設計
- QRadar の導入と構成
  - ログ取り込み、ルールの設定
- テスト
- ドキュメント作成
- 引継ぎ

作成物
- 設計書兼設定書
- テスト計画兼報告書
- 操作手順書

※お客様ごとに、取り込むログの数・フォーマットなどをヒアリングの上、作業スケジュールおよび費用についてお見積もりをさせていただきます。

※当サービスには、基盤構築（ハードウェアのセットアップ、OS導入など）、セキュリティ運用設計は含まれません。

**実現イメージ**