

IBM® QRadar®

ネットワークに潜む脅威をリアルタイムで検知し、オンプレミス・クラウドで提供

オンプレミス



物理アプライアンス、仮想アプライアンスから選択することができます

クラウド環境



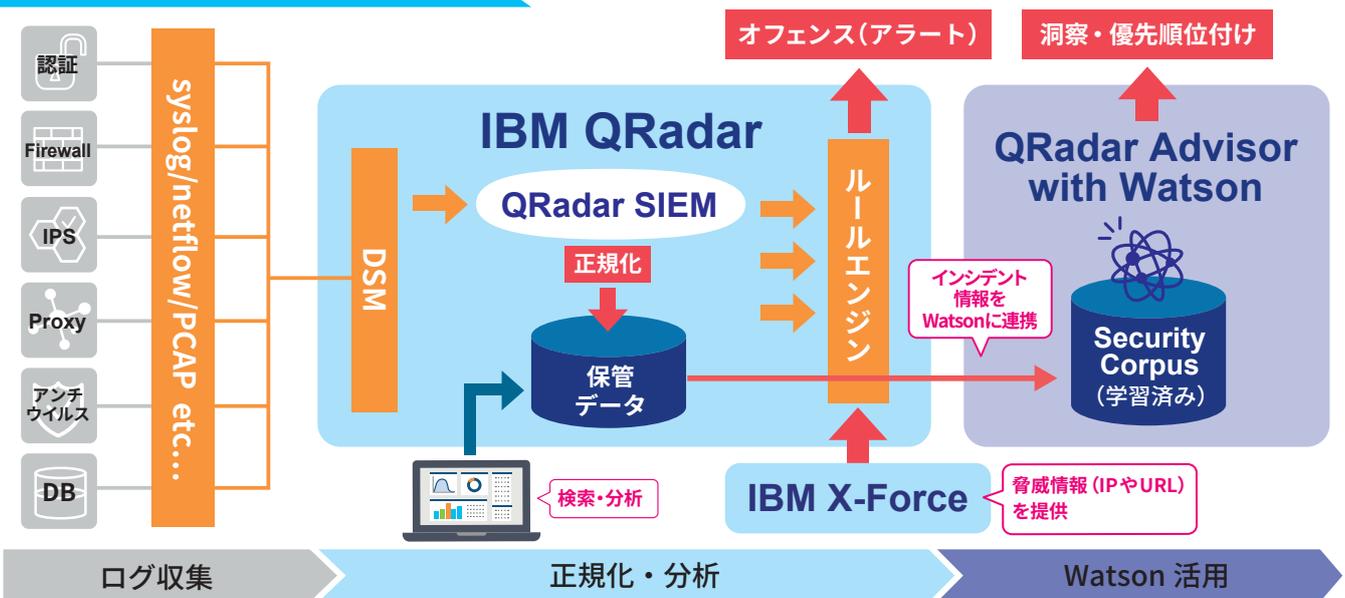
AWS、Azure、GCPのマーケットプレイスよりクラウド上にIBM QRadarを導入することができます

クラウド環境 (IBM QRadar on Cloud)

