情報分析型セキュリティー・ソリューション
「IBM Security QRadar(R)」取り扱い開始！

QRadarとは？

ログや脅威、脆弱性やリスクに関連したデータを収集、蓄積し、分析するための統一アーキテクチャーを提供するセキュリティー・インテリジェンス製品

セキュリティー・インテリジェンスとは？

企業のITセキュリティーとリスク管理に影響を与える、ユーザーやアプリケーション、IT基盤から生成されるデータをリアルタイムに収集、正規化、分析すること

セキュリティー・インテリジェンスは、**防御、検出、改善**を行うことでリスクと脅威を管理し、実行可能で包括的な洞察を提供します

セキュリティー・インテリジェンスが必要となる背景

標的型攻撃、 ワーム、トロイの木馬、マルウェア	巧妙化する攻撃	**攻撃の高度化・多段階化により、セキュリティー脅威の発見がますます困難になっている**
セキュリティー担当者	セキュリティー担当者のスキル・人材不足	**IT部門にはセキュリティー担当者の技術力、および人材が不足している**
	IT環境の複雑化	**複雑化する IT 環境において、単一のセキュリティー対策では追いつかない**

「IBM Security QRadar」は巧妙化する脅威にも対応致します！

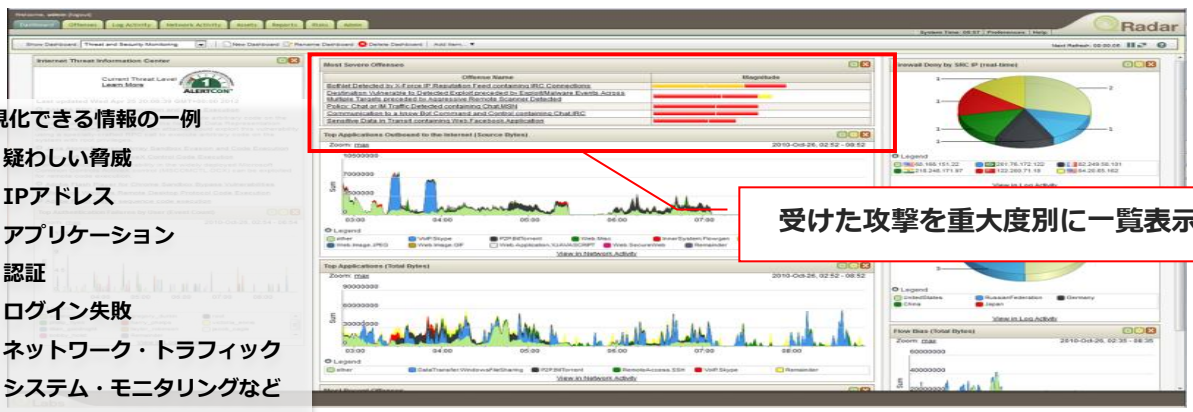
QRadarの３つの特長

１． 膨大なログ情報から、潜在的な脅威や不正を解析・予測

膨大なログ情報	相関分析、振る舞い検知により、疑わしい脅威のみを絞込み	相関分析、振る舞い検知により、疑わしい脅威のみを絞込み

■人手では分析が困難な、大量のログ情報から異常を検知、予測することが可能
■ネットワーク上を流れるデータとログ情報をマッチングする技術により、問題の発生源と発生範囲をリアルタイムに把握することが可能

２．社外からの攻撃や社内の不正状況をリアルタイムに可視化 対策の迅速化が可能に！



可視化できる情報の一例

- 疑わしい脅威
- IPアドレス
- アプリケーション
- 認証
- ログイン失敗
- ネットワーク・トラフィック
- システム・モニタリングなど

３．知見を生かしたルール、検索パターンを製品に装備

１０００種類以上のルールと分析

・ボットネットC&C通信の検出
・脆弱性情報と現存する脆弱性の比較
・複数の認証失敗後の認証製鋼

１００種類以上の検索パターンとレポート

・各ログで失敗したログイン情報
・国ごとの受信イベント情報など