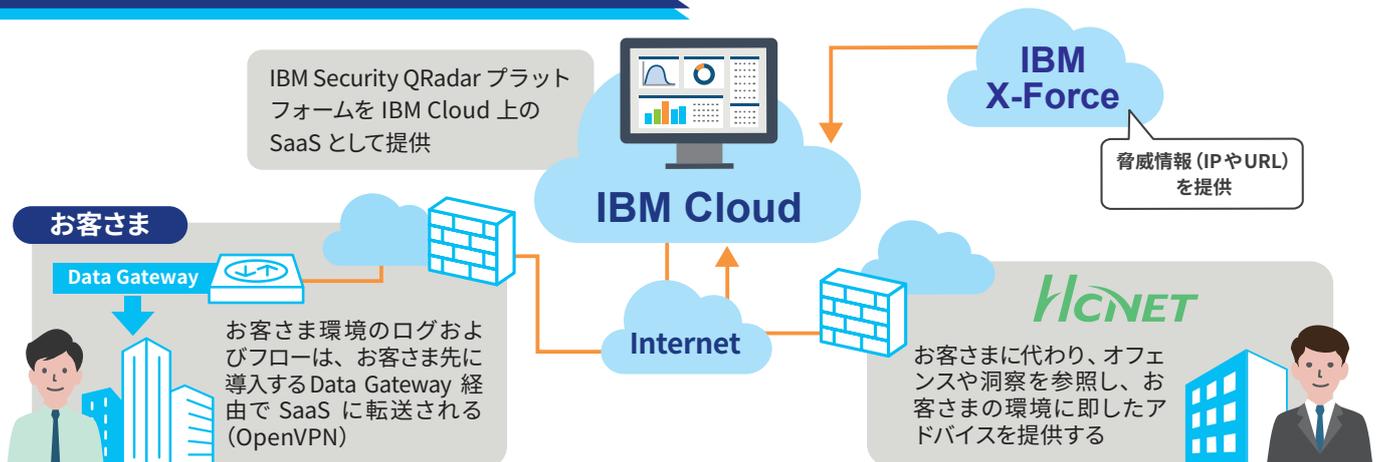


IBM Cloud 上の QRadar を、SaaS として利用することができます

IBM QRadar アーキテクチャ



IBM QRadar on Cloud 提供イメージ



優位性



解析ルール

(セキュリティを見える化)

- ▶ 100 種類以上のデフォルトルールにより、構築を早期に実現
- ▶ 継続的なアップデートもご提供しており、最新の脅威にも対応可能



幅広い情報源

(X-Force による知見)

- ▶ X-Force の知見を生かした 100 種類以上の関連ルールを標準提供
- ▶ レピュテーション情報を高い頻度でアップデート



リアルタイム

(運用負荷の軽減)

- ▶ 脅威検出から即時アラートすることによる素早い調査・対処が可能
- ▶ セキュリティログだけではなく、ネットワークトラフィックも関連対象とすることにより、未知なる脅威の早期発見を実現



解析の自動化

(相関分析による異常検知)

- ▶ 1 日に何十万件にもおよぶログデータを横断的に自動解析
- ▶ 人手では不可能な瞬時の解析とコスト削減
- ▶ DSM (デバイス・サポート・モジュール) によりデータの意味付けを行いログを正規化し解析



コグニティブ技術と拡張性

(セキュリティ監視プラットフォームとしての拡張性)

- ▶ Watson (コグニティブ技術) のセキュリティ領域への活用
- ▶ QRadar は SIEM だけでなく、リスク管理、脆弱性管理、フォレンジックスなどへの段階的な機能拡張が可能 ※1

機能



App Exchange

- ▶ さまざまなベンダーセキュリティソリューションを効果的に活用



インシデント フォレンジックス ※2

- ▶ PCAP からのネットワークセッションの復元
- ▶ データピボットと可視化ツール
- ▶ 誰が/何を/何時? の明瞭化を提供



リスク&脆弱性管理

- ▶ ネットワークセキュリティの構成管理モニタリング
- ▶ 脆弱性スキャン & 優先順位付け
- ▶ 予測された脅威モデリングとシミュレーション



フロー収集

- ▶ Layer 7 アプリケーション・モニタリング
- ▶ 物理および仮想環境に対応



相関分析 (SIEM)

- ▶ ログ、フロー、脆弱性、相関分析
- ▶ 洗練されたアセット・プロファイリング
- ▶ オフェンス管理とワークフロー
- ▶ データ・ストア (正規化・保管・検索)

従来の SIEM 製品との違い

▶ セキュリティインテリジェンス

▶ イベントログやセキュリティログを蓄積・管理・分析

▶ イベントログを一元的に管理

ログ管理製品

SIEM 製品

IBM QRadar

イベントログやセキュリティログに加えて、**ネットワークトラフィック情報**をリアルタイム収集し、**自動的に正規化**。また、**知見を生かした提供ルール**に基づいて自動的に分析。

※1: QRadar on Cloud は除く (フォレンジックス、リスク管理) ※2: QRadar on Cloud は除く

HCNET エイチ・シー・ネットワークス株式会社

〒111-0053 東京都台東区浅草橋 1-22-16 ヒューリック浅草橋ビル 4F

▼ お問い合わせ・資料請求

<https://www.hcnet.co.jp/form/inquiry>

HCNET QRadar



HCNET およびそのロゴは、エイチ・シー・ネットワークス株式会社の登録商標です。IBM は、世界の多くの国で登録された International Business Machines Corp. の商標です。AWS は、米国その他の諸国における、Amazon.com, Inc. またはその関連会社の商標です。記載されている社名および製品名は、各社の商標または登録商標です。掲載した商品は、改良などのため予告なしに内容を変更することがあります。記載の製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国輸出管理規則などの外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、弊社担当営業にお問い合わせください。